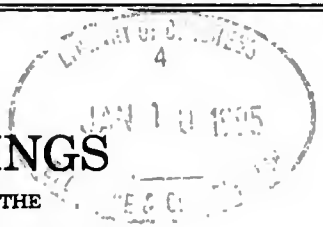
S. HRG. 103–836

HIGH-TECH PRIVACY ISSUES IN HEALTH CARE



HEARINGS

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED THIRD CONGRESS

FIRST AND SECOND SESSIONS

ON

EXAMINING THE QUALITY AND HIGH TECHNOLOGY PRIVACY ISSUES WITH REGARD TO HEALTH CARE OF THE NATION'S CURRENT MEDICAL DELIVERY SYSTEM, FOCUSING ON THE USE OF HIGH-TECH EQUIPMENT TO IMPROVE PATIENT MEDICAL RECORD SYSTEMS AND INSURE THE SECURITY AND PRIVACY OF PATIENT INFORMATION

OCTOBER 27, 1993, AND JANUARY 27, 1994

Serial No. J–103–34

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

84–464 CC WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-046274-6

COMMITTEE ON THE JUDICIARY

JOSEPH R. BIDEN, JR., Delaware, *Chairman*

EDWARD M. KENNEDY, Massachusetts
HOWARD M. METZENBAUM, Ohio
DENNIS DECONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
CAROL MOSELEY-BRAUN, Illinois

ORRIN G. HATCH, Utah
STROM THURMOND, South Carolina
ALAN K. SIMPSON, Wyoming
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
HANK BROWN, Colorado
WILLIAM S. COHEN, Maine
LARRY PRESSLER, South Dakota

CYNTHIA C. HOGAN, *Chief Counsel*
CATHERINE M. RUSSELL, *Staff Director*
SHARON PROST, *Minority Chief Counsel*
MARK R. DISLER, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

PATRICK J. LEAHY, Vermont, *Chairman*

HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California

ARLEN SPECTER, Pennsylvania
LARRY PRESSLER, South Dakota

ANN HARKINS, *Chief Counsel*
RICHARD HERTLING, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

WEDNESDAY, OCTOBER 27, 1993

THURSDAY, JANUARY 27, 1994

ALPHABETICAL LIST AND MATERIAL SUBMITTED

APPENDIX

ADDITIONAL SUBMISSIONS FOR THE RECORD

HIGH-TECH PRIVACY ISSUES IN HEALTH CARE

WEDNESDAY, OCTOBER 27, 1993

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:00 a.m., in room SR–328A, Russell Senate Office Building, Hon. Patrick J. Leahy, chairman of the subcommittee, presiding.

Also present: Senator Specter.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Good morning. I am Patrick Leahy. I am the Chairman of the Technology and the Law Subcommittee of the Senate Judiciary Committee.

We know that reform of the health care system in America is a priority, both for the Congress and for the President. In fact, the President will outline his plan later this morning. But reform requires cost containment and reduction of administrative overhead without sacrificing the quality health care Americans demand and deserve.

I found it interesting that one of the newest technologies that has been developed to streamline the system and expedite patient care is a health data card. This is what it can do: You can take a patient's entire medical history, compress it onto one card that is about the size of your average credit card. My wife is a nurse and I know what the files generally look like in the hospital—about yea big. Any time any one of us go in for our own medical checkups, our doctors see these records. But these records are something that actually could be carried around very, very easily, and I think the health data card has great potential for the health care system.

The health data card also has built-in features to enhance the privacy of our personal health information. None of us wants to think that everything about us, probably from childhood to the current time, could be put on one credit card-sized information package that is also available to our neighbors or to our employers or to anybody who really has no need to know what is on there. Federal law has to keep pace with this new technology in protecting the privacy of the intimate details of our medical records.

So this hearing will be a first step in formulating a comprehensive Federal law for the privacy and the confidentiality and security of our medical records. I truly believe that instead of having

large files with information about your medical conditions that will follow you around in the near future we will all have a card that will contain all the information. But I do not want to see a situation where my neighbor or your neighbor, my employer or your employer or anybody, who just has a prurient interest, is able to go into your card, my card, or anybody else's. In my work on the Electronic Communications Privacy Act of 1986, and other privacy legislation, I have seen American companies learn that protection of individual privacy is just good business. Recent surveys confirm that protection of privacy is important to the public. Privacy has to be the cornerstone of health care reform.

Without assurance to the American people of adequate safeguards to protect the privacy, the security and the confidentiality of their medical information, the public is going to resist healthcare reforms that call for increased government involvement or increased use of high technology. We know that the high technology is there; we know that we have a nationwide health care plan that calls for increased Government involvement.

But I know very much that most people feel, as we do in Vermont, that we must protect our privacy. We cherish our privacy. The high-technology devices that are available to us in the medical field will be resisted by the public unless we can guarantee that the privacy of individual patients will be protected.

So I think we are fortunate in the people we have here today. We have Sherman Hope from the Brownfield Rural Health Clinic in Brownfield, TX. The doctor has been a great innovator in the field of keeping computerized medical records, and he will start off the testimony. Dr. Hope will be followed by Richard Haddock, who is the president of the LaserCard Systems Corporation of Mountain View, CA. He, in fact, just showed me a very quick overview of some of the things he is able to do with the laser optical care technology.

I feel as I always do when my youngsters or their friends come in and explain how we do things and how we store things on computers. They try their best to teach me. They have gotten up to the point where I know how to turn the VCR on and off and even knew how to stop it from blinking "12, 12, 12, 12" all day.

[Laughter.]

[The Prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

President Clinton's Health Security Act takes bold steps in reforming our health care system and the President has actively engaged Congress and the American people in this discussion.

Hardly a day goes by without the latest turn in this debate being reported in our local and national press. Such terms as cost containment, portability and universal coverage are the focus of much of this debate, but there is a great deal more to the comprehensive plan put forward by the President.

Today, we will discuss one aspect of the Health Security Act that goes beyond the new health care jargon and affects each of us in a very personal way—a national computerized health care network that will hold basic information on each of us. My concern and the focus of this hearing is safeguarding the personal privacy of all Americans with regard to their medical care.

The legislation pending before Congress uses technology aggressively to achieve the savings necessary for delivery of health care to all Americans. This Act builds upon piecemeal efforts already going on across the country and envisions medical information flowing across a network from the health care provider to the alliances

that each state will be required to create, to a regional center, and on to a National Health Board.

The days are gone when, after a visit to your doctor, medical records were locked away in the office, our privacy protected. Personal information is now disseminated to insurance companies, third-party payors, and clearinghouses. Today, this very personal medical information is even sold for marketing purposes to commercial firms.

No longer can the focus of security be on the actual location where the record is made. We must be concerned about private information itself, wherever it may go. With or without health care reform, and I believe that the President has made a compelling case for why reform is needed, we want to regain control of our personal medical information. Others should not have access to it without our knowledge and consent.

Today, we will hear from Congresswoman Nydia Velazquez about the trauma of having personal medical information disclosed publicly. Hers is a compelling case but, unfortunately, not an isolated one. I spoke with Jeanne Ashe a few weeks ago on this subject. In his autobiography, *Days of Grace,* Arthur Ashe wrote about how he and his wife Jeanne learned in 1988 that he had contracted AIDS during a heart operation. Arthur Ashe was not only a great athlete, activist and scholar, but a husband, father and private individual. Tragically he was forced to live his remaining days in the glare of public knowledge of his battle with AIDS. In his case, he was forced to confirm his condition after the press got a tip about his medical condition. His family is still feeling the effects of this intrusion into their privacy.

I am sure you will understand that even now, almost a year after Arthur Ashe's death, his wife wished to maintain the privacy she has left and has chosen not to appear at this time. Our thoughts are with her and her daughter. We should learn from their experience so that no one else need bear the intrusion they have had to suffer to their privacy in addition to illness and great loss.

The Administration has recognized in the Health Security Act that "health security" not only requires universal coverage but also assurances that personal health information will be kept private and secure from unauthorized disclosure.

I know that in my own state of Vermont, efforts are already underway to develop a modern, integrated health care information system that is community-based and community-run. The Vermont Health Information Consortium (VHIC), working closely with the Vermont Health Care Authority, is developing confidentiality, privacy and security standards for this system.

Past experience might have given Vermonters reason to resist the computerization and dissemination of records. It was two years ago that—in error—nearly every property owner in the town of Norwich was listed by one of the nation's largest credit reporting agencies as delinquent in their taxes. But rather than be deterred by past pitfalls, my state as been encouraged by the promise of emerging technologies.

At the last hearing of the Subcommittee on October 26, we saw demonstrations of some of the new technologies being used in health care. It is now possible to carry our entire medical history, including health and psychological profiles, blood tests, x-rays, and family medical histories, on a piece of plastic the size of a credit card. Without the proper security features, however, anyone with the right machinery could take the card and look at that information.

The same problem exists with computerized medical information. Without the proper safeguards, anyone hooked up to the computer where our medical records are on-line, could look at the intimate details of our personal medical history. If the computer is on a network, access to our medical information is multiplied exponentially. There is no doubt that the increased computerization of medical information has raised the stakes in privacy protection.

New technologies have the capability of enhancing the privacy of personal health data, however. In fact, in many ways, technology can provide better protection than paper records. In order to take full advantage of the privacy and security features technology has to offer, we should address questions of who should have access to personal medical information and the appropriate safeguards and we should do so now, in advance of implementation. Then, as the information systems contemplated in the Health Security Act and in states like Vermont take shape, the computer programmers can work with clear privacy and security directives set forth in law.

The American public cares very much about protecting its privacy. As policymakers, we must remember that the right of privacy is one of our most cherished freedoms. It is the right to be left alone and to choose what we will reveal of ourselves and what we will keep from others.

The Administration's health care reform proposal provides that privacy and security guidelines will be required for health data cards and computerized medical records to assure the public that their privacy will be protected. I look forward to

hearing from the witnesses from the Department of Health and Human Services, the American Hospital Association and the ACLU about the adequacy of those privacy and security provisions.

Senator LEAHY. Dr. Hope, why don't we start with you, sir.

PANEL CONSISTING OF SHERMAN HOPE, M.D., BROWNFIELD RURAL HEALTH CLINIC, BROWNFIELD, TX; ACCOMPANIED BY RICHARD HOPE, M.D.; AND RICHARD HADDOCK, PRESIDENT, LASERCARD SYSTEMS CORPORATION, MOUNTAIN VIEW, CA

STATEMENT OF SHERMAN HOPE

Dr. SHERMAN HOPE. Thank you, Senator.

As you mentioned, I am at this hearing to enumerate some experience I have had with computerized medical records. I am a practicing physician. I have been in Brownfield, TX, practicing family practice for approximately 32 years. I am from Lubbock, TX, born there. My son, Richard, has done like you were talking about, has taught me about computers, and he is a practicing physician in a little town called Little Rock, AR. I think most of us have heard of it.

Senator LEAHY. We are all required now to be able to spot it instantaneously on a map.

Dr. SHERMAN HOPE. Instantaneously. Even tell what State it is in. [Laughter.]

Senator LEAHY. That is right.

Dr. SHERMAN HOPE. Brownfield, TX is a city of approximately 9,000 people. We have a 5-county medical society composed of 17 doctors. In this area, we have 57,000 people that we are taking care of. This figures out to be 1 doctor per 3,366 patients. I think I have got twice that many. This is 1 doctor per 300-square miles of area.

With these capabilities, necessity is the mother of invention. Because of our patient load, we felt like we needed to do something to help expedite and improve the medical care in our area and for our patients. I have 7,006 patients on the computer as of Saturday morning. This figures out to be 16 percent Medicare patients, 52 percent Medicaid patients, 31 percent private insurance and private pay. It is obvious that the Government is strongly involved in the financial survivability of my practice.

Taking advantage of the Rural Health Clinic clause, I established one of the first 10 rural health clinics in Texas approximately 3 years ago. This enabled me to utilize the services of a physician assistant to see patients, and our average patient load last year was 54 patients a day.

Now, if you are going to see that many patients, you have certainly got to do something to improve the efficiency, and we chose to computerize our medical records. The medical records are sort of the doctor's heartbeat. They are his lifeblood in his office. It is your medical records that will help keep you out of malpractice trouble. It is your medical records that will determine whether Medicaid, Medicare, private insurance is going to pay. The old adage, if you do not document it, you did not do it, certainly applies, and most of the doctors' handwriting is known for its hieroglyphic type of things that even I cannot figure out an hour later.

Computerized medical records seemed to be the answer. So with the aid of my son as the computer expert, and he can also work a VCR and a few things like that, we undertook to set up a program, develop a program for computerized records, and I have been using such a program in my office for 7 years. So we were ahead of the game before there were virtually any other medical records systems available.

As you mentioned, there are medical records for computerization that involve several different concepts. You can have a total record from birth certificate to death certificate on there. You can have records that are totally stored on the computers. You can have your computers that will basically organize and continue to print out hard copies of your records, and anything in between.

Because of the cost and capabilities and not wanting to change things from the way doctors usually do, we developed a system which actually prints out a hard copy, although we can maintain total electronic storage if desired, utilizing the power of the computer not just for electronic storage, but instead trying to utilize the power of the computer to actually improve the patient care.

For example, automatic drug interaction checks, side effects, health maintenance, patient recall, all kinds of capabilities along that line. We developed what we call the SOAP system. SOAP is an acronym standing for what doctors are supposed to keep their medical records: subjective, what the patient complains of; objective, what the doctors sees, x-rays, et cetera; assessment, what is the matter with the patient, what you are going to do with him, prescription, put him in the hospital, surgery, what-have-you; and plan, how you are going to take care of the problems.

[Dr. Sherman Hope submitted the following:]

PREPARED STATEMENT OF SHERMAN A. HOPE, M.D., ON BEHALF OF THE BROWNFIELD RURAL HEALTH CLINIC

The medical profession, working with our elected governmental leadership, is challenged with the responsibility of providing medical care to all citizens of our nation. This must be done in an efficient and cost effective manner by building on the experience and structure of our current medical delivery system. High quality and compassionate care available to every individual should be the goal. This medical care should not be denied to those in need because of circumstance, whether financial or geographic.

BIOGRAPHICAL INFORMATION

I am Sherman A. Hope, M.D., a 61 year old family practitioner from Brownfield, TX. I was born in Lubbock, TX, and graduated from Baylor University (pre-medical education) and from the University of Oklahoma School of Medicine in 1957. I served three years in the United States Air Force, where I was a flight surgeon. I have been engaged in family practice in Brownfield for 32 years, doing "small town family practice," i.e. doing surgery, delivering babies, and caring for a full range of patients, treating them for everything from arthritis to zoster. I am a Fellow of the American Academy of Family Practice and a Diplomat of the American Board of Family Practice. I have been certified and recertified by this board. My wife and I have raised seven children and have been active in our community and church.

Richard Hope, M.D., was born in Brownfield, TX. He graduated from Angelo State University with a Bachelor or Science degree in computer science. He obtained his medical degree from the University Health Science Center at San Antonio. He is currently working in the University Hospital, University of Arkansas Medical School, in Little Rock, AR. (I'm sure most of you know where that is and know at least two famous people from there.) Richard and his wife have two children. Dr. Richard Hope is the "computer expert" and is with me today to answer any technical computer questions you may have.

PRACTICE DESCRIPTION

I began practicing medicine in Brownfield, TX, in 1961, after three years in the Air Force. After ten years of practice, I constructed my medical clinic building which contains a laboratory and x-ray facilities. I have recruited other physicians for Brownfield and this clinic, and we practice in this facility. I am currently active in practice.

Taking advantage of the Federal Rural Health Clinic legislation, I established a rural health clinic (one of the first ten in Texas) in 1990. Our computer read-out shows that as of the end of this week that I have an active patient population of 7006. These patients are served by myself and by a physician assistant who began work here when the rural health opened. During the past year we have had 13,546 patient visits, an average of 54 patients per day. The breakdown of patient types is as follows: Medicare 16 percent, Medicaid 53 percent, and private pay 31 percent. It is obvious from these statistics that the federal government is strongly involved in the financial viability of my practice. We are currently serving the medical needs of pediatric and adult patients in our community, with referral services for obstetrics and surgical needs. We furnish care at the two local nursing homes and provide hospital care for our patients in the Brownfield Regional Medical Center (our local 50 bed hospital). Complicated cases are referred to secondary and tertiary medical facilities in Lubbock.

DEMOGRAPHICS OF MEDICAL CARE IN THE BROWNFIELD AREA

Brownfield, TX (population 9,560) is located in the Texas Panhandle, 45 miles south of Lubbock, TX, and 40 miles from the New Mexico state line. It is a rural community with the economy depending approximately 80 percent on agriculture and 20 percent on oil and other business. It is the county seat of Terry County (population 13,218). Our local Medical Society is composed of five counties (Dawson, Gaines, Lynn, Terry, and Yoakum). The total population of this area is 57,234, with an area of 4,979 square miles. This area has a total of 17 practicing physicians or *1 physician for every 3.366 persons, or 1 physician for every 293 square miles.* The nearest "metropolitan center" is Lubbock, TX, (population approx. 200,000). The referral hospitals in Lubbock are Methodist Hospital (patient bed capacity of 900). University of Texas Tech Medical School Hospital (patient bed capacity of 300), and St. Mary's Hospital (patient bed capacity of 422).

COMPUTERIZATION OF MEDICAL RECORDS

In order to meet the medical needs of this population, it became apparent that I needed to develop the capabilities of serving patients more efficiently. With the constant threat of malpractice suits and "non pay" by Medicare, Medicaid, and private insurance companies (if the medical records didn't reflect quality medical care and "prove we did it"), it became apparent that we must improve on our medical record system. The use or a "computerized medical record system" was the logical solution. We (Richard and myself) instituted the development of a computerized patient record medical system which we refer to as the "S–O–A–P System." The acronym S–O–A–P it derived from the current medical terminology and methodology of keeping records.

"S" stands for Subjective (the patient's complaints).
"O" stands for Objective (the physician's finding upon examination, laboratory, x-ray, etc.).
"A" stands for Assessment (evaluations and diagnosis).
"P" stands for Plan (what you undertake to do for the patient).

Using our computerized medical record system, we were able to increase our patient load and markedly increase the efficiency in our office.

Computerized medical records are a new concept in physicians' offices. Although 50 percent to 60 percent of physician' offices currently are using a computer for the purpose of billing, scheduling, and submitting insurance claims, less than 1 percent of physicians are using computers for patient care. Even a smaller percentage are utilizing computers for maintaining patients' charts.

Computerized medical record systems that are available currently can be divided into two classes.

1) The first class is those which do total electronic storage, requiring typing of the progress notes directly into the computer by the physician, nurse, or transcriptionist. This also requires scanning of laboratory reports, x-ray reports, permission slips, consultation reports, etc., into the patient's computer record. Of course, if the computer is "down" at any particular time, patient visita and treat-

ments may come to a screeching halt. Currently these systems require a significant amount of computer expertise by the user. They usually do not print out "hard copies" of the record except by special request. Currently they require more expensive computers and support.

2) The second type of computer programs for computerization of patient charts (medical records) utilized the chart system currently used by 99 percent of physicians and clinics. This usually creates a "hard copy" of the information of the patient visit. It takes advantage of the power of computers to organize and clarify the records and assist in patient care. Better care is rendered because the computer automatically flags drug interactions and warns immediately of potential drug allergies or adverse effect with certain diseases. Automatic prescription writing and patient recall abilities by diagnosis, age, diseases, drug usage, etc., are important features. Utilizing the computerized record system has enabled me to get the maximum use of my "physician expander," i.e. my physician assistant. His supervision is enhanced by my ability to check his prescriptions, diagnoses, and records, using the computer.

Other advantages of the computer are discussed in the attached "S–O–A–P Mini Manual." Please refer to this literature for more specific information.

ECONOMICS OF COMPUTERIZATION

Economics of computerization must be taken into consideration, especially by private physicians with no special funding for such projects. The S–O–A–P System was specifically designed to operate on the *least expensive, most readily available computers* in existence. With the exception of the ChartCard reader/writer, S–O–A–P operates with equipment available in any standard computer supply store. It requires no special installation and is not written in a special language. If a physician, clinic, hospital, or the government is considering the use of computers for patient records, it is *absolutely necessary to keep the cost down* by using currently available equipment and programs and avoid "reinventing the wheel." The medical profession needs to begin where technology is now and not wait until the "ultimate systems" is developed. Men didn't wait on the jet air liner before we started to fly, we began with the bi-plane.

In our clinic we chose to utilize the second concept in developing a medical record system. I have chosen to illustrate our medical records by including actual copies of the charts of the patients that I treated recently in a one day period. These records were generated by the S–O–A–P System and required no secretarial help.

PATIENT PROFILES

The heart of any medical record system is creation of a patient database, which the S–O–A–P System calls the "Patient Profile." S–O–A–P's patient profile contains basic information that any physician *should have immediately available* when treating any patient For any condition. This includes: demographics (name, address, phone, spouse, insurance, etc.), acute illness (diagnosis, date, and doctor of last two visits), chronic disease list, drug list (including dosage and directions), conditions affecting drugs (sex, smoking, allergies, etc.), major procedure, hospitalizations, and surgeries, health maintenance information (including lab, and immunizations), and brief significant family history.

Since an outdated data base is essentially useless and occasionally even dangerous, the data base or the S–O–A–P System is updated with each patient encounter. By utilizing the power of the computer, drugs are checked for interactions and side effects. The problem list of diseases is checked for drug cautions and warnings, and drug allergies are checked. This is all done on a "real time basis," while the patient is in the examining room and *before* the prescription is written.

USING THE COMPUTERIZED MEDICAL RECORDS SYSTEM

I make extensive use of our computerized medical records in patient care. A computer terminal is turned on in each examining room in order that the patients may review his/her medical profile as displayed on the screen. Working with the nurse or physician the patients update their own data. I use the system to write prescriptions and this information is automatically transferred back to the patient's chart (providing more accuracy).

I use the computer for patient health maintenance. Health maintenance and disease prevention is a very important feature of family practice. The S–O–A–P system has two concepts in health maintenance.

First, consider the individual. For a particular patient, using a single key stroke triggers S–O–A–P to search the profile of that patient and displays on the screen

(or prints out) the status of health maintenance recommendations. Not only are such routines as regular pap smears, mammograms, blood pressure checks, cholesterol checks, etc., included, but S–O–A–P also takes into account the patient's special situations, such as family history (example: cancer of the breast) or place of residence or occupation (examples: a patient living in an institutional setting needing a flu vaccine or a coal miner needing a chest x-ray). Information obtained will tell what procedure is needed, how often, and the date the procedure was last done, flagging in color if delinquent. Although the criteria for health maintenance procedures are taken from recommendations of recognized authorities such as the American Heart Association, American Cancer Society, American Academy of Family Practice, etc., the physician may modify these criteria to fit his/her practice.

The second health maintenance responsibility of the physician is to his practice in general. In using this computerized system, I am able to recall patients for procedures that need to be done. We send reminders for annual physicals, pap smears, immunizations. etc. In addition to routine reminders, I hold screening clinics in my office. I will use the computer to recall patients with certain conditions that need to be followed carefully. For example, I will have an ophthalmologist come from Lubbock, TX, (the nearest ophthalmologist), and check my diabetic patients for diabetic retinopathy. This is practical because of the power of the computer to search the profile of over 7000 patients and identify those with diabetes. It then prints address labels for them in only a few minutes. I use this same concept in screening for kidney disease, peripheral vascular disease, etc., for hypertensive patients, cardiovascular patients, and other groups. We have screening clinics for skin cancer with dermatologists coming to the clinic, and utilizing the computer to call patients in by age. *Preventive care is cheaper* than treatment of the complications after they have occurred.

Patient education is a major function of primary care, especially in chronic illnesses and diseases of the aged. Our computer system allows us to print out educational material which is customized for individual patients.

PHYSICIAN INFORMATION EXCHANGE; CHARTCARDS—SMART CARDS

No single physician can fulfill all of the needs of all of his patients; therefore, we have a developed network of physicians to whom we refer. All physicians must do the same. To some physicians this may be a more formal arrangement such as an HMO or PPO. We use our computerized medical record system to support this referral process. Not only do we print the patient profile, but we also print a list of all previous visits (with date, doctor, and diagnosis) and previously prescribed medications. This may be mailed or hand carried by the physician to the next provider (hospital or doctor).

However, the S–O–A–P Medical Record System furnishes the capability of creating a *portable medical record* for the patient. This technique involves the use of "smart cards." Utilizing an imbedded computer chip in a credit card size plastic card, S–O–A–P copies she most current "Patient Profile" onto his "ChartCard" (our trade name for the smart card). This card, which looks like a credit card, contains the patient's medical information. On each visit to his physician, this card is updated at the end of the office visit simply by inserting it into the ChartCard reader/writer of the computer. When the patient goes to another physician, emergency room, hospital, etc., the patient furnishes them with his ChartCard. This is inserted into their card reader/writer, and the new provider has the most current medical information on this patient. After this institution or doctor treats the patient, prescribes medications, etc., the ChartCard is updated via the computer and returned to the patient to take to the original physician. In this manner, each medical provider has the latest information on the status of the patient.

The S–O–A–P System is unique in that it contains the basic medical data of the patient needed by a treating physician to take care of the patient in a new encounter (the "Patient Profile"). All of this necessary information is *displayed on one computer screen.* There is no need to "page through" multiple screens to get the information.

Using the ChartChard eliminates each provider's having to "start a new medical record, fill out forms, etc." The ChartCard does this for him. These cards are especially useful in HMOs, PPOs, hospital-physician networks, medical area networks, and hospital-physician marketing. Those ChartCards can be customized as needed by a particular institution or provider. They may have bar coding strips and magnetic strips for identification and financial information (such as insurance companies, policy numbers, etc.) and may even carry the patient's picture for identification.

These ChartCards are a new concept in the transferring of medical records and have the potential of time-saving, accuracy, and cost efficiency for doctors. They will save money in eliminating duplication of clerical work, helping to reduce unnecessary duplication of laboratory and x-ray work, and in helping to eliminate prescribing of duplicate medication by different physicians, etc. From a patient acceptance standpoint, the ChartCard will help eliminate some of the major complaints that the public has against medical care facilities. The first complaint is cost of care; the second is lengthy waiting time in care facilities; and finally the resentment at having to repeatedly fill out medical information questionnaires at each point of delivery of services.

PATIENT'S PRIVACY AND CONFIDENTIALITY OF MEDICAL RECORDS

Confidentiality of the information used by computerized medical records poses virtually the same problems that arise when not using computers to maintain the patient's medical records. Obviously, it depends upon the integrity of the physician and the people under his supervision who are entrusted with creating and distributing of the medical records. Because of the computer's ability to "lock out or grant access" information to particular individuals, medical confidentiality on computers is probably better than that usually experienced in todays medical environment.

Security under the S–O–A–P Patient Medical Record System is built into the program. Currently there are five levels of security. When the program is installed in any institution, the director, or supervisor of that institution may set the access levels according to the direction of the supervisor and needs of the individual computer user. The highest access level is for the general supervisor (which usually would be the physician in charge of that clinic). The second level allows the nurses and the doctors to enter information onto the patient's medical record (such as writing prescriptions, updating the problem list, adding drugs, etc.) The third access level allows the receptionist to transcribe information and take dictation using the program but would prohibit her from modifying the patient's profile or changing drugs. The fourth level allows "viewing only" of the patient's records (for such people as insurance clerks which may want to get a diagnoses). A fifth level allows a pharmacist to enter data into the drug data base but not to view patient records or modify the patient's chart. All of these levels require the user to "sign on" using a pass words and to type in the user's ID number.

Most of the S–O–A–P Systems utilized in larger clinica would be on a computer network. These computer networks also contain a security system requiring "login" and "logout" capabilities with certain levels of access allowed.

As mentioned previously, I try to assure the accuracy of the patient's medical records by having the computer turned on in the examining room. The patient will read his own chart and tell me if the information is correct. He will also inform me if there is information that he does not wish to have recorded on his record. (This could be information such as AIDS, or taking the drug AZT, etc.) In this manner, the chart printout as well as the ChartCard information which is taken from this patient profile and will be suitable to the patient. The ChartCard has the same information as the patient profile (that the patient will have reviewed with the doctor). This allows the patient to eliminate diagnoses that he does not want maintained in his records, such as alcoholism, AIDS, or other information that he might feel he would not want other people to know. Unfortunately, when the patient begins to select what he wants physicians to know and not know, the accuracy of the medical information on the chart will decrease. This is nothing new. Patients withhold information frequently, especially when they are seeing another doctor for a particular condition or that they have taken some of Grandma's pills for their arthritis and they really do not want to tell me.

The information placed in the computerized "patient profile" and subsequently onto the ChartCard, would be akin to what the patients have in a written record. The patient has a choice of either furnishing or refusing to furnish his card (or written chart) to another institution, including medical institution, prospective employer, or insurance company. There is an additional benefit to these institutions in using the ChartCard. The identification capabilities of the ChartCard can confirm that the card carrier is indeed the correct person to receive the medical care, employment, or insurance.

In summary, the computerization of medical records has been a necessary endeavor for my office. Although it was a major effort, it has provided valuable dividends through better patient care, enhanced accuracy of the medical records, and efficiency of office personnel. I have found that my office personnel take pride in their new computer skills, and the economics of practicing in this manner justified the efforts to computerize my medical records. Thank you.

SHERMAN A. HOPE, M.D.,
BROWNFIELD RURAL HEALTH CLINIC,
Brownfield, TX, January 11, 1993.

Hon. PATRICK J. LEAHY,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY: I am responding to the questions posed in your letter of December 28, 1993, about our computerized medical record program called the S–O–A–P Patient Medical Record System and its ChartCard capabilities. ChartCard is our trade name for a portable medical record health card that can be carried by the patient on either the smart cards or laser cards. I hope my answers are clear; and if you have any questions, feel free to have your office call me for further clarification.

I hope these answers have satisfied your questions and feel free to call me if I can furnish further information.

I would like to take this opportunity to offer to you, for your personal physician and your mother's physician, our S–O–A–P Medical Record System. Simply have your office contact me, and we will be glad to send it to your office or directly to them. There would be no charge for this service. It would be our honor to provide this for you.

I wish to thank you for the opportunity to express my views and to demonstrate our system to your committee. Give my regards to your staff, who have been very cordial and helpful. I wish the best for you, your family and staff this coming year.

Yours truly,

SHERMAN A. HOPE, M.D.,
Family Practice.

SHERMAN A. HOPE'S RESPONSE TO QUESTIONS SUBMITTED BY SENATOR LEAHY

Question 1. What privacy and security guidelines do you think should be required for health data cards and computerized medical records to assure the public that their privacy will be protected?

Answer. The health data cards are actually a copy of data generated from the computerized medical records. Therefore, the security that should be required should reside in the medical record system. The medical record system should have "built in security" that would require proper identification and authorization of any person using the card reader. The computerized medical record system should have levels of authorization and the ability to shield certain fields so that privileged information can be either concealed or revealed to the reader according to his predetermined authorization. I would avoid writing specifics into laws which define what fields of information are to be shielded and who would be authorized to use the medical record system. Leave it up to the vendors, users, and the medical legal personnel to develop specifics according to the needs of that particular application program. The emphasis of the law should be aimed at individuals who are not authorized to have the information on medical records. The law should define abuse and set defined punishments for those persons. I do not think that laws placing undue responsibility for information security on the industry will help very much. No matter how well the medical record program is designed in today's technology, tomorrow someone will find a way to "crack the code," and if there are not specific laws prohibiting them from pirating medical information and illegally using this information, there will be problems.

Question 1. If the smart card you demonstrated at the hearing is lost or stolen, the patient's medical information can be retrieved from a database and put on a replacement card. Does the use of these cards rely on the storage of the medical information in a central database?

Answer. Since the card is really just an electronic picture of the database generated by a computerized medical record system, the basic data on this patient will reside in a medical database. That medical database may be as limited as a single physician's office or as extensive as an area network such as a hospital, HMO group, or limited geographical area. The larger the database, the more subject to misuse; therefore, I would propose keeping the databases in relatively small units limited to geographical and provider groups. I see no need medically for a national medical database. Assuming a "health card" system was in place, each person could carry his medical data with him.

A second part of this question has to do with features of the actual card. These cards can be developed to provide patient identification, utilizing pictures, finger-

prints or other methods. They can be produced in such a way that they could not be read except by an "authorized" card reader. For example, an "authorized" card reader would be in place in the emergency room; but if a health insurance company wanted to scan people's health cards, it would not have an "authorized" reader, even if it purchased the medical record system and a generic reader.

Question 3. Have you developed any technological features that protect the privacy and security of such a central database of medical records?

Answer. On the S–O–A–P System we currently have five levels of access. The clinic director assigns privileges, with a particular level assigned to personnel according to their need for patient medical information. For example, the physicians are allowed the entire medical records; and they may change data, write prescriptions, etc. (all of which is transferred to the health card); whereas, a secretary can only read the patient's profile but cannot change drugs and diagnostic information. However, she can type the clinical notes into the patients' medical records. In contrast, the pharmacist can not review a patient's medical history but can change drug database information. Virtually any level of access can easily be built into the medical record system simply by defining the needs and functions of the medical personnel and allowing them access capabilities according to their job description. In addition to the medical record system having levels of access, the Novell network system, under which the S–O–A–P System operates also has security and access features; therefore, requiring the user to "login" through two security systems. This "login" feature creates a "tracking" system to see who had access to medical information and when.

Question 4. Would you have any concern over your ability to protect the privacy of your patient's records if your computerized medical records were connected in a network with other doctors' or hospitals' medical records?

Answer. Yes, I would have an adverse feeling about leaving a modem running on my computer allowing virtually anyone at another institution to access the medical records out of my office. I feel the concept of using smart cards or ChartCards alleviates this problem because it provides for the patient to carry his own medical records with him and give them to whomever he wants. A national database is great for research and statistical uses but I would question as to whether it would be applicable to local real life practice situations. Both physicians and patients are likely to be very resistant to transfer of privileged information to the safe keeping of large governmental bodies.

Questions 5. So-called computer viruses are a damaging nuisance about which everybody with a computer worries. Can computer viruses destroy information on health data cards?

Could a computer hacker or a virus be able to alter information on a central database of health records and, for example, make every AIDS test result a positive?

Answer. To date there have been no reported cases of viruses infecting medical software or medical computers. However, just as adding new programs via disk or electronic transfer may infect a computer or program, it is certainly possible that a hacker could cause problems with medical records. This problem can be solved in our system by maintaining a printout on each patient's record, usually with each visit. If a medical record system relies totally on electronic storage, it is much more vulnerable to serious alteration of the medical records. Perhaps all medical record systems need a requirement of hard copy printouts, or at least extensive, secure back-up procedures. I do not see a way that a computer hacker could access local health databases such as physicians' offices, local hospitals, HMO's, etc., and change fields arbitrarily in a computerized medical system. Of course, the ingenuity of the computer hackers is not to be denied, and I envision that such an event could happen. The larger the database and the more users that are connected, the more likely problems could develop, especially in large databases that are connected from institution to institution.

Senator LEAHY. Who has access to that?

Dr. SHERMAN HOPE. Who have access to it?

Senator LEAHY. Yes, to the records you keep.

Dr. SHERMAN HOPE. The records I keep are accessed by myself and my office staff.

Senator LEAHY. And that is it?

Dr. SHERMAN HOPE. Yes, sir.

Senator LEAHY. But if you had a patient, who was traveling away from Texas to my own State of Vermont, are you able to, are

you, to transmit any of those records, if you wanted to, to somebody with a compatible computer?

Dr. SHERMAN HOPE. Yes, sir. There are two methodologies. Obviously, one is a modem, but the most popular one, as you mentioned, is the use of a card and the card is designed to display what we refer to as the patient profile, which is the basic medical needs that the doctor must have each time he sees a patient.

Senator LEAHY. So the patient would have that and you would have access to it?

Dr. SHERMAN HOPE. Yes, sir.

Senator LEAHY. The patient would have access to it because he would have the card with him?

Dr. SHERMAN HOPE. Right.

Senator LEAHY. But nobody else could go in and just pick that up?

Dr. SHERMAN HOPE. No, sir.

Senator LEAHY. If we started using cards as a common thing, would you feel that we should have something built in so that employers or others could not have a right to just arbitrarily ask employees to see their card, to access it, to go through the material?

Dr. SHERMAN HOPE. To run into the same situation as we currently have in medical records, if a patient has information that he does not want other people to know, he may request that it be kept off of his written records. Certainly he could keep it off of his computer records in the same manner.

Senator LEAHY. Or you could set up a separate file. You could have different levels of access on your card if you wanted to, too, couldn't you? I mean, keep the information on the card but with different levels of access?

Dr. SHERMAN HOPE. That is correct. And we currently do that. For example, only certain levels of access, the doctor can see the patient's record and change, say write a prescription. In contrast, the insurance clerk can only read the patient's record.

Senator LEAHY. I wonder if your son could demonstrate some of how that works.

Dr. RICHARD HOPE. On this card right here, we have a sample patient. This was as if you came into the physician's office, your family practitioner referred you to the neurologist or something, and you just plug this little card into the reader and just view the information from this card.

Here are the basic demographics and the drugs, allergies, which is very important, and the diseases and problem list on this patient. You get all this information from the card.

Any information can be changed on here. You make your diagnosis, write your prescriptions for the patient, put it back on the card, and the next day the patient may go back to his family practitioner and the family practitioner then has an updated record.

Senator LEAHY. I would note in case the screen is being picked up on the camera, that the addresses and other information on the screen are obviously for a fictitious case?

Dr. RICHARD HOPE. All of our patients are fictitious, right.

Senator LEAHY. I see various telephone numbers and zip codes and so on. Just in case anybody's trying to read just what this poor person is suffering from, it is not a real person.

Dr. RICHARD HOPE. Right. I think that is one of the main advantages of the card, is that you have at least a summary of the information that any physician of any specialty needs to treat that patient for any particular visit, and this can certainly be expanded to keep more detailed records on the card and levels of access are built in into this card and they can be built into other cards and other systems.

But yes, this information can certainly be sensitive and as we put information on the card, the patient has the opportunity to view the information that is being put on the card, and he can request that information not be put on there.

Senator LEAHY. I would think on that, you've got something that, particularly from the emergency room basis, you have immediately what drug allergies——

Dr. RICHARD HOPE. Very important information.

Senator LEAHY. And problem lists of things of this nature.

Dr. RICHARD HOPE. Just last year I was actually working in an emergency room in Little Rock, and if we had a list of the patients' medicines when they came in unconscious, their diseases and their drug allergies, it would certainly be of benefit a lot.

Senator LEAHY. How much information beyond the detail you have on the screen, can you put on the card?

Dr. RICHARD HOPE. On our current system right now, we can store 2,000 bytes of information, which is our basic profile. That is certainly expandable to store it on other types of cards, other types of media, with minimal modification of the program. And, again, you can build in all the levels of access that we currently have in the program and any more with minimal effort.

I think one of the key points we are getting is that this is something that is realtime, that we are already using, and it is currently already developed, that can potentially be used by other physicians at this time that will help with the medical care of patients in general.

Senator LEAHY. All right. And that also would be information that you could transmit to somebody else quickly and easily?

Dr. RICHARD HOPE. Yes, sir.

Senator LEAHY. Or you could print a hard copy of what you had there, too?

Dr. RICHARD HOPE. Yes, sir. You can print hard copies or transfer it over a modem to other physicians, if so desired.

Senator LEAHY. Do either one of you have much experience with people asking just to see their records, then, if they have got one of these cards? Or do they sort of feel, well, OK, if the doctor put it in, it must be right?

Dr. SHERMAN HOPE. In my office, I have a computer terminal in each examining room and while the nurse is getting the patient ready for examination, she calls the medical record up on the computer. The patient will sit there on the examining table and actually read their own record, and they will say, "Well, I'm not taking this drug," or, "I saw Dr. Jones and he told me I had rheumatoid arthritis, so take off that other diagnosis." So they actually read their own records almost routinely.

Senator LEAHY. We had a situation in the IRS that came to light a few months ago, where a number of IRS employees were pulling

up the files of celebrities, movie stars, well-known people, and so forth, and going through them just for the fun of it to see what they invested, how much they really made last year, and so on and so forth.

Now, suppose you had somebody working at your clinic and he was thinking of buying stock in a particular company and knew the president of that company or the chief designer of that company was a patient. Is there anything to stop the clinic employee from saying, "Gee, I would just kind of like to see if he or she is going to be around 2 years from now before I buy the stock," or, "I am just curious if they really are that healthy. They look to me like somebody who might have had some problems with depression or something else like that in the past."

Is there anything to stop a person with access to the medical records from just saying, "I will just pull the record up and take a look at it"?

Dr. SHERMAN HOPE. Well, if you give access to the proper people as you install the program, for example the physicians, there would be nothing to keep a physician from doing such a thing. But there is nothing to keep in our current system from doing that, also. So no, I don't know how you would stop them if they have access to the patient's medical information.

Senator LEAHY. Can you program the record in such a way that it would show who did call it up?

Dr. SHERMAN HOPE. Yes, that can be done. Normally, under the security thing, when you make an entry—well, currently when you make an entry, it will initialize the record as to who made the entry. Now, just viewing it, that is not built in right now, but that is not a problem.

Senator LEAHY. But that could be done?

Dr. SHERMAN HOPE. Yes.

Senator LEAHY. If we were going to start having medical records computerized like this on a general, nationwide basis, it would be relatively simple, would it not, to program that whoever accessed the record would have to use his own identification number to access it, and once he accessed it, there would be a permanent record kept?

Dr. SHERMAN HOPE. Permanent record, yes, sir.

Senator LEAHY. As an example, it would show that Dr. Hope accessed it on July 12.

Dr. SHERMAN HOPE. Yes, and that would be created as a permanent record on it.

Dr. RICHARD HOPE. Yes, that is easy to build into the system. You can have an audit trail of who calls up the record and if a particular user gets someone else's access code or whatever, you would know that at least that person was signed onto the system and that they did look at that particular patient's record. You can make an audit trail.

Senator LEAHY. One thing occurred to me, especially when your father was talking about the type of practice you have. I come from a rural area, but we are not spread over the kind of distances you are. I suspect you have counties that would just about swallow up our State.

But I think of something like this as being especially helpful in a rural practice. Does that turn out to be your experience?

Dr. SHERMAN HOPE. It has been a major lifesaver in my office. It has allowed me to spend much more time with my patients and still give them adequate medical care and yet have more volume, because I am not spending all the time handwriting things, and my nurses have considerably more efficiency because they don't overlook things.

For example, immunizations: That is brought forward each visit. You do not overlook health maintenance. You can see immediately that either they are current on their Pap smear or they are behind.

Senator LEAHY. Well, let us take immunizations. You go in and get a flu shot. Would that get entered right then and there on your medical data card?

Dr. SHERMAN HOPE. Yes, sir.

Senator LEAHY. So that if that person shows up again 2 weeks later in an entirely different office, they would know it?

Dr. SHERMAN HOPE. Yes, sir, if they were accessing this. It is on the profile. That is part of the basic things we think doctors ought to know.

Senator LEAHY. Now, Mr. Haddock, your system goes beyond this in the amount of information that gets stored, is that correct?

STATEMENT OF RICHARD HADDOCK

Mr. HADDOCK. That is true. Our system is based on the optical memory card and as such, it can store about 4 million bytes of information in comparison to the 2,000 you see there, so this is equivalent to about 2,000 times that capacity. They could easily transfer that data onto this card in continued development of their same program with this media.

Senator LEAHY. So that if somebody from Dr. Hope's clinic went into an area where they had that system, it is relatively simple just to load it on?

Mr. HADDOCK. Yes. This card looks like a logical DOS device to the computer system, like a floppy disk or hard drive, and therefore their system is capable right now of transferring to such devices, so in a matter of minutes, I believe, they could take that data right there and put it on this card.

Senator LEAHY. Mr. Haddock, would you give us a demonstration of your system?

I have been in various health clinics back home where a patient may be asked about his or her past medical history and would be asked, "Well, what did you get?" The patient might respond "Well, they gave me a pink pill," or, "It was such-and-such." "Well, that sounds like it, but I am not sure." The doctor has to pick up a phone to call somebody else or find somebody else who is in. About an hour later, somebody will look through a record to find the answer, which I guess you would have already on the card.

But go ahead, Mr. Haddock.

Mr. HADDOCK. Part of what we came here to show you today was some security features related to health cards. There are many levels of security, from things as simple as PIN numbers that you are familiar with at ATM machines, to passwords to files. The most advanced level of security is biometric devices, and so this card is pro-

tected by a series of biometric devices, such as hand recognition systems, fingerprint scanners, signature recognition, and so forth, which can be selected to the degree of security you think is necessary for the card.

When I insert the card in the drive, it first looks to see who owns the card. It brings up just the name on the screen and goes no further until you enter a PIN number. At that point, it opens a basic record of the card, such as you might find on a driver's license or passport, of name, address, and so forth.

To go further and unlock the files, you must first verify that you have the right person, such as the photograph of the holder. With that verified, you can see things on there, you can verify the signature, you can verify dynamically on a dynamic signature tablet if required. In this demonstration, I am going to show you the verification of my actual hand geometry. It will not open until my hand is put in this unit. When it verifies that, it opens my medical record. If that was not my hand, it would not have gone any further.

At this point, you have your emergency medical information, similar to their program. However, now you can drop down into a menu of the other files on the card, and because our card actually looks like a logical computer device, like any other media, there are a number of files here that can be accessed in the same manner, such as patient demographics.

Regarding the question of updates and so forth, the optical media is an archival media. Once it is written, it cannot be altered or deleted but it can be updated, and so I have entered an address here. If I wanted that removed, I have a new address, it writes a new record to the laser card and now when you go back to it, you see that record has been changed the way you would expect, with typical magnetics.

The advantage of the laser card is that it maintains a complete audit trail of every change made. If you want to go back to what it once was, you select the history of the card and it drops back and shows you the audit trail of how that card was changed.

Senator LEAHY. So you could find out that the person lived in a different State before?

Mr. HADDOCK. Correct.

Senator LEAHY. Or had a different employer?

Mr. HADDOCK. And as you have said also, it date-time stamps exactly how it got changed and you could add to that easily who and where and so forth. And that is a permanent entry on the card that cannot be changed.

Senator LEAHY. If you have that much memory in there, there would be no problem showing when anybody accessed it?

Mr. HADDOCK. No. The card can store tens of thousands of updates, so that is a lot of action on one card. This is the case of a little history here. If you have a shot today, you would just enter that into the card and it would write an update for the flu shot. Now, you see, that has been changed and you have a history to go back and see how it got changed.

Similarly, things like prescription history, the doctor can fill out a prescription for a card. To find out whether refills are allowed,

and at the bottom of the screen, the pharmacist can read that but can only enter the date, showing that they refilled, the record.

The card's data capacity also allows it to hold images. In this case, x-rays controlled by this program. Every x-ray has a linked doctor's report against it of the doctor's diagnosis. At the time the x-ray is scanned and put onto the card, we create two actual image files. One is a small icon so that you can visually select which one you might want.

In this case, I will take this image of the spine. You select it and it now reads from the card the complete image file and then it displays it on the monitor, where you are free to zoom in and move around. You can change the contrast of the image or whatever.

You can store about 100 image files of that type on the card in addition to the text files. Again, to make sure you have the right patient, you have complete verification photographs.

This type of photograph is also used in another area of security, and that is things like passports and documents issued by governments, where files like this could be given an added level of security called the digital signature, which shows that not just any person put the photograph on there; it was put on by the issuing authority, such as the U.S. Government, and it was verified by them. This is done at MIT by a professor up there who actually applies visual signatures for such security.

I will show you one other security feature of the card, and that is this card contains the same basic medical information but it does not have a code which says that this is a—that I am authorized to read it, and this is not a valid medical card, have the administrator validate it. So you can put secret keys onto the card that says you are not authorized. So in the case of an employer, his terminal would not have the ability to read that code and you automatically reject them like that, and he could not open this record. It is impossible to open this record.

The other aspect of the card is because it does look like a logical DOS device. You can just read the directory off. This is loaded with a commercial program, so you can see the directory files of the card. So these are the files I am reading which shows there are 55 files on the card containing about 450,000 bytes of data.

The advantage of this program is that immediately, if you highlight the name of a file, it reads it from the card. So these are WordPerfect documents, so the minute you highlight it, it is reading from the card the conventional WordPerfect documents. If you want a copy of that, you can highlight it and say copy that to the hard disk drive. It reads it from the card, transfers it to the computer in that amount of time.

Senator LEAHY. Can you print it, too, if you want?

Mr. HADDOCK. If that was connected, I could have printed it in that amount of time. You can encrypt files, so I have taken that same file and applied a password protection to it, so when I highlight this file, it says the file is password protected and must be unzipped to view.

So along with open text records, you can have password protected ones which no one can view unless they have the password. So you can see, in a fairly simple demonstration, you can have mul-

tiple levels of security which can be designed to whatever the requirements of your system are.

Senator LEAHY. One thought occurs to me. You could also build in perhaps too much security. I am thinking of the signature access or something like that in the context of the emergency room and an unconscious patient.

Mr. HADDOCK. Yes. What the card initially does is bring up the emergency medical record which would be something the patient would agree is viewable at the time.

Senator LEAHY. Which would be immediately?

Mr. HADDOCK. Yes. One other thing is, some people do not want to use a keyboard. They want to use text documents. If you just wanted to take your handwritten notes, you could apply those to the card as well, and the way that we do this is through a conventional, like a fax machine. You can scan documents, in this case like a personnel file, where you want to see signatures and confidential notes, and you can store more than 100 such scanned document files on this card, as well.

Senator LEAHY. Do you have any concerns about a hacker getting in there? You hear about the dream of student hackers being able to get into the dean's files and suddenly they can explain to their parents, they really are working hard because they got all straight A's, notwithstanding a lost weekend during Homecoming.

I say this from books I have read, not from any personal experience. [Laughter.]

I went to a school with strict disciplinary methods.

But what about that concern?

Mr. HADDOCK. Well, the easiest way to show how you prevent that is by taking the card out. Once the card is out, no hacker can do anything to it. The card is now totally protected against that. If the dean takes records and puts them in his wallet, it can certainly hold enough records for an entire school year for a good-sized university. It is protected from that.

Senator LEAHY. You are not going to have somebody's AIDS test go from negative to positive?

Mr. HADDOCK. Well, but the records are not on a mainframe system and they are provided whatever degree of security you wish to apply to them in terms of, as I showed you, the biometrics.

If that person is not present, you could have that handprint actually encrypt his files so that he must be there for that file ever to be accessed, which is the ultimate case.

Senator LEAHY. If we are going to have a national health care plan, I expect we will go to an ability to carry your records around. Even without a national health care plan, we are going to use health data cards in one form or another anyway, because the technology is there, because we are a far more mobile society than we used to be, and because, to keep down costs, the doctor, whether it is Dr. Hope or somebody in my State, should not have to go down or have his staff go down and spend 30 minutes to find out whether you have had your flu shot or whether you have an allergy to any drug. Such cards will be helpful especially with patients who might have forgotten. Or might not fully realize how they have been diagnosed.

So we are moving to a system like this. Do you think it would be wise if we do, for us to start thinking of legislation which completely protects the card holder from being asked the questions? I am thinking of an employer who may say, "Well, I want to see your medical records." Of course the easiest thing to say now is, "My medical records are down in Dr. Hope's office in a big file. I don't have those." And nothing happens. If the employer says, "Hand me your card," shouldn't we have legislation that says an employer cannot do that?

Mr. HADDOCK. I think you should, although I also think that concern is maybe a little overstated, inasmuch as an employer's system would not be able to access this card even if the person handed it to them. The actual read-write card would recognize that this is not appropriate and would not open, and so the amount of protection could be in there.

Senator LEAHY. But so long as you have systems that can read the card in emergency rooms and elsewhere, it is not going to take very long before personnel offices in large companies to buy a set of the system.

They are going to be able to. I guarantee you, if 250 million Americans are walking around with these cards, it is not going to take long for employers to think, "We had better have something that can read those cards so we can ask all these questions." And then you run the risk with a large database on people that some of the information is going to be salable. We have had hospitals that have tried to make up mailing lists for purveyors of particular types of prescription drugs or other products.

We passed a law, which I helped to write, to make it difficult to go into a video store and find out what videos you rent. Well, that is one thing. You know, whether you rent Aladdin or Bondage Babes of Bombay or something—I am going to be terribly embarrassed if there is such a tape. [Laughter.]

If there is, I did not rent it. I did not rent Aladdin, either.

But if we are going to protect that information, we ought to protect whether you have been tested for hypertension or a sexually transmitted disease or gall bladder problems.

Mr. HADDOCK. I would certainly agree with that, and I think laws probably are required to prevent abuse of the system, and if you build a secure system, obviously people could get around that, but if that was made illegal, that would add another level of security to the overall system.

Senator LEAHY. True. And the same with selling the information.

Mr. HADDOCK. Yes.

[Mr. Haddock submitted the following:]

PREPARED STATEMENT RICHARD M. HADDOCK ON BEHALF OF THE LASERCARD SYSTEMS CORPORATION SUBSIDIARY OF DREXLER TECHNOLOGY CORPORATION

SUMMARY

This presentation is intended as a short introduction to the use of optical memory cards in health care. Optical memory cards, the size of a normal credit card, are designed for use as a personally carried database. They are a secure storage media, functionally the equivalent of a computer floppy disk drive or a hard disk, and support all security and privacy techniques used by industry and government to protect computer information. They offer the highest storage capacity any card type, enough to store up to 2,000 pages of text on one card. The data is updatable, but cannot

be tampered with or altered without detection. The card has the ability to store thousands of individual transactions per card. A review of some of the security and privacy features used on the card are presented, as well as a partial list of optical card users in healthcare. Also included is a brief comment on the U.S. position in the world market for information cards.

A short demonstration of an optical memory card system will be made, featuring medical, security, and biometric aspects of the technology.

INDUSTRY BACKGROUND

California Technology. The optical memory card was invented and patented in 1981 by Drexler Technology Corporation of Mountain View, California (a public corporation). Drexler Technology built a $25 million manufacturing facility with a capacity of more than 25 million cards per year. More than one million cards have been produced there. Additional manufacturers of optical cards are Dai Nippon Printing, and Canon Inc., both of Japan, who operate under license to Drexler Technology patents. There are multiple sources for card reader/writer units.

Optical card systems are being developed in more than 40 countries worldwide, with LaserCard Systems Corporation, (as a wholly owned subsidiary of Drexler Technology) a primary supplier of cards, hardware and software to application developers since 1990.

Description of the optical card system

The optical card is used in a reader/writer unit, which in turn is linked to the computer system by an SCSI (Small Computer Standard Interface) connection. The card, when inserted into the reader/writer by the user like an ATM card, is immediately confirmed as a valid card, and then the card file directory is read. At this point, it appears like a conventional floppy disk to the host system.

Depending on the security features of the controlling application software, the user is allowed to read or write files to the card. Once the transaction is finished, the card is automatically ejected, and given back to the user.

Any information on the card can be accessed in less than one second, and over 200 pages of text can be transferred from the card in less than a minute. Images, voice, charts, and graphs may also be stored on the card, as well as all types of security biometric identifiers. All standard data privacy and encryption methods may be applied to the card, such as Personal Identification Numbers (PIN), DES (Digital Encryption Standard), private/public keys encryption, including digital signatures. Several applications can be stored on a single card, and each kept confidential and secure from other applications. Some file areas may be used for open information, such as basic emergency medical information, with additional file areas controlled by increasing levels of security required for access. One optical card, having about 500 times the capacity of an integrated circuit card, provides the ability to store and partition information for dozens of separate applications relating to the card holder, and offers the maximum potential for growth as future data requirements develop.

The data stored on the card is secure and cannot be affected by magnetic fields, static electricity, and similar problems that cause memory loss in other cards. While it is true that the optical card surface can be scratched, the card format has error detection and correction functions, which allows most data obscured by typical surface damage to be reconstructed automatically.

Additionally, the optical card may be combined with a magnetic stripe to allow use of both the conventional magnetic stripe applications along with the use of the advanced features of the optical card in the future.

Optical card advantages

Optical memory cards, physically the same size and shape as conventional credit cards, offer significant advantages over magnetic stripe or I.C. cards, particularly in the area of healthcare information. All these cards can store information digitally.

Three key features differentiate the optical card from all others:

1.) *Data Capacity.* The magnetic stripe card has a memory capacity of 100 to 300 characters, or bytes, of data. This represents a few sentences of information. The I.C. card, containing a silicon memory chip within it, comes in many configurations, covering a memory range from about 2,000 to 16,000 bytes of information, representing 1 to 8 pages of text. However, current versions of optical memory cards hold more than *4,200,000* bytes of information, allowing one card to hold the equivalent of up to 2,000 pages of text (alternately, dozens of high quality medical and document images, plus a few hundred pages of text may be stored on one optical

card). This high memory capacity, coupled with the optical cards ability to safely store this information is a primary advantage over other cards.

Card Type	Number of pages stored per card (at 2K bytes/page)
Magnetic Stripe Card	0.1
I.C. "Smart Card"	1 to 8
Optical Memory Card	about 2,000

2.) *System Compatibility.* The optical card functions in a computer network exactly like a floppy disk or a removable hard disk. The large memory capacity of the optical memory card allows conventional computer file structures to be used on the card, which is not possible on other cards. This allows use of normal system and network software to access, read, write, and maintain data security on the optical card in the same manner aa used for the hard disk drives within the network or individual workstation.

3.) *Durable, Secure Data.* A key feature of optical memory cards is the use of passive, permanent memory, unlike the volatile, erasable memory used in other cards. Writing on an optical card is done by a low power laser diode, similar to that used in CD disk players. The laser melts a series of holes into the reflective optical media surface, lowering the reflectivity within the holes. This string of holes, like punching holes in a paper tape, represents the digital data, and once written, cannot be physically erased or altered. This gives the optical card a high degree of data security and protection against unauthorized modifications. However, although the optical card cannot be erased, new data can be added to it, allowing information updates and additions, which is essential in any application. A permanent audit trail of all changes is maintained on the card for security.

DATA SECURITY AND PRIVACY ISSUES USING OPTICAL MEMORY CARDS

The optical memory card looks, to the computer system and the user, like a normal disk drive, and therefore all normally applied security and privacy techniques used on magnetic disk media can be applied to optical cards. In any configuration of a new U.S. healthcare system, it is clear that the computer network, with high-speed data links, will surely play a central role. These networks will automatically send secure messages and files, using data encryption, digital signatures, PIN numbers, and other techniques to assure the security and privacy of the information transferred between storage media on the sending and receiving stations. The optical card can directly link into any such network, and send and receive secure information, in the same secure manner.

As previously mentioned, the optical card can be partitioned for separate applications, with each partition having its own type and level of security. While the actual security structure for use in the National Heath Security card would have to be defined, it is clear that almost any level of required security can be achieved by the use of optical cards.

In comparison to magnetic stripe cards, the non-alterable recordings and large capacity allow the optical card to duplicate and exceed any security method used on the magnetic stripe. Again, the optical card can be produced with an added magnetic stripe on the back if required.

In comparison to IC "Smart Cards," first one must realize that there are a large number of variations of IC cards, with different features and complexities, as well as price. The most complex and expensive version is used for comparison, such an I.C. card containing both memory and a microprocessor. This processor is used to give added security to the IC card, by allowing it to internally encrypt and decrypt passwords and data. While these are good features, the optical card can obtain the same degree of data protection as afforded network data and magnetic disk drivea, without the need for a internal processor within the card. The protection process in the attached reader/writer, or the host computer system can provide the same functions, with much higher performance and capability, as well as convenience in backing up the card data.

EXAMPLES OF OPTICAL CARD SECURITY FEATURES

Optical cards are secure against counterfeiting

Each optical card can have a factory encoded serial number, which can be used to "lock" the data to that one card, and eliminate any possibility of counterfeit cards being produced. The entire data structure on a card is determined by first reading

its unique serial number, which is used in conjunction with encryption to read and write records to the card.

Optical cards are secure against unauthorized access to private data

PIN numbers, encryption (such as the Data Encryption Standard D.E.S.), Public/Private keys (such as RSA, DSA, or the Public Key Cryptographic Standards P.K.C.S.), and for the maximum security, biometric identification, can all be used with optical cards. Different techniques can be used on different areas within the same card, to allow the maximum flexibility to designing a system that is both simple and secure.

Biometrics assure individual identification

No system is totally secure if the personal accessing the aystem cannot be positively identified. A "secure" magnetic or IC card can be handed to another person, along with any access codes. The card will be accepted as valid, and can still authorize payments and create electronically "aigned" documents, but with the wrong card holder. Using optical cards allows the full use of biometrica for absolute identification when required.

Individual privacy assured

Protection against the misuse of a health card as a type of citizen identification card can be assured by partitioning the data by authorized user type (hospital, pharmacy, insurance company, clinics, individual doctors, etc.). Each group may access only those files previously authorized. This allays the fear that one's health card could be demanded for inspection by a prospective employer, for example, since the files would be encrypted against unauthorized access.

Doctor's confidential files

Given the large data capacity of the card, each doctor wishing to could define a confidential area for their own private notes on the patients card. Only that doctor could later access and read this area.

Ease of secure data back-up

All systems need a good system for data back-up and to re-issue cards. Data back-up and the issuing duplicate cards for those lost, damaged or stolen is a matter of system design. Since the files on the card are themselves secure, optical cards may be backed-up onto a network or other central atorage system *without requiring the knowledge of card access codes or pass words,* and still maintain the same data privacy. If a new card must be created due to the loss or damage to the original, the central files are simply copied to a new card. The actual method of where, when, and how often the data is backed up is again a matter of system design. (In the case of IC cards access and back-up to the entire card data content is much more difficult, since data security is handled in the card, and cannot be accessed for back-up without passwords and PIN numbers. All the card data must be copied from the card to a central system for back-up, and therefore additional security measures must be taken).

Overall, the optical card offers the widest range of methods of any card to assure privacy and security of confidential records, with the added benefit of partitioning the card to keep a hierarchical structure of between users and applications as required.

THE US POSITION IN COMPARISON TO THE REST OF THE WORLD REGARDING OPTICAL AND IC CARD USAGE

In comparison to Europe and Japan, the United States in general has been slow to adopt either optical or IC cards in health care. There are many reason for this, with the top two reasons being questions on electronic records legality, and secondly, the wide use of magnetic card for financial services in the U.S. While magnetic stripe technology is a simple choice for closed centralized financial systems, they cannot offer secure data storage for any useful amount of patient information. An optical card with a magnetic stripe on the back can function in these existing systems. The legal barriers associated with a computerized patient record are well known, and have been discussed extensively in forums on health care.

IC cards are seen in many French, German, and to lesser degree, Japsnese health care systems, due in large measure significant government subsidizes. For example, in Germany, they have begun implementing a I.C. card health card system intended to cover all 80 million citizens. The German laws forbid the state to have the medical records of the citizens, and so the actual data content on the card is very low, about 280 bytes of information, covering name, address, insurance and account

numbers, with no medical information at all. This project is seen by many as an effort in Germany to subsidize their IC card producers, and to establish a network of read/write terminals across Germany for other uses. Likewise, in France IC cards have wide use primarily as a telephone card and now are moving into basic medical cards, holding name, address, and insurance information. Similar projects in Europe focus mostly on the financial and insurance information, since the IC card cannot hold much patient data.

Optical card applications face an uphill battle in Europe, particularly in France (the IC card is a French invention), where the government subsidized IC cards make adoption of American optical cards politically difficult for many interested users there.

RECOMMENDATIONS

As a means of building broad support for the optical card uses in health care, some limited implementation of the optical card system could be done quickly, and could demonstrate the cost savings and health benefits achievable with this technology. The card would be a "dual stripe" type, having both an optical and a standard magnetic stripe, to assure overall system compatibility. The optical card could initially be used with two populations. First, for those specific groups within the population having high health care costs due to chronic illness, such as diabetes or kidney problems, as well as pre-natal care and other such important areas. Second, the card could be offered as an option to those in the general population wishing to carry their health records on their Health Security card, and paying for this additional service.

This approach may avoid most concerns that the individuals' privacy is at risk, since the optical card would be a voluntary upgrade, with the person knowingly electing to carry their own health information.

It is really the individual who is most concerned about their own health records, so it should be the individuals' choice on how much, if any, health information they wish to carry with them. The use of the additional information contained on the optical portion of the card, even a few times, should quickly result in health benefits and cost savings due to quicker diagnosis and earlier treatment, and the elimination of unnecessary testing and evaluations, as well as paper work reductions.

Medical facilities interested in implementing the hardware systems required for the optical cards could be given a tax credit or other such encouragement to set up to use this technology. After an initial period, the normal competitive forces in the health care business should then take over. Also, equipping all 160 V.A. hospitals with a basic optical card system would implement the system over a wide geographic area.

It appears possible that the government could generate an income from the sale of optical dual stripe cards to those electing to use them. This income could in turn be used to supply cards to other population groups needing the card for specific health concerns, but not able to afford additional expense.

OPTICAL CARD PROJECTS

California-made optical cards have been used in the example projects listed below:

United States: California. Novus Technologies, of Del Mar, California, has developed and implemented a medical image archive system using optical memory cards. Their system functions as an integral part of MRI and CAT imaging center operations, with each system projected to offer significant cost saving in film archive and retrieval costs alone. Typically 80 medical images are stored on each optical memory card. Sites have been installed in several cities in California and Nevada.

United States—California—VISX, Inc., a medical equipment company in Santa Clara, California, uses optical memory cards as part of its system for laser eye surgery—for both machine setup and as a cost-control measure. The equipment setup data for each patient's surgical operation is written to the cards in advance of the procedure. When the patient is later brought into the surgery, the pre-programmed optical memory card is inserted into the equipment control panel, where the patient data is used to automatically set up the hardware for the operation. The actual machine parameters during the operation are also recorded to the card.

United States: Houston, Texas. The City of Houston sponsored an "Immunization Fair" at the Houston Astrohall during November 1992, where parents of all school-age children were invited to get free vaccinations for their children. As part of this event, optical memory cards containing the child's basic demographics, photograph, and immunization history were created. The optical cards were then issued to parents by the City Health Department. The program has been budgeted to be implemented during this fiscal year in Houston.

United States: California—Loma Linda School of Medicine. A complete multimedia patient card program, including doctor's voice recording on the card for dictation, x-rays images, and photographic patient identification has been developed by the WIN2 group at the School of Medicine.

United States: Minnesota—Summit Medical. Summit Medical has developed several optical memory card applications, one of which uses the optical memory card for tracking medical procedure follow-up, such as cardiac and/or lung transplant patients. The card functions as part of a distributed database on the patient registry, to maintain accurate and confidential records of the outcome of major surgeries.

United States: Department of Veterans Affairs, Information Systems Center, Albany, New York: The VA began development of an optical card application in 1989. Their initial emphasis was to develop a standard interface method to access the existing VA database information in the regional centers. The VA had planned on initiating pilot projects in up to 7 different medical centers, however, due to lack of funding and a clear mandate, the program remains on hold. The main application areas are patient record cards, with the optical card holding all the basic patient file data, drug prescription information, and specialized treatment history. A significant area of the card system design is the intention to allow patients requiring care not available in their local facility (such as open heart surgery) to be transferred to the appropriate facility with their entire medical history contained on their optical patient card.

Another important element of the VA patient card application is the ability of the card to store the individuals benefits eligibility. The VA patient benefits vary widely due to factors such as branch of service, tour of duty period, combat history, and special factors, such as exposure to hazardous environments. The VA system is further complicated by the wide range of hospital and clinics the patient has to choose from. Although within a given facility, local area networks are usually present, the entire VA medical system is not currently networked together, making it difficult or impossible to have complete health and benefits files available for all incoming patients. The optical card pilot project was designed to demonstrate the great value of having the individual patient be capable of bringing a comprehensive medical file with them to any facility within the VA system.

United States: U.S. Air force. Texas, Wilford Hall Medical Center at the Lackland Airforce Base, created an optical card system designed by Digital Equipment Corporation, beginning a plan to use optical patient cards within the U.S. military hospital system. Implementation has been delayed due to re-structuring of military bases and the shifting of computer resources within the hospital system.

United States—Defense Logistics Agency—Cargo Manifest optical cards are used to record military cargo manifests, with the card being kept with the shipped goods. The optical card allows the in-field inventory database to be immediately update with the incoming material, and allows maintaining an accurate inventory on a pallet level. Since pal lets are frequently moved between locations, having an updated pallet level inventory on optical card solves this difficult problem. The optical cards' excellent durability characteristics, including the ability to withstand temperatures up to 100 degrees C. (212 degrees F.), make it the only media capable of meeting this demanding applications need. Projects started in 1991, focused initially in achieving proper data exchange between the many different computer environments already used for military inventory systems. This system has been expanded after extensive field testing with the U.S. Army.

England: Chelsea/Westminster Hospital project by British Telecom: started in 1988 at the West London Hospital, the optical cards hold the pre-natal care data from mothers during the entire course of their pregnancy. The initial pilot trial was successfully concluded in late 1990, after more than 1,000 women participated in the program. During the pilot, more than 1,000,000 transactions were logged on optical cards. With more than 1,500 cards used, the trial was the basis of the continuation of the optical card program in Chelsea/Westminster Hospital system. The program is planned be expanded, by the British National Health Service to allow the pre-natal care data to be shared between several medical facilities. The basic information stored are the results of each medical check-up during the pregnancy term, ultrasonic scan results, doctors notes, and the patients own diary during this period. The system is to be expanded into individual doctor's offices, as well as additional clinics and hospitals.

Australia—patient record cards, starting with pre-natal care, are being implemented at the Queen Victoria hospital in the Adelaide, Australia. The pilot began in 1991, and is based on the successful West London Hospital program. This project tracks all maternity records, with the added feature of the ability to record the entire fetal heart monitor chart onto the optical card.

France—Nuclear medicine image files are stored on optical cards at the University of Paris medical center. Each optical card stores up to 150 nuclear medicine images.

Japan—projects underway for several years involve storing dialysis records on optical cards.

Japan: Tokyo University Medical and Dental Hospital has been working for several years to develop the software interface for optical card storage of medical records. Their efforts have created a system capable of allowing immediate access to a wide range of patient medical history, including basic medical profiles, immunization records, charts, patient photographs, and basic medical x-rays.

MR. RICHARD M. HADDOCK,
DREXLER TECHNOLOGY CORPORATION,
Mountain View, CA, January 17, 1994.

Hon. PATRICK J. LEAHY,
Subcommittee on Technology and the Law,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY, I appreciated your giving me the opportunity to testify before the Subcommittee on Technology and the Law October 27, 1993. I have received your additional questions in your letter of December 28, 1993, and have enclosed my answers for the final record. I would be pleased to provide additional information if the enclosed answers are not sufficient, or if more information on other topics is desired.

I appreciate the in-depth evaluation your Subcommittee is pursuing in order to assure that the proper balance between the need for privacy and the benefit of fast information access is achieved in future health care policy. I hope that I have been of assistance in helping your group progress toward meeting these objectives.

Best Regards,

RICHARD HADDOCK,
President,
LaserCard Systems Corporation.

RICHARD M. HADDOCK'S RESPONSE TO QUESTIONS SUBMITTED BY SENATOR LEAHY

Answer 1. Required privacy and security guidelines: Privacy of an individual's health record is a primary concern for everyone. While the need to have immediate access to a patient's health information is recognized as a great asset, this benefit is balanced against the fear of improper use of such confidential information. Storing patient information on health data cards, kept in the patients' possession, can minimize the opportunity for violation of privacy of patient records. The distributed data approach of patient cards is far less prone to abuse than the concentration of all patient information into a central database that allows general access by all in the health care community.

However, any form of patient records, including the current paper record systems, need to be protected by laws to enforce the rights of the individual against improper access or disclosure of their information. Legislation is needed not only to define the proper use of all levels of patient information, but also to provide for a means to verify when and by whom such information has been accessed, in as simple and foolproof method as possible. The requirement of an unalterable audit trail of all accesses to a medical record would provide the means to determine the validity of the records access, and to provide for a means to enforce any privacy laws covering medical records. Such a audit trail is virtually impossible with paper records, and while perhaps possible in a central database approach, will not convince the public that such a centralized system cannot be modified or abused. However, to keep a data log of such audit trail information stored upon the actual patient health card itself, in a non-volatile, permanent recording media, is not only a simple and straightforward approach to the problem, it is also a concept the general public can easily understand and accept.

Additionally, the patients are in a position to review their own records, as well as the data access log on their card, and to see by whom and how their information has been used. Patients should also be entitled to define the degree of privacy associated with their information, what information can be accessed in certain situations such as emergencies, and how much information is placed on their card. See figures 1–4 regarding the multiple levels of security available.

Answer 2. Optical Cards at Lackland Air Force Base: The optical memory card project at the Wilford Hall Medical Center at the Lackland Airforce base was created to improve efficiency, reduce waiting time, and provide for immediate access to emergency information. The project was implemented by DEC (Digital Equipment Corp.), using optical memory cards manufactured by Drexler Technology Corporation, as part of the existing information system at Wilford Hall. The funding was sufficient to cover only the initial prototype of the application, in order to validate the full program. The prototype phase was successful, and worked well. The cards were issued to a limited number of people, with medical information such as demographics, health background, and even scanned images of birth certificates written on the optical cards. The first funding was not sufficient to move into the next planned phase, for pre-natal and pediatric records. Wilford Hall is now in the process of implementing the Composite Health Care System (CHCS). The full use of the optical patient card is anticipated once the CHCS scheduling system software has been upgraded. The optical card will link into the patient scheduling module of the CHCS software, which is currently being installed. Once this has been done, the optical card patient record system is expected to be put into service, funding allowing.

Answer 3. Optical Cards at the West London Hospital: The optical memory card program has been broken down into phases: Phase 1, to verify the technology and functions was started in 1990 and ran through early 1992. This was successful, and validated the use of optical memory cards to hold patient records. Over 1,000 women were involved in this phase. The positive response from this program led to the funding of Phase 2, which started in May 1992.

Phase 2, funded by the National Health Service, had the objective of spreading the use of the technology outside of the hospital, into doctor's offices and to midwives clinics, in order to improve communication and healthcare. 302 women participated in Phase 2, which has just finished as of January 94.

Professor Steer, of The Charing Cross and Westminster Medical School, has been in charge of this program and makes the following comments on the increased efficiencies:

> The Medical Research trials carried out using the OMC (optical memory card) in Phase 1 and Phase 2 at the Charing Cross and Westminster Medical School since 1990 have clearly demonstrated that "an improved patient care can result from using the OMC as a portable patient record in antenatal care services". With Phase 3 due to commence in mid-'94, at the Chelsea and Westminster Hospital and extended to include ante-natal care at St. Mary's Hospital Paddington, London, both hospitals will utilize OMC's and advanced software as an integral feature for some 6,000 patient records that will be involved during this continuing medical research program.

Additionally, since British Telecom has been the systems integrator for the OMC program in London, included is a brief overview from the British Telecom Tall is group from April '93 outlining their view on the OMC project.

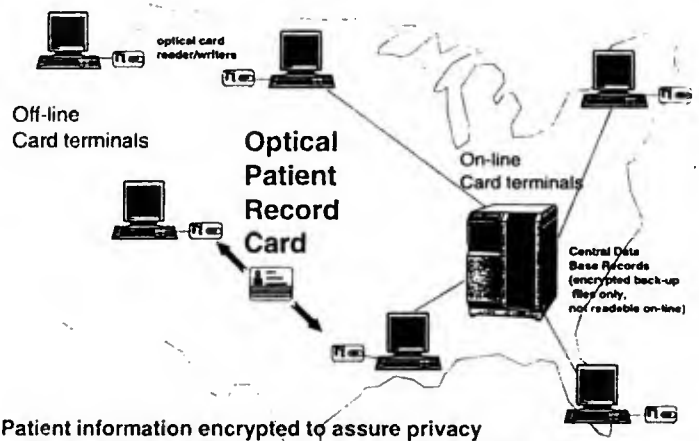
Answer 4. Loss and Replacement of Cards: Patient information stored on an optical card can be stored in an encrypted form, readable only from optical cards in proper terminals authorized to access particular records on each card. While all the information on the card can be backed up onto local or even central databases to provide for replacement cards, such back-up data files would not be readable or accessible by the user community, and only would be usable to re-create a patient record card. The patient information, once written back onto a card, can then be appropriately accessed in a authorized reader/writer terminal. Therefore, while a back-up database is required to assure for replacement of lost or stolen cards, the general use of optical cards in not dependent upon a central database, since the access and use of the cards is normally a off-line transaction.

Answer 5. Security of Central Records: As noted in answer 4. above, individual computerized medical records can be protected in a central database if the only use of such a database is restricted to back-up of card information, and not as a general central database providing on-line access to all. Since the purpose of the back-up records is only to restore or create patient cards, the encryption methods used can protect the information against any other uses. Thus, these encrypted records may be passed between users via the normal telecommunication and network channels for back-up without any compromise of their security.

Answer 6. Computer Viruses: Optical memory cards are WORM media, meaning "Write Once Read Many." This means that information can be written to the card at any time, but once written, it cannot be altered or erased without detection. Software provides the ability to simulate erasure, by writing new information in a different area of the card and having the application only recognize the most recent data. However, all the information written on the card is always present on the

card, and can be recalled when necessary. This permanent audit trail ability, plus the non-volatile nature of WORM optical media, make it the best possible choice against computer viruses, whose typical trick is to erase or alter existing information on magnetic or silicon memory in hidden ways. Optical cards are immune to such alterations. In answer to the final part of the question, no, it would not be possible to alter the health records, such as to create positive results in place of negative, if optical cards are used. Additionally, even the magnetic based card information back-up records could not be altered, since they would be stored in an encrypted form, and cannot be added to without the use of the optical card read/write system.

Medical record system configuration using optical memory cards



* Patient information encrypted to assure privacy
* Medical records can only be read in optical card R/W unit
* Permanent audit trail of all data accesses

Figure 1

Multiple level record security system configuration using optical memory cards

* Patient information encrypted by area to assure privacy
* Each department can only read appropriate files in optical card R/W unit
* Permanent audit trail of all data accesses at all sites

Figure 2

Data Security Levels using Optical Memory Cards

Figure 3

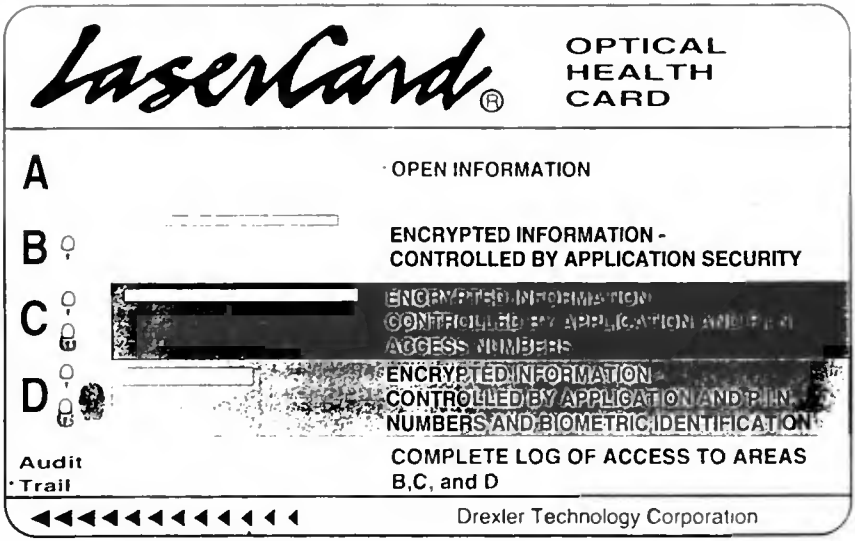


Figure 4

LASER OPTICAL OUTPATIENT CARD PROTOTYPE IMPLEMENTATION AT WILFORD HALL USAF MEDICAL CENTER

SUMMARY

Wilford Hall USAF Medical Center (WHMC), located at Lackland AFB, San Antonio, TX, has taken a first step toward implementing an electronic medical record by developing the Laser Optical Outpatient Card (LOOC) Prototype. In addition, this is an initial effort by a military hospital toward a worldwide standardized laser card technology and medical record format. LOOC was designed and developed as a joint effort between WHMC and Digital Equipment Corporation.

LOOC is intended to replace the use of embossed patient cards, print patient identification information on existing forms, and provide electronic access and storage of medical information for patients at WHMC during a patient encounter.

WHMC is the largest Air Force Medical Facility in the world. Digital is a leading systems integrator and has completed more than 5,000 systems integration projects to date with current systems integration revenue worldwide of more than $2 billion.

If your organization is interested in implementing this technology or if you would like additional information, please contact Lezlie Odstrcil, Digital Equipment Corporation, at 210/524–2819.

Wilford Hall Medical Center (WHMC), the largest Air Force Medical Facility, is located at Lackland AFB, San Antonio, TX. It is a 1,000 bed hospital with over 90 clinics and subclinics. WHMC is the Air Force medical training and research center and is rated a Level-1 Trauma center for the San Antonio area. Over 1,000,000 outpatients are seen every year; over 9,000,000 laboratory procedures are conducted every year; and over 2,000,000 prescriptions are filled annually.

Wilford Hall currently uses the embossed "credit card" to identify patients during a visit. All medical treatment forms, lab slips, and consult sheets are stamped with this card. Unfortunately, many problems have arisen with this method of identification. The last copy of many of the multi-part forms is unreadable; copies smudge easily; the raised characters become worn, causing inadequate impressions; and lastly, the card contains only a minimum of information.

Medical Systems Directorate (SGI) at WHMC proposed the development of a Medical Record Imaging System with the eventual goal of total automation of medical record processing and the electronic medical record. The benefits that such a system can provide are innumerable. Patient "in-process" time is greatly reduced, thereby increasing the time the patient can spend with a provider. This system also provides easy patient tracking throughout the medical facility. A patient's longitudinal medical history is quickly available with minimal administrative intervention, improving health care delivery. In a military setting, a card-based medical record system would definitely enhance the readiness and mobility mission by speeding up the medical record checking process prior to deployment. Vital medical information could be obtained from patients who otherwise may not be able to communicate with the medical staff in emergency situations. Providers are also immediately presented MedAlert data, possibly circumventing legal action on the part of the patient. Personnel in transit or on TDY would also always have their medical records available.

A team was assembled to make this proposal a reality. Medical Systems provided the requirements definition, the overall design and a operational test site. Digital Equipment Corporation (DEC) was responsible for systems development, configuration and integration; and LaserCard Systems Corporation provided the optical memory card technology.

The requirements defined for the laser card by SGI were durability, the versatility to store various types of medical data in various formats, the ability to add new information and replace lost cards quickly and easily, and permanence (i.e., non-modifiable by the bearer). The requirements for the generated forms were readability of all multi-part medical forms and the ability to store and update numerous formats. The overall system requirements were ease of use, based on Commercial Off-the-Shelf (COTS) software, resideon a PC, a Windows-based application with a Graphical User Interface (GUI), controlled access (i.e., password protected), and on-line HELP.

The overall hardware configuration is as follows: a VAX 9000 provides the storage for all patient demographic and medical information. Access to these data will be from workstations in the various clinics using the Digital product "Pathworks." Our in-house AQCESS system for patient appointment scheduling is an alternate source of patient demographic data, using the Dynamic Data Exchange (DDE) abilities of the terminal communications package, Smarterm 320. Each workstation consists of

a Personal Computer (386 or faster CPU), a thermal printer, a scanner, an impact printer and the LaserCard reader/writer. The thermal printer is used to engrave the patient's name on the back of the laser card. This printer is accessed through a parallel port on the PC. The image scanner is used to scan in birth certificates, or any other image, into an electronic format that is then displayable by Microsoft Windows' GUI. The LaserCard reader/writer electronically stores information on the optical card. This is the only means of creating, accessing, and updating patient information on the card.

The Laser Optical Outpatient Card Prototype has five major software processes: Arrival, New Patient, New Card, Maintenance, and Help. "Arrival" processes a patient who has arrived for an appointment and provides the printing of forms used during the visit or ordered by the provider. This process assumes that a patient has been registered in the database and that a Laaer card has already been generated. The "New Patient" process is used for the creation of a new patient identification record in the LOOC database. It queries the user for basic demographic data, the military sponsor's information, insurance information, and significant medical information such as MedAlert, immunizations, allergies, etc. The "New Card" process allows for the creation of the laser card once the patient's information has been obtained and stored via "New Patient." "New Card" is also the process that must be exercised to regenerate a lost or damaged card. To perform any updates to a patient's card, any of the store patient, sponsor, or insurance information, or the format of any of the standard forms, the "Maintenance" process must be selected. The last process available to the user is "Help," which provides the user with complete on-line guidance and information necessary to complete LOOC tasks.

In conclusion, the development and implementation of the Laser Outpatient Optical Card Prototype by Wilford Hall Medical Center are initial efforts toward worldwide standardized laser card technology and a medical record format. Once these objectives have been accomplished, the goal of a standardized electronic medical record can be realized.

Wilford Hall USAF Medical Center
(WHMC)

digital™

Laser Optical Outpatient Card Prototype Implementation

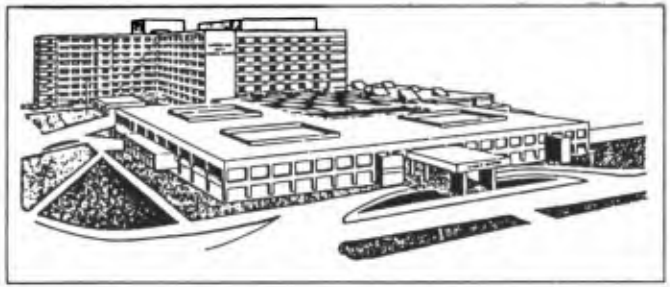
(A joint effort with Digital Equipment Corporation)

Principal Investigator
Lac V. Tran

Presenters
Janelle Feltman (WHMC)
Paul Lozano (WHMC)
Michaela Phillip (WHMC)
Lac V. Tran (WHMC)
Eugene Dowen (DEC)

BACKGROUND

dmrtal™



Commander: Major General Edgar R. Anderson

Vice Commander: Colonel Jack L. Saylor

Administrator: Colonel Terence T. Cunningham

Largest Air Force Hospital

Located at Lackland AFB, San Antonio, TX

1,000 bed hospital

90+ clinics and subclinics

1,000,000 outpatient visits per year

2,160,000 prescriptions per year

9,000,000 lab procedures per year

Air Force training and research center

Community Level-1 Trauma center

PATIENT CARD PROBLEM STATEMENT

d I g I t a I ™

- Current situation: Use WHMC Outpatient Card "credit card" to identify patients during visits
- Problems:
  - Unreadable copies of multi-part forms
  - Smudging
  - Raised letters on card become worn
  - Contains limited personal information

TEAM

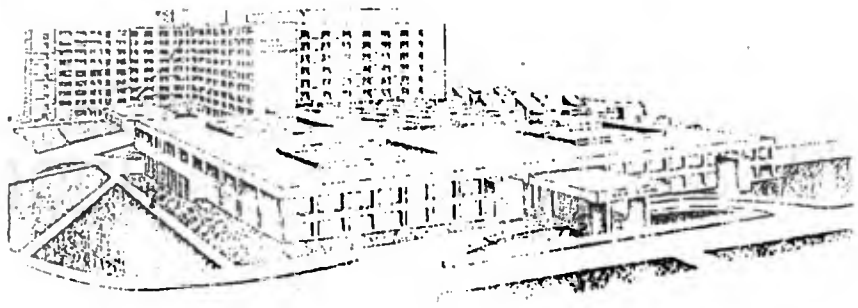
DIGITAL™

- WHMC Medical Systems (MIS) for user requirements, design and operational testing
- Digital Equipment Corporation for systems integration
- LaserCard Systems Corporation for optical memory card and data system

USER REQUIREMENTS PATIENT CARD

digital™

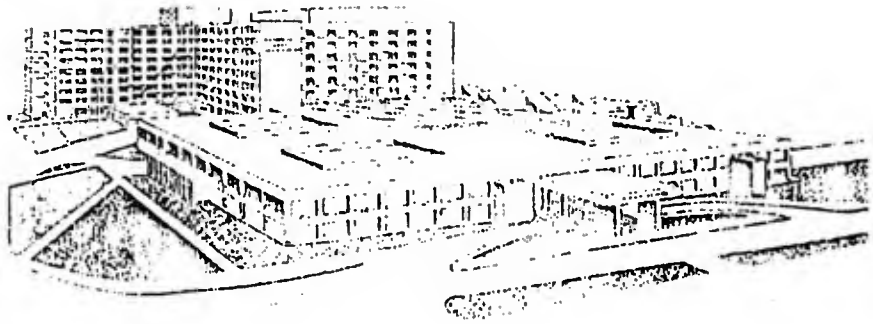
- Optical memory card
- Durability of card
- Medical data to be stored on card
  - MEDALERT
  - Immunization record
  - Allergies
  - Blood type
- Ability to store images (Ex: Birth Certificates)
- Ability to add new information easily
- Non-modifiable storage of data
- Ease of replacement of lost cards



USER REQUIREMENTS FORMS PRINTING

digital™

- Readability of printed forms
- Standard Form 600
- Various templates



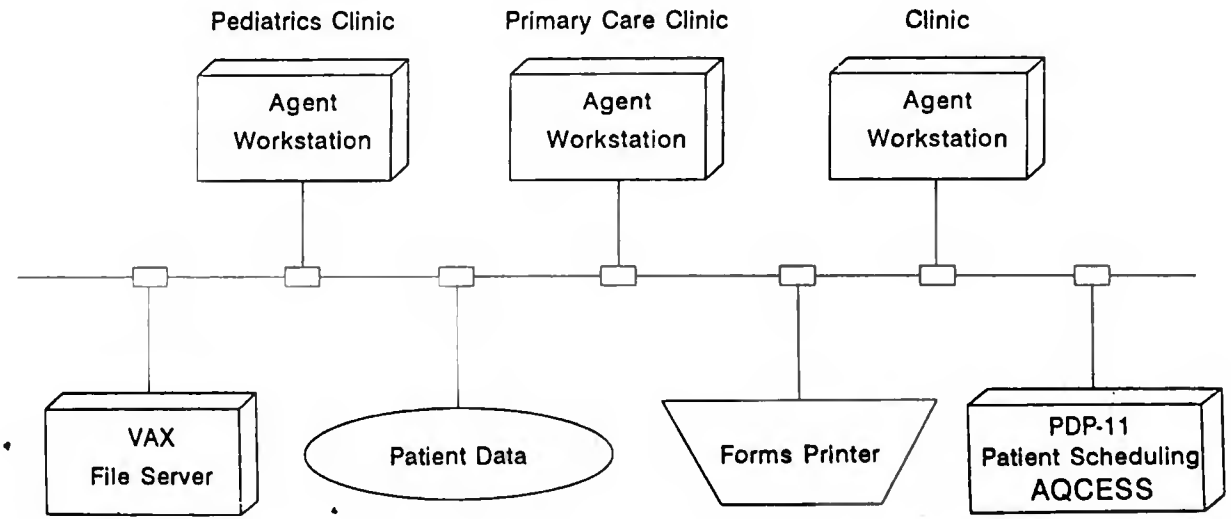
USER REQUIREMENTS SYSTEM

dTgTtaT™

- Easy to use
- Commercial Off The Shelf (COTS) based
- PC based
- MS-Windows interface
- Password protection
- On-line help

SYSTEM CONFIGURATION

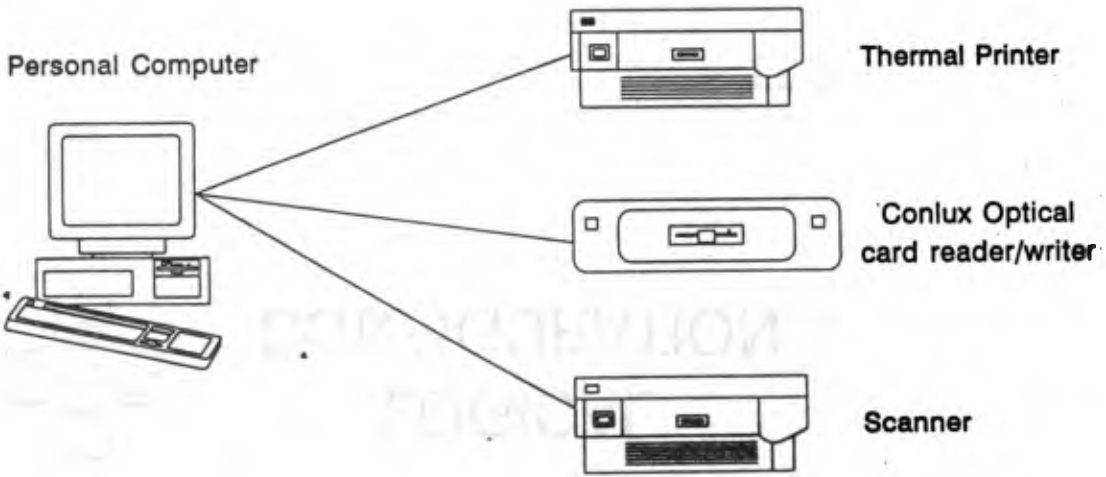
digital™



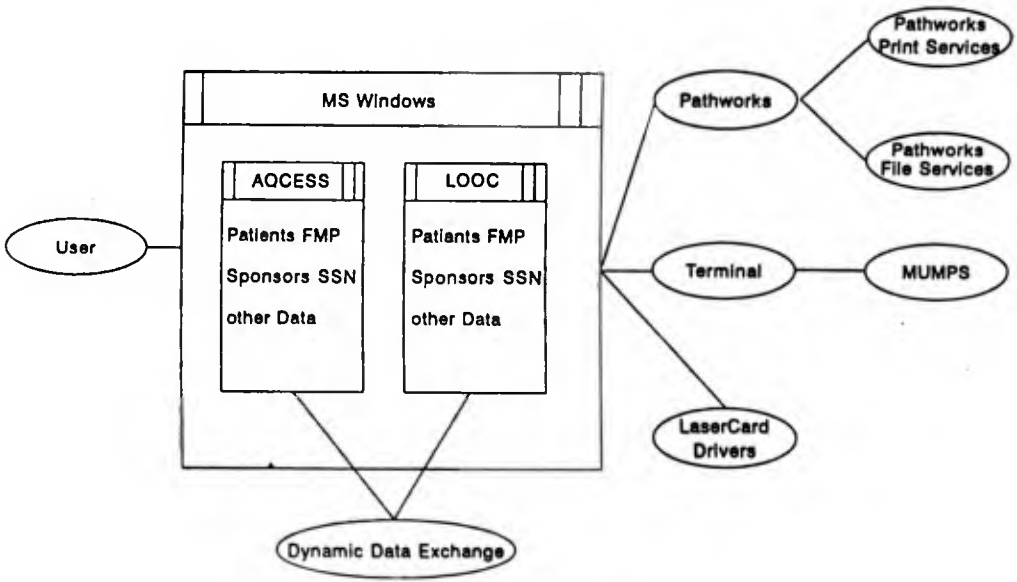
AGENT WORKSTATION CONFIGURATION

dmgmt™

LaserCard System 1000

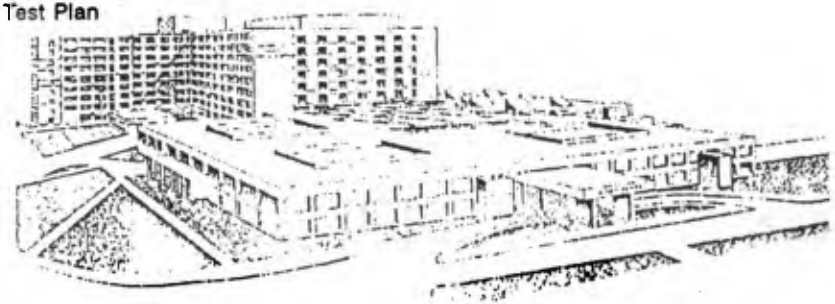


LOGICAL CONFIGURATION



ENGINEERING PROCESS dmgttal™

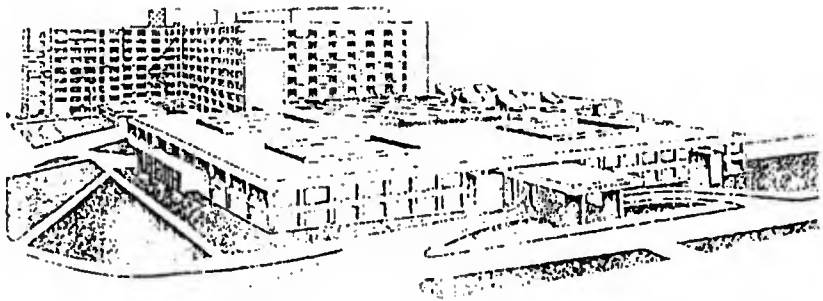
- Selected laser optical card WORM technology for enhanced security of data
- Software design based on object-oriented technologies
- Documentation based on DoD MIL-STD 2167A (tailored)
  - Requirements Specification
  - Preliminary and Detail Design
  - Test Plan
- Reviews
  - Requirements
  - Design
  - Acceptance Test



BENEFITS

dIgItaT™

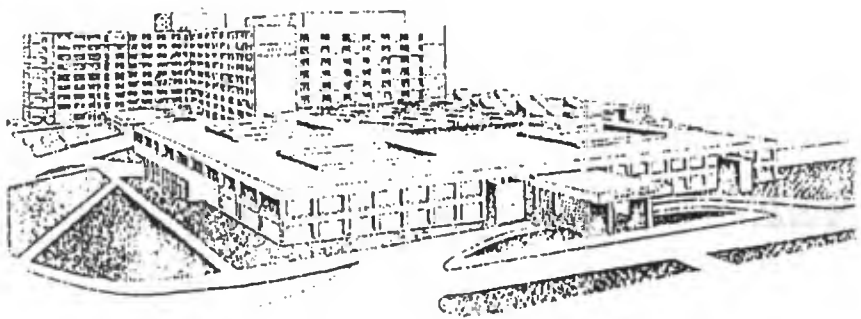
- Patient's medical history is available immediately
- Provide patient tracking
- Reduce patient waiting time
- Rapid deployment for military
- PCS/Emergencies - medical information available
- Circumvent many legal repercussions
- Improved forms readability



CONCLUSION

dgmtal™

- DOD world wide application
- Portability
- Pertinent medical information on patient card
- One step closer to Electronic Medical Record

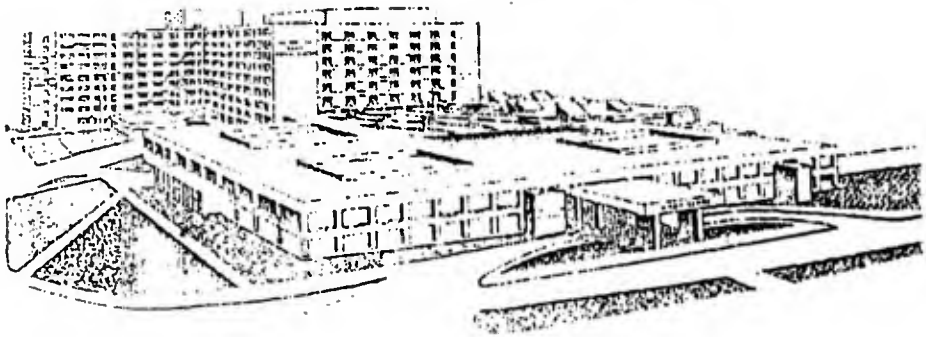


DEMONSTRATION

digital™

Visit WHMC, LaserCard Systems, and Digital at

Booth 31



THE OPTICAL MEMORY CARD—AT THE WEST LONDON HOSPITAL

This document provides a brief overview of a trial involving the use of the Optical Memory Card (OMC) for antenatal care at the West London Hospital.

Further information may be obtained from BT Tallis Consultancy at the address indicated below.

BACKGROUND

The West London Hospital Obstetrics Optical Memory Project (OOMP) started several years ago and was developed for antenatal care at that hospital. Over 1000 women were booked on the system and issued with Optical Memory Cards. These cards were used to store their medical records during their pregnancy and this initial phase was designed to test the technology and user acceptance before extending its use to the community. The success of Phase 1 led to a second phase, which commenced in May 1992.

PHASE 2

The principal objective of Phase 2 is to use the OMC system to help improve communications between the hospital team, the GP teams and District Midwives. The expectation is that improved communications between separate points of care will improve the delivery of that care and thus the clinical outcome. For this reason, Phase 2 is restricted to pregnant women who opt for shared care with delivery at the West London Hospital and whose OP is one of the six practices taking part in the trial.

Eleven personal computers (PCs) are connected on a network at the hospital, with two OMC reader/writers located at the booking desk and one in the ultrasound room. Six GP surgeries and a Midwives clinic have stand-alone PCs equipped with OMC reader/writers.

Before arrival at the hospital, brief details of each newly referred woman are entered into the computer system by a Booking Clerk. On her arrival, the woman has a booking interview with a Midwife during which per personal and medical details are keyed into the system. She will then be examined by a Doctor and have an ultrasound scan, with results of both being entered into the system.

Having completed her booking visit, the women included in the trial are given an OMC containing all the information recorded during that visit. On visiting her GP, the woman hands over her card and the data on it is used to update the GP system. The GP can thus see all entries made at the hospital, add further data, save this data to the card and hand it back to the woman.

In this manner, the OMC is used to transfer data between points of care and always contains the most up to date record of that care. At each visit, the computer checks to see if the information on the card is more up to date than its own file (and updates where appropriate) before the consultation commences. The information recorded on the system and the OMC includes: personal details, medical history, past obstetric history, booking investigations, booking examinations, regular examinations, early ultrasound scans, anomaly ultrasound scans, regular ultrasound scans, haematology tests, other investigations, birth care plan, antenatal admissions, additional notes and pregnancy risk factors.

For this trial, the OMC system is only used for antenatal care and excludes labour and delivery details. However, there is no reason why use of the OMC should not continue if funding to extend the scope of the trial were available.

Surprisingly, the loss of a card (or even forgetting to bring it) has proved a very rare event. Should a card be lost, the woman is asked to return to the last point of use, where the latest record is kept, to have a replacement card issued.

Phase 2 will end for new booking in May 1993, but all existing women will continue to use their cards for the duration of their pregnancy. The final end date is thus not determined but will be around October 1993.

PHASE 3

The West London Hospital recently closed down and the OOMP system was moved to the new Chelsea and Westminster hospital where it will continue to be used until the end of the trial. A new phase (Phase 3) is already under consideration and it is hoped that this will be extended to include additional hospitals and GP clinics in the district.

Being several years old, both the software and hardware are due for replacement and this will be one of the main changes for Phase 3. In particular, new software will permit more flexibility, easier use and provide additional features such as the

graphical display of medical data (eg blood pressure), warnings of tests which should be undertaken following certain input (eg a sickle cell test), a drugs database giving an indication of normal dosage, known side effects etc.

A paper on the West London Hospital trial was presented to the HealthCare Computing Conference '93 in Harrogate by medical staff from the hospital. Anyone attending the conference should have a copy of the proceedings. If you would like a copy, BT is in the process of obtaining permission to reproduce this paper and will forward a copy on request to the address below.

Phase two of the Chelsea and Westminster OMC project is nearing completion, with the analysis of results and project reports being the main outstanding items.

One main driver for the use of patient cards in the UK is the move towards shared care in the community. Medical care is currently in a state of transition from centralized care to shared care in the community, whereby patients are treated as customers of a service delivered within the community. In addition, care will be provided not just by the NHS, but other agencies (social services, private organizations etc). In general, patients will be visited by a range of different types of care rather than be asked to come to an appointed point of care. However, whilst this has many benefits, one major problem is the availability of up to date patient information at the point of care.

Furthermore, the move towards electronic patient data provides a possibility of using patient data pro-actively to provide better care, rather than just recording it passively. A key objective of phase three of the project is to use intelligent software that will act on data input, and provide appropriate feedback responses to ease diagnosis and help ensure that the clinician does not miss the significance of their input. In order to achieve this, it is essential that previous patient data is immediately available for comparison and calculation (eg weight change, blood pressure measurements, blood sugar levels, fetal growth).

The whole premise could be summed up as 'the better the information available and the more that information is used proactively to provide clinical feedback, the better the care provided.'

Thus by providing the patient with a simple means of carrying their own notes, the requirement of having *all* patient data *immediately* available at *any point of care* is elegantly achieved.

LASERCARD SYSTEMS CORPORATION,
MARKETING ADMINISTRATOR,
Moutain View, CA, January 19, 1994.

Ms. BERYL HOWELL,
Office of Sen. Patrick Leahy,
U.S. Senate, Washington, DC.

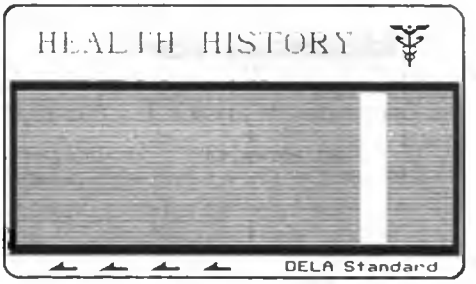
DEAR MS. HOWELL, Enclosed are the screen images from the Medical Applications demonstration program Richard Haddock demonstrated for the Senate Subcommittee on Technology and the Law on October 27, 1993.

The screen images were saved and imported into PhotoStyler® to convert into a black & white image (for better photo coping), and then printed. The images were not otherwise altered. The resolution of the images (photos, x-rays) were greatly reduced in this process and therefore are not representative of the Medical Applications program (color) screen resolution.

Sincerely,

EVE MCKAY,
Marketing Aministrator.

LaserCard

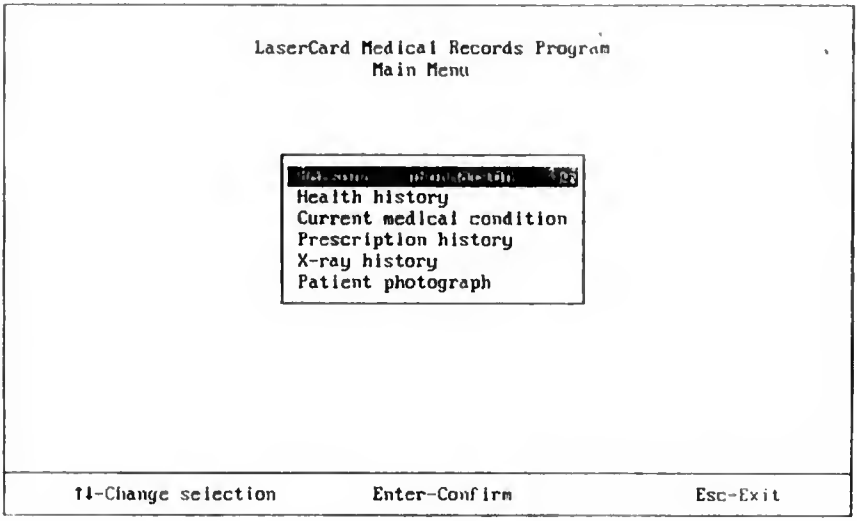


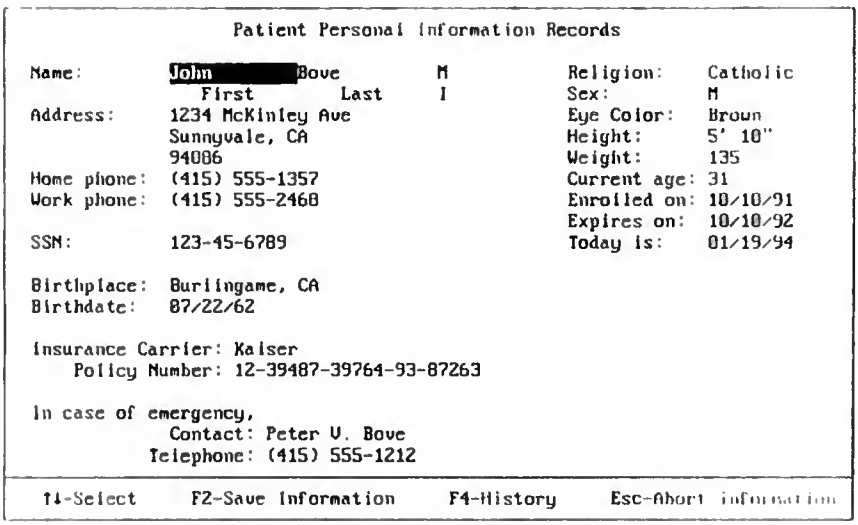
Emergency Medical Record Abstract

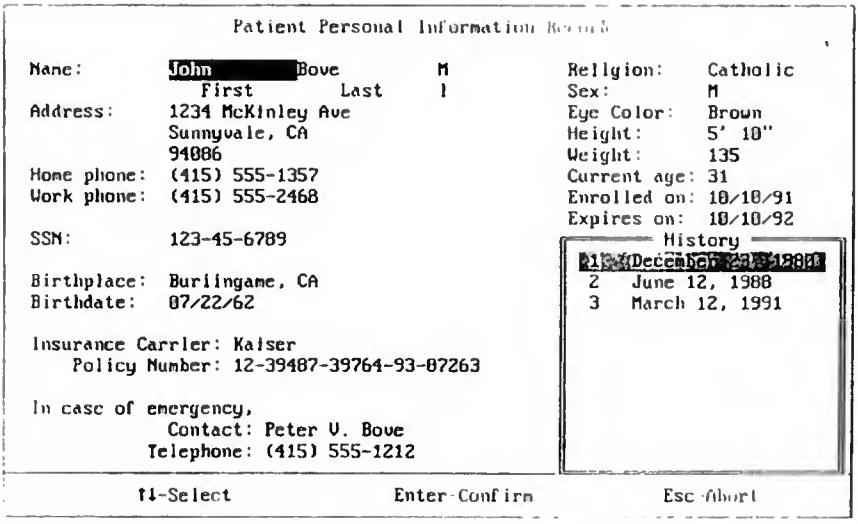
Emergency Information

Patient:	John M Bove	Sex:	M
		DOB:	07/22/62
Blood type:	O pos.	Age:	31
Allergies:	Pine needles	Contact:	Peter V. Bove
	Insect stings	Phone:	(415) 555-1212
	Flightless waterfowl	Relationship:	Father
	Alfalfa		
Conditions:	Asthma	Insurance:	Kaiser
	Heart murmur	Religion:	Catholic
	High cholesterol		
Height:	5' 10"	Eye color:	Brown
Weight:	135	Prosthetics:	None

Press P to print Press any other key for menu


LaserCard Medical Records Program
Main Menu
Health history
Current medical condition
Prescription history
X-ray history
Patient photograph
↑↓-Change selection
Enter-Confirm
Esc-Exit


Patient Personal Information Records
Name: John Bove M
First Last I
Address: 1234 McKinley Ave
Sunnyvale, CA
94086
Home phone: (415) 555-1357
Work phone: (415) 555-2468
SSN: 123-45-6789
Birthplace: Burlingame, CA
Birthdate: 07/22/62
Insurance Carrier: Kaiser
Policy Number: 12-39487-39764-93-87263
In case of emergency,
Contact: Peter V. Bove
Telephone: (415) 555-1212
Religion: Catholic
Sex: M
Eye Color: Brown
Height: 5' 10"
Weight: 135
Current age: 31
Enrolled on: 10/10/91
Expires on: 10/10/92
Today is: 01/19/94
↑↓-Select
F2-Save Information
F4-History
Esc-Abort information



Patient Personal Information Record

Name: John Bove M
First Last I

Address: 1234 McKinley Ave
Sunnyvale, CA
94086

Home phone: (415) 555-1357
Work phone: (415) 555-2468

SSN: 123-45-6789

Birthplace: Burlingame, CA
Birthdate: 07/22/62

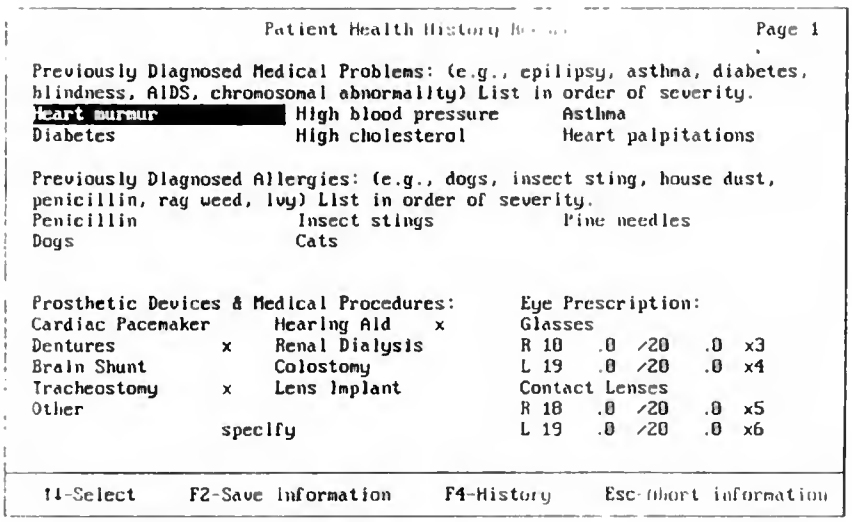
Insurance Carrier: Kaiser
Policy Number: 12-39487-39764-93-87263

In case of emergency,
Contact: Peter V. Bove
Telephone: (415) 555-1212

Religion: Catholic
Sex: M
Eye Color: Brown
Height: 5' 10"
Weight: 135
Current age: 31
Enrolled on: 10/10/91
Expires on: 10/10/92

History
1 December 23, 1988
2 June 12, 1988
3 March 12, 1991

↑↓-Select Enter-Confirm Esc-Abort



Patient Health History Record Page 1

Previously Diagnosed Medical Problems: (e.g., epilipsy, asthma, diabetes, blindness, AIDS, chromosomal abnormality) List in order of severity.

Heart murmur	High blood pressure	Asthma
Diabetes	High cholesterol	Heart palpitations

Previously Diagnosed Allergies: (e.g., dogs, insect sting, house dust, penicillin, rag weed, ivy) List in order of severity.

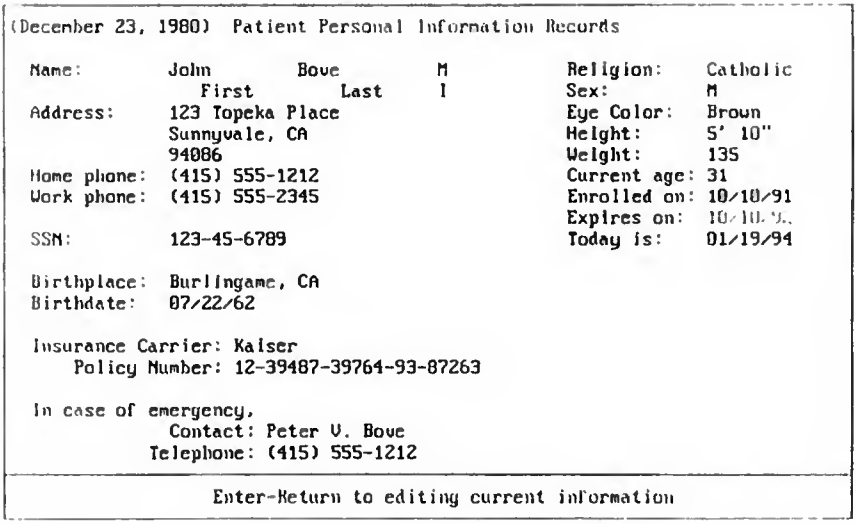
Penicillin	Insect stings	Pine needles
Dogs	Cats	

Prosthetic Devices & Medical Procedures:

Cardiac Pacemaker		Hearing Aid	x
Dentures	x	Renal Dialysis	
Brain Shunt		Colostomy	
Tracheostomy	x	Lens Implant	
Other			
	specify		

Eye Prescription:
Glasses
R 18 .0 /20 .0 x3
L 19 .0 /20 .0 x4
Contact Lenses
R 18 .0 /20 .0 x5
L 19 .0 /20 .0 x6

↑↓-Select F2-Save Information F4-History Esc-Abort Information



(December 23, 1980) Patient Personal Information Records

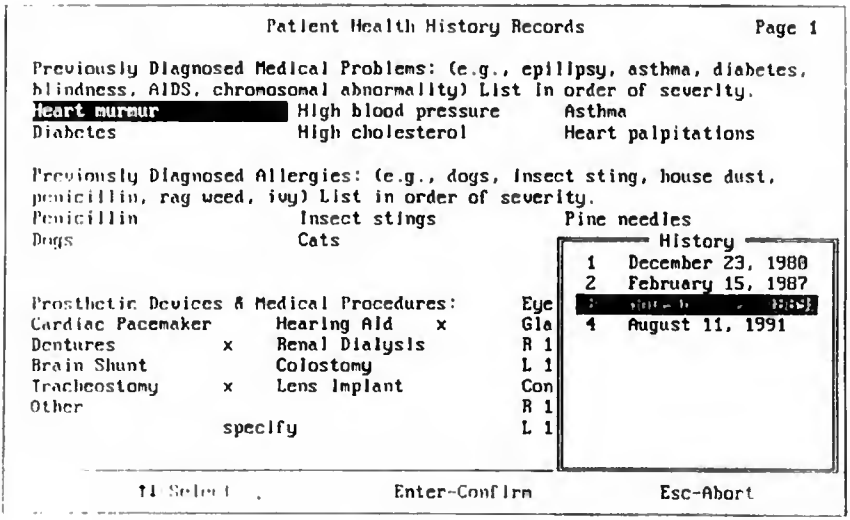
Name:	John	Bove	M	Religion:	Catholic
	First	Last	I	Sex:	M
Address:	123 Topeka Place			Eye Color:	Brown
	Sunnyvale, CA			Height:	5' 10"
	94086			Weight:	135
Home phone:	(415) 555-1212			Current age:	31
Work phone:	(415) 555-2345			Enrolled on:	10/10/91
				Expires on:	10/10/9[illegible]
SSN:	123-45-6789			Today is:	01/19/94

Birthplace: Burlingame, CA
Birthdate: 07/22/62

Insurance Carrier: Kaiser
Policy Number: 12-39487-39764-93-87263

In case of emergency,
Contact: Peter V. Bove
Telephone: (415) 555-1212

Enter-Return to editing current information



Patient Health History Records Page 1

Previously Diagnosed Medical Problems: (e.g., epilipsy, asthma, diabetes, blindness, AIDS, chromosomal abnormality) List in order of severity.

Heart murmur	High blood pressure	Asthma
Diabetes	High cholesterol	Heart palpitations

Previously Diagnosed Allergies: (e.g., dogs, insect sting, house dust, penicillin, rag weed, ivy) List in order of severity.

Penicillin	Insect stings	Pine needles
Dogs	Cats	

History

1 December 23, 1980
2 February 15, 1987
3 [illegible]
4 August 11, 1991

Prosthetic Devices & Medical Procedures:				Eye
Cardiac Pacemaker		Hearing Aid	x	Gla
Dentures	x	Renal Dialysis		R 1
Brain Shunt		Colostomy		L 1
Tracheostomy	x	Lens Implant		Con
Other				R 1
	specify			L 1

↑↓ Select . Enter-Confirm Esc-Abort

(November 2, 1989) Patient Health Hi... Page 1

Previously Diagnosed Medical Problems: (e.g., epilipsy, asthma, diabetes, blindness, AIDS, chromosomal abnormality) List in order of severity.

Heart murmur	High blood pressure	Asthma
Diabetes	High cholesterol	

Previously Diagnosed Allergies: (e.g., dogs, insect sting, house dust, penicillin, rag weed, ivy) List in order of severity.

Penicillin	Insect stings	Pine needles

Prosthetic Devices & Medical Procedures:				Eye Prescription:				
Cardiac Pacemaker		Hearing Aid	x	Glasses				
Dentures	x	Renal Dialysis		R 20	.0	/20	.0	x3
Brain Shunt		Colostomy		L 20	.0	/20	.0	x4
Tracheostomy	x	Lens Implant		Contact Lenses				
Other				R 20	.0	/20	.0	x5
	specify			L 20	.0	/20	.0	x6

PgUp-Previous page PgDn-Next page Enter-Return to current information

Prescription 2 of 2

LaserCard Medical Records Program
Prescription History

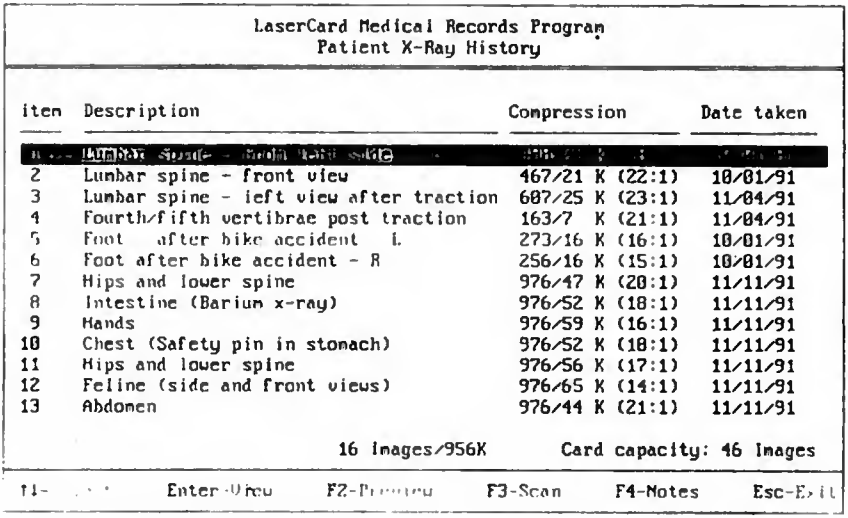
Physician: Dr. Paul Johnson
Hospital/Clinic: Chope Medical Center
Phone: (415) 555-1212

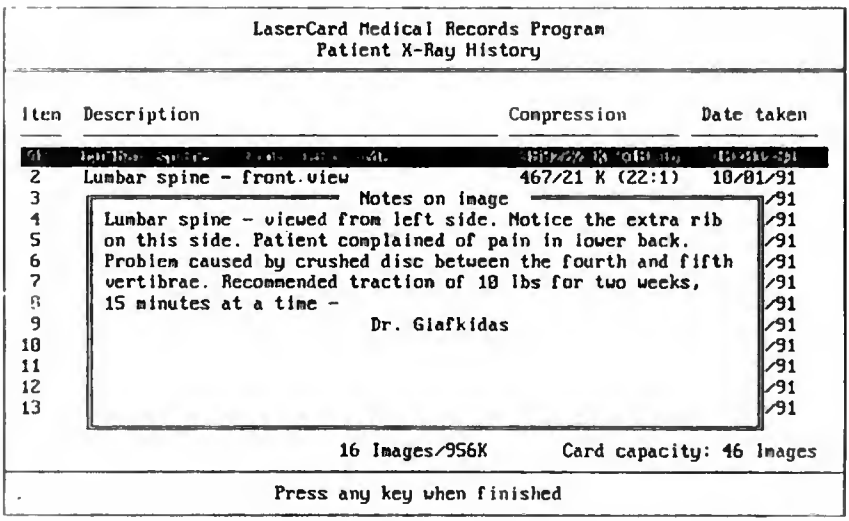
Drug: Ampicillin (25mg)
Prescribed for: Stomach flu
Amount: 30 Refills: 2
Date prescribed: 10/10/91 Fill before: 11/10/91

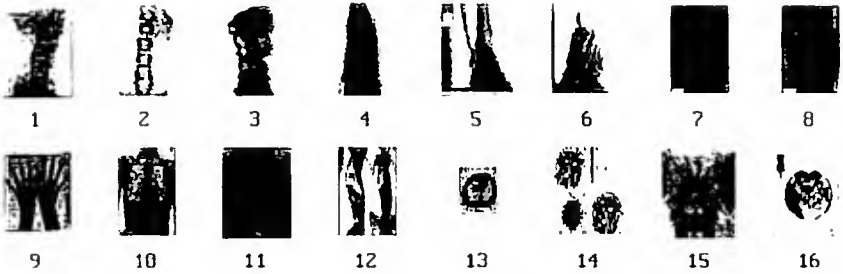
Instructions: Take one before each meal
Use all the pills prescribed

Pharmacist: Garry Kornblum
Pharmacy: Payless Drug Location: Sonora, CA
Date filled: 10/23/91 Refill: 1
Amount: 30 Brand: UpJohn

↑↓-Select prescription ↔-Select pharmacy update Esc-Exit


LaserCard Medical Records Program
Patient X-Ray History
Item Description Compression Date taken
2 Lumbar spine - front view 467/21 K (22:1) 10/01/91
3 Lumbar spine - left view after traction 607/25 K (23:1) 11/04/91
4 Fourth/fifth vertibrae post traction 163/7 K (21:1) 11/04/91
5 Foot after bike accident L 273/16 K (16:1) 10/01/91
6 Foot after bike accident - R 256/16 K (15:1) 10/01/91
7 Hips and lower spine 976/47 K (20:1) 11/11/91
8 Intestine (Barium x-ray) 976/52 K (18:1) 11/11/91
9 Hands 976/59 K (16:1) 11/11/91
10 Chest (Safety pin in stomach) 976/52 K (18:1) 11/11/91
11 Hips and lower spine 976/56 K (17:1) 11/11/91
12 Feline (side and front views) 976/65 K (14:1) 11/11/91
13 Abdomen 976/44 K (21:1) 11/11/91
16 Images/956K Card capacity: 46 Images
Enter-View F3-Scan F4-Notes Esc-Exit


LaserCard Medical Records Program
Patient X-Ray History
Item Description Compression Date taken
2 Lumbar spine - front view 467/21 K (22:1) 10/01/91
Notes on image
Lumbar spine - viewed from left side. Notice the extra rib
on this side. Patient complained of pain in lower back.
Problem caused by crushed disc between the fourth and fifth
vertibrae. Recommended traction of 10 lbs for two weeks,
15 minutes at a time -
Dr. Glafkidas
16 Images/956K Card capacity: 46 Images
Press any key when finished



· · Change selection Enter-View Esc Exit


L

LaserCard Medical Records Program
Patient Photo Identification

Name: John M Bove
Age: 31
Sex: M

Height: 5' 10"
Weight: 135
Eye color: Brown
DOB: 07/22/62

Press a key when finished

Senator LEAHY. Drs. Hope, does anybody want to add anything further on this one?

Dr. SHERMAN HOPE. I think you touched very correctly on some of the problems, that the medical profession needs the cards to treat the patients, but we do not want it abused, and yet if we make the information available in almost any manner, and including his is great, to the doctors, we still have the unscrupulous people like the employer that says, "I will not hire someone who checked AIDS positive." We still need legislation to protect them from having to furnish this information to that employer.

As you stated, if we have the card and it has the patient's medical information on it that the doctors, the medical profession needs to know but that employer does not, then the law, I would think, might be aimed at saying it is illegal to demand such a card from the patient, from the prospective employee.

Senator LEAHY. I think we are going to need to do something like that. I might ask, gentlemen, if I could submit further questions for the record to you. The reason for this is that we are going in about ½ an hour to a series of votes. Then a number of us who are involved in this health care legislation are going directly from there to a meeting with the President and the First Lady over in Statuary Hall, where they are going to present their proposals to the Congress. If I might send you follow-up questions, it would help.

I would also ask if, after we finish, you could just print out some sample records. Work with the staff to get a better idea of what we want. I would like to keep it in the permanent record of this testimony.

Dr. SHERMAN HOPE. I have brought actually a set of patient records which was one day's real life work.

Senator LEAHY. Great.

Dr. SHERMAN HOPE. It is in a folder that—that was an awfully busy day because my physician assistant was out.

[Laughter.]

Senator LEAHY. OK. Thank you.

Gentlemen, thank you very much.

Mr. Rothfeder, thank you very much for coming down. In going over your writings, I looked at one of the notes we had about the freelance artist who had incorrect information in his medical record that he was HIV positive. If I recall correctly, that record then got circulated widely and he started wondering why he kept getting turned down for health insurance.

Mr. ROTHFEDER. Yes.

Senator LEAHY. It does not take any great imagination to figure that you could be turned down for jobs, you could be turned down for any number of things, depending upon what was in your medical record, even if it was put in erroneously. So you go ahead, I do not want to put words in your mouth. I will let you start.

STATEMENT OF JEFFREY ROTHFEDER, SENIOR EDITOR, BLOOMBERG BUSINESS NEWS, AUTHOR OF "PRIVACY FOR SALE"

Mr. ROTHFEDER. Those were pretty much exactly my words.

In researching Privacy for Sale and in researching privacy in general, which I have done for the last 5 or 6 years, computer

databanks and privacy, in talking to loads and loads of just plain folks out there, medical records are probably the most important things that they own and that they want to keep private, because if the wrong information gets out or even if correct information gets out, if it is information that is looked at wrongly or inappropriately by society, it can ruin your reputation. You could lose chances to get jobs, you can get fired from jobs you already have. You could get locked out of insurance. Your kids could be harassed at school. And all of this has gone on. You even have to make decisions that the insurance companies make you make.

One problem, you raised the question with them about whether if we set up a smart card system, even with all the controls, will eventually everyone else be looking at it, that's exactly what happens with data banks. I mean, once you have a data bank in place, information will flow to any place it can flow. Once you open up new outlets for that data bank, if you have 1,000 outlets nationwide, information is going to flow to every one of those outlets and eventually there are going to be new arteries, because more people are going to get access to it at each site.

The Medical Information Bureau, which you were raising in terms of the gentleman who got wrongly listed that he had AIDS, that was a Medical Information Bureau record. Now, that is run by the insurance companies. That is a consortium of insurance companies. So there are thousands and thousands of brokers that have on-line access to medical information bureau records.

What happens is, if a broker anywhere wants to look up, let's say your record, and see what your listing is on MIB, they can look at it.

Senator LEAHY. What is MIB?

Mr. ROTHFEDER. The Medical Information Bureau.

Senator LEAHY. Oh, yes.

Mr. ROTHFEDER. And at that point, if they do not want to keep that private, and as you know, there are no Federal laws protecting medical privacy, it is just purely an ethical thing, they do not have to keep it private and they can whisper it at some local club meeting.

That did happen in the case of a gentleman who lived in a small town in upstate New York. He did have AIDS. It was on his MIB record, and some local insurance programs just looking around for marketing purposes, to see what people in the area need in terms of insurance needs, found this guy, found that he had AIDS. He was a prominent local businessman, just a small town. He went to the Kiwanis Club meeting that night, this broker, and told everybody. By the next morning, this man, who was trying to keep it secret that he had AIDS, was being looked at differently as he walked down the street. His whole life was changed forever.

Add onto that an issue, for instance, like genetic records, as an example. Now, you know, as technology is improved, we tell people, before you have a child, before you conceive, take genetic tests so that we see what kind of offspring you're going to have. Some people have done that and find out, like there was one couple in the Midwest, a farm couple, who took a genetic test, both found out they were carriers for a terminal disease, if a child was born from them it would be terminal. Now, only 25 percent of their offspring

would have this disease. Nevertheless, just because they took that genetic test, that also got on a databank. The insurance company found out about it and said, "We're not giving you insurance any more for pregnancy," just because they took a genetic test.

They said, "Well, didn't we do the appropriate thing? We did what the hospitals and the doctors told us to do."

Senator LEAHY. They would have been better off not to take the test.

Mr. ROTHFEDER. Absolutely. Don't provide more information is part of the problem. So they even had to go so far, because they can't afford to have a baby if they don't have insurance for it, they even have to go so far as to beg the insurance company to say that, "We will sign up in writing, if tests show that the offspring has this disease, we will abort the baby," which is against their religious beliefs, and even then the insurance company said no, they just won't give them that kind of coverage.

Then there have been cases that I have run into of people, again with genetic tests, who were predisposed to, let's say, a muscular condition. One woman I ran into like this, she didn't have any signs of the condition right now and if she got it, it would probably be 30 years hence. Well, she still couldn't get a job because—she wanted to get a job working in warehouses and every place she went, they said, "Well, you're going to get this muscular condition in 2 years; we're going to have to be paying for your insurance bills and put you on disability for the rest of your life, so we're not hiring you."

So again, there is another case of taking a genetic test and getting it put against you.

What all of this says, of course, is that once you create information, it just continues to flow into places that want to see it and feel that they can use it in some way. One quote I have in my book is that we have become a data-driven society and not a values-driven society, and that is exactly what it is. It is data, it is what your electronic profile says about you, that says so much more than who you are as an individual and what your background is.

If you take it to the extent of—I think employers, though, is one of the big areas. You know, you're raising that with the smart card. Already that is happening in terms of employers getting access to that information, and I guarantee you that if the smart card system was available, they will make sure to get access to that as well.

I think 70 percent of the employers in the United States already run or partially run their own insurance program, their re-insurance programs, and because of that, because they have a much more vested interest than they did in the past, one of the things they are doing is cosying up to the insurance companies and saying, "Well, we would like to know what everybody on our late shift has been going to the doctor for, mainly because we are trying to do studies on why people are out of work a lot." I mean, "Do they have backaches, you know, so we can help them ergonomically."

Well, unfortunately, what has been happening is, some people have gotten fired because they went to alcoholic out-treatment centers, or for mental health centers, and so on. So——

Senator LEAHY. In that regard, if I can interrupt a minute, we are going back to the problem that we have seen, for example, in government. We have had people who have been in certain types of high-stress jobs in government, law enforcement, for example, and who have had a problem with alcohol. As a former prosecutor, I saw instances of police officers under my jurisdiction, urged to go for AA or whatever might work for them. They were terrified of doing that because going for the help, which would make them better police officers and less of a risk, automatically put their jobs at risk.

They are in a Catch-22. If they seek the help, they might be out. The same situation occurs with new technologies.

Mr. ROTHFEDER. Yes.

Senator LEAHY. Where you cannot seek help without suddenly being out. Now, we claim to be more enlightened in government, more enlightened in business, and now we seek to ask them to go there. But you know and I know, when you start getting up into the more ratified promotions——

Mr. ROTHFEDER. Right.

Senator LEAHY. And you have four people, all on the record look pretty much the same. But you run that medical card through and you see, that 5 years ago one had a problem and was in detox, so on and so forth. That person may not have touched a drink since then, but now we only have three of these people we have to worry about because he or she is out.

Mr. ROTHFEDER. Yes, that is it.

Senator LEAHY. And that is what worries me. How do I go and seek the help?

Mr. ROTHFEDER. Right.

Senator LEAHY. Or a member of your family has a problem, and that problem is on your family record. Or, you have a member of the family with a problem, but one of the suggested treatments is that the whole family go to counseling to deal, for example, with the kid who has been out stealing cars, or whatever.

Mr. ROTHFEDER. The problem is, the employees wouldn't know about this being used against them. That is the whole other issue. You know, if you do not get that promotion, well, it is just you did not get that promotion. They are not going to tell you, "Because we found this on your record," opening up liable to some kind of law suit. And also, obviously, in terms of not getting a job.

The other problem, by the way, even when we sign up for jobs now and we sign at the bottom of the form that you can do a background check on us, at this point, in terms of because there are no laws protecting any of this, that is an open-ended background check. And with smart card, it is going to get even more open-ended, because that means that 5 years from now, an employer literally can because you signed 5 years ago that we can do background checks on you for employment purposes.

"Well, we are considering you for promotion. We want to check on you now, and by the way, part of it is a medical check."

Senator LEAHY. With all due respect to the members of the Fourth Estate who are here, to what extent can the press go bouncing around here? One of the people, we were unable to have testify because of a scheduling problem, but whom we had talked with

earlier was Mrs. Moutassamy Ashe. Arthur Ashe was a person I admired greatly, and I remember his very painful press conference saying, the press is disclosing that he had AIDS from a blood transfusion when he had open-heart surgery, and he had to go public with that.

I thought to myself, what a terrible tragedy for him, his wife, and his child anyway, and then to have to share it with hundreds of millions of people worldwide. There are things that should be allowed to be private. As I have said, I come from a State where we value our privacy, value it greatly.

I cannot think of anything I would less rather see, or my family or my friends or my staff or anybody else, to have their medical records automatically available to anybody who wanted them.

Mr. ROTHFEDER. Well, that is the problem. And, you know, you mentioned the press. One of the interesting things, of course, is that the press has become much more aggressive, obviously, in terms of the kinds of information they seek out. I am part of the press and I know how that happens. You know, you are all fighting for the same story and somebody gets some kind of thing about somebody, especially a politician or celebrity, it is going to get out there one way or the other. Your organization might hold it back just so long, but after a while, someone is going to do it and it is going to get out.

Of course, politicians use it against each other, as well, which has been a whole other problem.

Senator LEAHY. That shouldn't be allowed, either.

Mr. ROTHFEDER. Yes. So, I mean, one of the interesting things I have learned in doing this book and in researching this is most of the letters I received from people are people asking me how to get information about other people, because as you probably know, I accessed Dan Quayle's credit report to prove you can do that. That was 3 years ago already, and ever since that came out——

Senator LEAHY. Dan sends his best.

Mr. ROTHFEDER. I'm sure he does. [Laughter.]

Ever since that came out and the availability of it has been shown, I get loads of letters from people saying, you know, "I abhor the loss of privacy. However, I just have to find out something about my girlfriend's ex-boyfriend and would you tell me how to find this databank."

So the problem is, we are gossips by nature, unfortunately, and once you start opening up data channels, it's just going to get worse and worse. Which is what really worries me about the whole medical privacy aspect.

Senator LEAHY. Well, Mr. Rothfeder, let me ask you about this. You showed how you could break in and get that. Over the years, I have had some remarkable people testify before the Subcommittee from hackers on through, who have the ability to get into major sources of information. You know how fast it can spread. Look at Internet, how that has expanded in just the last 2 or 3 years.

I would have to assume, at least with today's technology, it would be impossible to make an impregnable system.

Mr. ROTHFEDER. Yes.

Senator LEAHY. Let's start from that for the moment, and I think you would probably agree with me on that. But I would assume

there are at least a couple of things we could do. One, at least to the extent that technology allows, have a data trail showing whoever entered or at least where the entry came from.

Mr. ROTHFEDER. Yes.

Senator LEAHY. Where the source was and that the record was entered.

Mr. ROTHFEDER. Right.

Senator LEAHY. So if we can show that the file was entered and probably be able to identify who entered it, that is Step 1.

Mr. ROTHFEDER. Yes.

Senator LEAHY. But then, if you have that, have some very strict laws about wrongfully accessing a medical record, and make it a crime.

Mr. ROTHFEDER. Yes.

Senator LEAHY. Make it a crime whether you, as a reporter, or I, as someone who may be running in a tough election, or as an employer or as a busybody neighbor or anything else, it doesn't make any difference, we go in to the medical record wrongfully, we can get nailed for it. I mean, isn't that a bottom line that you have to have in any legislation?

Mr. ROTHFEDER. Yes, and I would add one other thing. I would also encrypt the data from one site to the next so that it is only de-encrypted at the site where it is being looked at. Because often hackers enter in the middle of the trail, so you are not going to know they came in through this file or through that file.

The audit trail, though, your first point, is absolutely important. That is almost not done, as you probably know. Phone companies don't do it; banks don't do it; hospitals don't do it; and that's why—and credit bureaus don't do it—which is why you can access people's records without anybody even knowing you accessed it.

But again, the encryption is important because this way it stops somebody from accessing in the middle of the trail.

The third side, though, the law, is very important because—and the law has got to be really specific about who is allowed to look at the information and under what circumstances, because as you probably know, one of the real problems with the Fair Credit Reporting Act, which supposedly protects credit reports, and one reason why I could access Dan Quayle's credit report is, they list a few places like somebody you're going to do business with, landlords and so on, and then it says, the last thing is, anyone with a, "permissible business purpose," which is the hugest loophole. You can drive a Mack truck through a loophole like that. Because I could say my permissible business purpose is I wanted to show what you could do in order to write a book about it, and I've gotten away with it on that basis, and others have gotten away with it because they are going to do some kind of car deal or something like that.

Senator LEAHY. Since I first came down here after being elected to the Senate, we have always had a listed home phone number. This is something I always worry about saying in public meetings like this because I end up getting a bunch of phone calls. But for about 6 months after we moved into Northern Virginia from Vermont when I first went in the Senate, we got calls for Patrick Leahy from irate former girlfriends, from people who had bad checks, car dealers whose cars had never been returned. All were

calling and screaming that, "Now we've finally got your number." I found this was going into credit records and everything else. Well, it was obviously an entirely different Patrick Leahy, who was someone about 20 years older than I was at the time and who had somewhat different ideas about paying bills than I have.

Fortunately, I had a different middle initial and that probably straightened the thing out, but it was kind of a hairy situation for a while. But think how much more could be done on something like this, where you really set out to do it.

Mr. ROTHFEDER. Yes, exactly. And with medical records, again, just think about those kinds of mistakes. We pointed out the one with AIDS, for instance. You are right. The middle initial is all that is separating two names. Well, then, you're going to get lost in it.

The other thing, by the way——

Senator LEAHY. But you may not know it. You see, this is the problem. It took us an awful long time to figure out what the heck was going on, and only because we got one of the people who called to stay on the phone long enough to quiet them down and finally convince them I was someone entirely different, and only because they finally realized that the person they knew probably would not be a U.S. Senator. [Laughter.]

I don't know, maybe we're giving the Senate too much credit. [Laughter.]

But the point is it took that long to unravel the thing, and we are talking about something nowhere near as complicated. I mean, I can just see the man or woman who thinks, "I was qualified for that promotion and I can't figure out why in heaven's name I didn't get it."

Mr. ROTHFEDER. Exactly. For instance, the gentleman that we talked about who didn't have AIDS but it said he did on his record could not get that expunged from his record, no matter how hard he tried. Every time he thought he got rid of it, it bounced right back at him again. He would go do something else and it would come back.

Again, which is the problem with data. Data has a life of its own. You also don't know how many places it has traveled to beforehand. I mean, let's say 20 insurance companies have picked up the fact that you have AIDS through MIB, through the Medical Information Bureau records, and then you finally get MIB to take it off the record. Well, you've still got 20 insurance companies that know about it and they're going to tell other people about it as the files get transferred.

Senator LEAHY. But then on the flip side, though, is what Dr. Hope was saying. You've got rural clinics big city areas where there is a great value in being able to carry medical records around. Certainly there is a value in keeping costs down if, as you go from one place to another or if you are suddenly taken ill on a trip or something like that. If you have your medical history on a card, you don't have to spend 2 hours doing the background. Or as Mr. Haddock was showing, you come in and you are having a real difficult pain, they can pull up your x-rays and say, "well, yes, but you had surgery three times on your spine," or whatever. They see the x-rays right there. Obviously, you're going to save a great deal of

time and money and, in some instances, it would be very easy to think of how you ultimately are saving the person's life in an emergency situation.

So there is certainly a value to it. I doubt if Dr. Hope could carry out his practice as well as he does and make medicine available to a lot of people if he didn't have the immediate access to these records.

Mr. ROTHFEDER. You have to be careful about just using technology for technology's sake. I don't know if he mentioned it, but the medical record itself has grown in terms of what kind of information is on a medical record from almost nothing, 100 years ago, to everything that you've ever said or done in your life, virtually. If you go skydiving, it is on your medical record now.

And so what happens is that if you do stop in some rural town, let's say you do have a heart condition and you're in some town, traveling through, and you need care there. Well, that would make sense to have that on your medical record because that is a primary condition in your life. But do you have to—look, we were talking about before the fact that you went in for alcohol treatment 7 years ago. Does that have to travel with you forever?

Senator LEAHY. That also goes to what Mr. Haddock was saying earlier about having access level A, B, or C. My expression, not his.

Mr. ROTHFEDER. Yes.

Senator LEAHY. But certain that the patient can say, well, fine, but that is only accessible by me.

Mr. ROTHFEDER. Yes, that would make a certain amount of sense. But it has to be broad enough also, because one of the problems now is a lot of places won't list that you have AIDS, for instance, so everybody knows when something isn't listed or it says "Record available only if you are authorized," everybody assumes you have AIDS at that point.

Senator LEAHY. And you also have in hospitals certain things on the patient talking about techniques of care or——

Mr. ROTHFEDER. Right, exactly.

Senator LEAHY. Or protection in care.

Mr. ROTHFEDER. Exactly. So I mean yes, I think that would be one way of doing it, though, separating out what should be carried with an individual or not. Unfortunately, if you look at the growth of data banks, everything gets thrown in there.

One of the problems with data banks, of course, is they are free. Once you have opened them up, the storage is there. You just keep adding stuff to it and dumping stuff into it, which is what has happened with credit bureaus, financial data banks, medical records, as well.

So given that opportunity to add to it, I just have a fear that everything is going to end up in there.

Senator LEAHY. Arlen?

Senator SPECTER. Thank you very much, Mr. Chairman. I think that your convening these hearings has an extremely important purpose one which is going to require a tremendous amount of study as we move to changes in our national healthcare delivery system.

A question which comes to my mind is whether the system ought to be constructed so that the individual has an opportunity to re-

move items from the records, having a judgment as to what he or she may wish to maintain totally private and evaluate what ought to be available. I took a look at a little card which the attending physician gave to me which lists some factors on my health card, and I think it might be worth exploring whether it would be possible to have an individual opt to carry something on their person which would give the critical data, so that it does not have to be available on computers.

Mr. ROTHFEDER. Yes.

Senator SPECTER. In this day and age, nothing is secret. It is something I learned a long time ago, when I was in another profession. Senator Leahy and I shared the profession of questionable reputability of being prosecuting attorneys.

Senator LEAHY. We were the front line of democracy.

Senator SPECTER. Maybe also the rear line of democracy. But that experience showed me how difficult it was to keep anything secret, and private records really need not be in the public domain or subject thereto.

Another question which is of concern to me is what this board is going to do on secrecy and confidentiality, which I have seen in President Clinton's initial 239-page report. I read that report and was struck with the 77 new boards and agencies which were created and the additional tasks given to 54 additional existing agencies for a total of 131 new bureaus, boards, commissions, et cetera, which were going to take up these questions.

I am anxious to see in the next hour the 1500 pages which I'm going to let Senator Leahy summarize for me this afternoon.

Senator LEAHY. Have you voted on this?

Senator SPECTER. No, I haven't voted, and I'm about to conclude. But I raise that question because we're going to have to make sure, to the extent that the Congress can, that there are not more complications than necessary.

I regret my late arrival, but I don't have to explain to the ladies and gentlemen assembled here what our competing pressures are, and I wanted to be present to at least thank the Chairman for convening the meeting and express those preliminary views.

Senator LEAHY. I should also note that Senator Specter is one who has been very concerned on these privacy issues. We are trying to work out the best way to do this, help with medical care, help with emergency situations, help people like Dr. Hope and others, and also protect our privacy.

We are going to recess now, subject to the call of the Chair, but I intend to have, Arlen, a lot of other experts come in on this. I think as we go forward with any type of a national health care plan, whatever it might be, you know and I know that there is, with electronic data streams, going to be more and more access to records. There are going to be more and more records kept, and how do we keep them private?

Senator SPECTER. Well, I think it is very important and we will have to pursue it. We will know better after we see the details of the legislation.

[Prepared statement of Senator Specter follows:]

PREPARED STATEMENT OF SENATOR ARLEN SPECTER

Mr. Chairman, I want to thank you for holding this hearing on the privacy concerns in health care and specifically the manner in which President Clinton's proposed Health Security Act treats these concerns.

The issue of privacy is a critical one on which you have been a leader during your terms in the Senate. There is no more important privacy issue facing us today than the security of health care records, especially as Congress debates comprehensive health care reform.

When anyone seeks medical treatment, we do so with the sense that the information the health care provider receives or learns will be kept confidential. Patients do not expect that such information will be made public without their express authorization. Yet, there are few State or Federal laws protecting personal health care information from unauthorized release. As the Subcommittee will hear, however, the unauthorized release of such information is not an unusual problem.

I have several concerns with the President's bill. First of all, I note that the President's bill would establish 14 new government entities and expand 8 existing government entities to deal with issues of privacy. While I agree with the President's goal of providing comprehensive health care to all Americans, I do not believe it is necessary to establish 105 new entities, as the President proposes in his Health Security Act, to address the problems we confront in our health care system. I do not believe we need big government to address privacy issues.

Of equal concern, however, is the fact that under President Clinton's bill, the Administration does not have to promulgate regulations on the protection of patients' privacy interests in their personal health information under the Health Security Act for two years after enactment. A third year will go by before the National Health Board set up under the Act has to forward recommendations to Congress on comprehensive legislation to protect all medical information, including that which predates enactment of the Act.

I believe that privacy issues surrounding personal health information should be dealt with on a shorter time line. I do not know why we cannot deal with the issue of privacy at the same time we deal with the other issues of health care reform. Nonetheless, I look forward to working with the Chairman and other interested parties on the important privacy issues as the Senate considers health care reform.

Senator LEAHY. Thank you.

The subcommittee will stand in recess.

[Whereupon, at 9:54 a.m., the Subcommittee recessed, subject to the call of the Chair.]

HIGH-TECH PRIVACY ISSUES IN HEALTH CARE

THURSDAY, JANUARY 27, 1994

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:42 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, chairman of the subcommittee, presiding.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Good morning. I apologize for the delay. Our 10:00 vote became a 10:15 vote; our 10:15 vote became a 10:35 vote, as you could tell—those who are familiar with the bells and whistles here—and that is why we were delayed. I apologize to the witnesses.

Congresswoman, I am delighted you are here. I was just explaining how fouled up we got with votes, the time for which suddenly got changed. But I am sure with your own experience in the other body, you know how that can happen.

Ms. VELAZQUEZ. I understand.

Senator LEAHY. President Clinton's Health Security Act has taken a bold step in reforming our health care system and I applaud him for that. But it also raises a lot of questions. We are going to discuss one aspect of the Health Security Act that goes beyond the new health care jargon. It affects each of us in a very personal way.

We are going to talk about a part of the health care act that is very personal to all of us. It is a national computerized health care network. That network is going to have basic information on every single one of us. My concern and the focus of this hearing is safeguarding the personal privacy of all Americans with regard to their medical care.

The legislation pending before the Congress uses technology aggressively. We have to. That is the only way we are going to achieve the kind of savings we need. And it builds on the kind of piecemeal efforts of different parts of this country to have electronic data banks and use technology in a way that saves money.

But before we go too far, I want people to look at the human face of this. I think we are very fortunate that Congresswoman Velazquez is going to talk with us. The Congresswoman will discuss the trauma of having personal medical information disclosed

publicly. Congresswoman, I applaud you for being willing to do this. Hers is a compelling case, but unfortunately—I am sure she would agree—it is not an isolated one.

During the past few weeks I have had a number of conversations with Jeanne Ashe on this subject. In his autobiography, Days of Grace, Arthur Ashe wrote about how he and his wife Jeanne learned in 1988 that he had contracted AIDS during a heart operation. Now Arthur Ashe was not only a great athlete, and an activist, and a scholar, and a man I admired greatly, but he was also a husband, and a father, and a private person. And tragically, he ended up having the remaining days of his life in the glare of public knowledge of his battle with AIDS.

In his case, he was forced to confirm his condition after the press got a tip about his medical condition. It meant that somebody took his personal medical information, called the press and said, "guess what is in here?" His family is still feeling the effect of this intrusion into their privacy.

Mrs. Ashe was going to testify, but I am sure you understand that even now as we approach the anniversary of his death, she chose to maintain the privacy she has left. I talked to her earlier this week. She said she would prefer not to appear and I am certainly respectful of her decision. My thoughts are with her and her daughter.

But we should learn from their experience. Nobody else should have to bear this kind of intrusion. It is not a question anymore of knowing just where the papers are about you, but wondering where little megabytes of medical information are. That information might not even be in the hospital or in the doctor's office you went to for treatment, but might be somewhere 1,000 miles away in somebody else's data bank. We have to be concerned about this.

In October, I had a hearing at which we saw various kinds of medical cards like the ones I am holding. This one says Hillary Rodham Clinton on it, but I do not believe that really is hers. I applaud my staff for somehow getting past security at the White House and getting this one. [Laughter.]

But these kind of cards have enormous amounts of information on them. We saw one card which looked like a little credit card. But put that card into the computer and it had enough information on it that if all the information were printed on paper, it would take up a filing cabinet the size of the whole witness table here. It had color photographs, black and white photographs, x-rays, handwritten notes, contained voice data if need be, and everything.

That is wonderful. It means that treatment can be expedited, money can be saved, we can know instantly where the necessary medical information is. But any time anybody goes into the hospital and hands over that card, it is possible for that information to go into a data stream somewhere. And I do not know, if that happens, whether anybody can tap into that, and the information we consider private, can be released, because what can happen in paper records can certainly happen in computer records.

Congresswoman, I have talked long enough. You are really the one that could tell us what happened. I have read your statement. It is a very powerful one. I applaud you—I really applaud you for being willing to be here, and the forum is yours.

STATEMENT OF NYDIA VELAZQUEZ, A MEMBER IN CONGRESS FROM THE STATE OF NEW YORK

Ms. VELAZQUEZ. Thank you. Good morning, Mr. Chairman. I would like to thank you, Mr. Chairman, for convening this very important hearing and for giving me the opportunity to testify. Unfortunately, due to the Democratic Issues Conference, I must depart before the end of the hearing. However, I will be happy to take questions immediately after my testimony.

Let me begin by stating that the only reason I have the strength to come before you today and discuss this very difficult, personal experience is because of the outpouring of love and support from my friends and constituents since its occurrence. I am indebted to them for standing behind me in my hour of need.

Mr. Chairman, technology is a double-edged sword. It provides us with more efficient ways to store and disseminate information, but it also poses significant problems in controlling access to sensitive data. As policymakers we should support the development of new technologies, such as the information superhighway, which improve our quality of life, but we must protect the rights of individuals, especially in the area of privacy.

With the existence of such entities as the Medical Information Bureau, which was created by insurers to reduce fraud and which contains information on 80 percent of health insurance policies in the country, and with state motor vehicle department selling information, it is very hard to keep sensitive data from ending up in the wrong hands.

During my campaign for Congress I realized that no one is immune to privacy violations. I had my private, personal medical records leaked to the newspapers in New York City.

Every time I talk about this, I relive it. The story of my experience is very difficult for me to discuss, knowing the stereotypes that exist regarding mental illness. A few years ago I sought needed medical treatment after a suicide attempt. I went to the hospital confident that I would receive treatment and that my experience would be private, between me and my doctor.

Let me explain to you what happened to me 1 year later. I had just been through the most difficult challenge of my life. For 4 grueling months, I walked the streets of my district, campaigning to represent the people of the 12th congressional district in Congress. I went up against an 18-year incumbent with a vast war chest. In addition, there were four other Latino candidates in the race. The conventional wisdom was that one Latino could not win against those odds.

Well, I beat the odds. For a Puerto Rican woman, from a community that has little money and few resources, these were tremendous odds.

Just imagine what I felt, 3 weeks after I won this victory in the primary, when I woke up one morning with a phone call from my friend Pete Hamill, a columnist at the New York Post. He told me that the night before, the Post had received an anonymous fax of my records from St. Claire Hospital. The records showed that I had been admitted to the hospital a year ago seeking medical assistance for a suicide attempt. He told me that other newspapers

across the city had received the same information, and the New York Post was going to run a front page story the next day.

For the press, it was a big story. For me, it was an humiliating experience over which I had no control.

How Ironic that 3 weeks before when I won the primary, I did not make the front page, but my suicide attempt of a year ago did. My records were leaked for one purpose only, to destroy my candidacy for the U.S. House of Representatives by discrediting me in the eyes of my constituents.

Very few people knew about my situation, and I made the decision of not sharing it with my family. I wanted them to always remember me as a fighter, happy and strong. My father and mother, 80 years old, they did not understand. They still do not understand.

When I found out that this information was being published in the newspaper and that I had no power to stop it, I felt violated. I trusted the system and it failed me. What is most distressing is that once medical records leave the doctor's office, there are no Federal protections to guard against the release of that information. In some States it is easier to access a person's medical history than it is to obtain the records of a person's video rentals. In New York City, the Manhattan district attorney's office is currently conducting an investigation.

After my experience, many people approached me and told me of their fears that records of their doctor's visits could be made public if they sought treatment for mental illness. It is this fear of being discriminated against that prevents people from seeking the treatment that they need. This fear also speaks to the larger issue of the stigmas attached to mental illness and treatment for mental illness.

Part of the Hippocratic oath reads, Whatsoever things I see or hear concerning the life of man, in any attendance on the sick or even apart therefrom, which ought not be voiced about, I will keep silent thereon.

I realize that laws governing disclosure of medical records vary from State to State, but it is distressing that sometimes some medical professionals do not abide by that part of the oath.

I do not profess to be an expert on all the legal ramifications of comprehensive privacy legislation, but I do believe that we need stringent, uniform and thorough standards for the disclosure of medical records—with the necessary medical and legal exceptions—that must be adhered to by all medical practitioners and administrators. I appeal to everyone not as a politician but as a victim, someone whose personal medical records were released to the press and the public without approval or even advance notice, someone who has experienced the pain and lingering effects of having intimate personal experiences exploited.

We must preserve an important historic principle underlying patient care: the preservation of confidentiality, the privacy and security of sensitive personal information.

President Clinton's Health Security Act, H.R. 3600, contains medical record and privacy provisions which are an important first step toward protecting the innocent victims from the unscrupulous use of medical records, but they need improvement. In the area of

privacy, the bill only provides for the development and implementation of a health information system which would enable a national health board to collect, report, and regulate the dissemination of health information. The President's bill further authorizes the same board to set standards regarding the privacy of individually identifiable health information.

The problem is that the bill provides no clues or guidelines as to what the standards should be or how they plan to reconcile the future standards with the various State rules regarding disclosure of medical information.

Furthermore, the technological improvements to the collection and storage of medical information which the President proposes, such as the computerization of medical records and the implementation of a health security card, drastically increases the numbers of individuals with access to private medical information. I recognize that computerization may lead to reduced medical costs, facilitate the exchange of information between medical professionals, and prevent fraud. But computerization also increases the likelihood that an individual or group would attempt to obtain such information without the consent of the patient.

In the House, Representative Pete Stark has introduced a prescription drug records privacy bill which would permit individuals to bring civil action against any retailer, physician or administrator of a health benefit plan who knowingly discloses a person's prescription drug records without his or her consent or for a reason not covered under the bill's established list of exceptions. This is the type of legislation we need for all medical record information.

Mr. Chairman, I am one of the few lucky ones for a number of reasons. First, I was able to afford the treatment that I needed to recover. It frightens me to think how many people suffer in depression and despair because they cannot afford the professional services or medicine that can make them whole again.

Second, I received a great deal of support from my community, and luckily, did not have my credibility diminished in their eyes. Most people are not so lucky. Most people are forced, because of the fear and social stigma attached to mental illness, to not seek medical treatment.

Further, the release of their medical records, if they seek treatment, could cripple their chances for credit, or work, or social acceptance. It is importance for you to recognize that the only reason I am able to testify today about this experience as a productive member of society is because I had the strength of will, the financial means, and the support of my community.

And speaking of support, I want to take this opportunity to express my appreciation and gratitude to Tipper Gore, the Vice President's wife, for all her commitment, compassion, and work on behalf of mental illness. I personally shared my experience with her and she has been very sensitive and supportive.

Mr. Chairman, a person's medical records belong to that person. I implore you to learn from my experience. I sincerely hope that you will join me, not only in working diligently for comprehensive privacy legislation, but also in addressing the larger issue of mental illness. Thank you.

Senator LEAHY. Congresswoman, I must tell you how much I appreciate your testimony. On one committee or another for 19 years I have been holding hearings and I have rarely heard any testimony as gripping or as moving as yours. I know from my own conversations with you and by our staff's conversations, this is not an easy thing for you to do.

I think, however, that your testimony can have far greater effect than all the work and lobbying I might do here. I think people realize that it is testimony, not of a member of Congress, but of a human being. You were violated in having your records released.

I suspect that if you are like most people, you trust the medical professionals to put in your records information that is accurate and necessary. You probably had not even read your whole medical records before they were released to the press; is that correct?

Ms. VELAZQUEZ. I never did. I learned in the New York Post after I read them.

Senator LEAHY. That is a pretty terrible. I mean, these are things that are so private that you were willing to leave them in the hands of professionals and had not even read them yourself. And then suddenly that information appears in a newspaper available to millions of people.

The obvious question is—and maybe there is no answer to this—but when you look back, do you think you would have gone and sought the help that probably saved your life if you had known that that experience was going to be on the front page of the paper?

Ms. VELAZQUEZ. When I was taken to the hospital, of course, I was unconscious. But the next day, the doctor was there and I told myself, he is my savior. I never expected that this experience would end up in the hands of any person and that I would read about it in the New York Post. I think that now when I have to go to a doctor, I just wonder how much—and I know that if I give him a lot of information about my medical history that I will be better served in terms of the treatment that I am seeking. But I wonder how much information I should share with my doctor.

Senator LEAHY. There are men and women, old and young, who are out there who should seek help, but are deterred by a whole lot of reasons: financial, inability to know where to go, or other issues. But all of them would be deterred to a greater or lesser extent if they thought that all their neighbors, their co-workers, their family, everybody else was going to be able to read about what they sought; is that not correct?

Ms. VELAZQUEZ. Yes. After my experience, it was so scary because so many people not only came over to show their support to me, but some of them to share their own experience. And they have shared their concern that—and some friends who have come to me and shared their pain and I have told them, seek professional help, they wonder. It is very frightening to know that some people who are in need of seeking professional help might consider not doing that because of their fear that their private life might be exposed.

Senator LEAHY. You mentioned that this is now under investigation. Do you know what the status of that investigation is today?

Ms. VELAZQUEZ. Through my lawyer—it has been very difficult, but I know that it is still going on and I should not discuss any information.

Senator LEAHY. That's all right. Let me ask you this question. Do you think that people who disclose personal medical information without a patient's consent should be punished? Should that be against the law?

Ms. VELAZQUEZ. It should be a criminal act. Yes, it should be punished.

Senator LEAHY. And that should be the same whether they are disclosing the records of a public figure or a non-public figure; would you agree?

Ms. VELAZQUEZ. Yes.

Senator LEAHY. We are all human beings. Sometimes they think that 535 of us might not be, but we really are.

Congresswoman, especially at the beginning of the session, I know you have got leadership meetings and other duties back on the other side of the Hill. Again, I apologize we started later than we had told you because of the votes. I cannot thank you enough for taking the time to be here.

I also appreciate what you said about Mrs. Gore. I will make sure that she sees a copy of this part of the transcript because I know of her commitment to that issue. Having served for years with then-Senator Gore, and knowing the Gores, this is not something that she suddenly discovered since she became the wife of the Vice President. As you know, this is a commitment that she has had in this area for years and years, and I think everybody would agree, Republican or Democratic, that we are fortunate she does have that commitment. But I will tell her of your kind words.

Ms. VELAZQUEZ. Thank you, Mr. Chairman

Senator LEAHY. Thank you very much.

Our next witness, Nan Hunter, is the Deputy General Counsel of the Department of Health and Human Services. I would note that Ms. Hunter was a professor of first amendment law at Brooklyn Law School from around 1990, I believe it was, until you joined HHS, which I am delighted to see.

Ms. HUNTER. That's right.

Senator LEAHY. As one who feels the first amendment is the bedrock of our democracy, I am delighted to have you here. Please go ahead, Ms. Hunter.

STATEMENT OF NAN D. HUNTER, DEPUTY GENERAL COUNSEL, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Ms. HUNTER. Thank you, Senator. I am delighted to be here. I am happy to discuss with you the information and privacy aspects of the President's proposal for health care reform.

The President's plan offers a new vision for delivering and paying for health care in the United States. Reliable data are essential to that system. Data are essential for research on medical outcomes, for monitoring access and practice patterns, and for policing fraud and abuse. Without adequate data we cannot perform those and other necessary functions.

Privacy protections, however, are an integral part of this system. Privacy is a first principle of our approach. Privacy protections will

ensure that individually identifiable information in this new system is used only when individual identifiers are truly necessary, and is used carefully, only for the purposes for which it is intended with close attention to privacy, and not in ways that will harm people.

Legal protections for health care information today are skimpy and uneven at best. They exist primarily at the State level and they vary greatly. Only a handful of States have comprehensive health care information confidentiality statutes. Many have statutes covering particular kinds of information like HIV infection, and some have privacy laws concerning insurance information.

The only Federal record confidentiality law covering the Nation generally is one protecting information about patients in drug and alcohol abuse treatment programs. The Privacy Act covers only records held by Federal agencies.

This Administration believes that confidentiality controls are essential. Under the Health Security Act, medical records would be far more protected from inappropriate uses or disclosures than they are today. The Health Security Act outlines a comprehensive national policy for protecting the confidentiality of health information. It includes provision for protecting the information to be gathered by the new system as well as, ultimately, national legal protections for information currently held by all health care providers.

This comprehensive policy will provide our people with much greater protection and control over the use and disclosure of information in their health records than they have today. In the system we propose there will be an administrative data system to record enrollment. The health security card will contain basic information, including a unique identity number and the person's health plan. Patient information needed for the operation of the system will be transmitted electronically in uniform data sets meeting national standards.

As part of the information system, the national health board will oversee the establishment of an electronic data network with regional data centers. The national health board will establish standards for the information to be collected. This will be done with public discussion and consultations with a wide variety of experts in data systems and privacy controls.

There are several elements for the safeguards for privacy in the President's bill. Let me talk about four principal features first. First, within 2 years the national health board will promulgate detailed standards for confidentiality. The standards will elaborate the principles set forth in the bill. Second, there will be controls with criminal and civil sanctions on improper use of the health security card or the unique identifier number.

Third, within 3 years the board will propose a comprehensive scheme of Federal legislative protection for health information. This will cover, for example, all preexisting records of physicians and hospitals. And fourth, there will be ongoing monitoring from people outside the Government to assure that privacy concerns are carefully considered. The national health board will have an advisory council on privacy and health data that will include members distinguished in data protection and privacy, ethics, civil liberties, and patient advocacy.

Let me describe some of these in more detail. The bill sets out basic standards upon which the board must base its rules. Disclosures will be carefully restricted to those authorized by the individual, or for purposes of operating the system, or for purposes meeting criteria established by the board that are consistent with the general principle that individually identifiable information is used only when necessary for some aspect of health care. Disclosure will be restricted to the minimum necessary to accomplish the purpose of the disclosure.

No identifiable information about an individual will be disclosed to set premiums based on risk adjustment factors, nor will it be used to make employment decisions. No individual's name will ever be associated with information transmitted between any of the entities in the system; that is, between the health plan, the alliance, or the regional data centers.

There will be technical and administrative safeguards, such as computer and communication security measures, to prevent unauthorized persons from ever getting information. Individuals will always be able to see and get a copy of information about themselves, and they can correct erroneous information. Individuals will have a right to know which entities hold or use information about them and for what purposes.

None of these protections exist today as a uniform national standard for confidentiality of medical records.

The bill does not alter the existing power of courts with respect to health care information, nor does it alter existing requirements for reporting to public health agencies disease, child abuse, birth, or death.

Each person enrolled in the system will have a unique identifier. That number cannot be used to connect individually identifiable information from the health care system with information outside the system except when necessary to administer the health program.

To require anyone to give his or her number, or to use the number for any purpose other than participation in the health program, will be a criminal offense and will also subject the offender to civil money penalties. The health security card will be used only for the purposes of the health system. To require a person to show it or to otherwise use it for any other purpose will be a criminal offense and will subject the offender to civil money penalties.

Let me conclude by putting the information aspects of the President's proposal in a broader perspective. The President's proposal will reduce health care cost for individuals and businesses by reforming the health care payment system using information necessary to achieve that purpose. This system will be surrounded by legal and operational confidentiality safeguards, built into the design at the beginning and basic to its operation, to protect the privacy of the people it serves. This combination of legal and other safeguards will offer the public assurance that individually identifiable information will be used respectfully and carefully.

We look forward to discussions with you, Mr. Chairman, and with the Congress on these proposals. Thank you.

[Ms. Hunter submitted the following:]

PREPARED STATEMENT OF NAN D. HUNTER ON BEHALF OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

I am Nan Hunter, Deputy General Counsel, U.S. Department of Health and Human Services. I am happy to be here to discuss the information and privacy aspects of the President's proposal for Health Care Reform.

The President's plan offers a new vision for delivering and paying for health care in the United States. That plan includes many features whose success will depend on having timely and reliable data at every level of the health care system.

USE OF INFORMATION IN THE HEALTH CARE PROGRAM

Good information is essential to the operation of a high quality health care system. The plans will need information on the enrollment of individuals. Aggregate data, not using patient identifiers but derived from enrollment and medical care encounter records about individual patients, will be used for the management of the system—calculating premiums, negotiating rates, and especially, monitoring quality and the performance of health care providers.

The information we can learn from these data is essential to help everyone who uses health care. It will be used to assure that everyone has access to care and to learn more about the outcomes of treatment.

Thus, the plan includes information systems designed to obtain those data. As an integral part of that system, privacy protections will ensure that individually-identifiable information in those systems is used only when individual identifiers are truly necessary, and is used carefully—only for the purposes for which it is intended, with close attention to privacy, and not in ways that will harm people.

Before I describe the existing state of safeguards for health care information and the privacy protections in the President's proposal, I want to talk about the basic reasons for medical confidentiality and the ethical and practical principles behind it.

The reasons for confidentiality

The primary goal of confidentiality in medical care is to permit patients to be totally frank about facts which bear on their health, and to subject themselves to examination and tests which reveal facts about them. Without confidentiality protection, sick people would be faced with having to choose between revealing information to obtain treatment, or retaining their privacy—a cruel choice, and one that would in some cases lead to untreated disease.

In public health and research there are even more pressing reasons: we want the patient to be frank not only for his or her own sake, but also for the health of society more generally. Only if we keep the patient's confidences will he or she tell the truth. This permits us to interrupt the spread of communicable disease, and to gather accurate information for research about disease.

Ethical protections

Personal information about patients has long been kept confidential under the traditions and ethical principles of the medical profession and other health care professions. For physicians, the obligation is found in the Hippocratic Oath, dating from the fourth century B.C., and is continued in current ethical statements. Other professions have similar ethical principles and codes of conduct. At the same time, the development of the health care system has led to use of records by many businesses or organizations that do not care for patients, and are not subject to the traditional ethical and social norms of the healing professions.

Legal protections

Legal protections for health-care information today are skimpy and uneven at best. They exist primarily at the state level, and they vary greatly. A few states have comprehensive health-care information confidentiality statutes, including two (Montana and Washington) which have enacted the Uniform Health-Care Information Act of the National Conference of Commissioners on Uniform State Laws. Many have statutes covering particular types of information (like HIV-infection and mental-health information). Insurance information (including health information about beneficiaries) is covered by privacy laws in several states.

In addition, there is some case law establishing confidentiality duties. The well-known physician-patient privilege (which most states have in some form) only applies when the physician is testifying in court or in related proceedings. It has nothing to do with other decisions the physician or facility may have to make about disclosing patient information.

The only Federal health record confidentiality law covering the nation generally is one protecting information about patients in drug and alcohol abuse treatment programs. The Privacy Act covers records held by Federal agencies, including health care records held by the Department of Veterans Affairs, the Indian Health Service, and the military services.

Uses of information

All these laws permit many uses of patient information without consent. It is important to recognize that health records are used for a great variety of purposes today, often with the patient'a consent, or pursuant to legal authority. In health care facilities there are many people involved in treatment of the patient, and in related activities like billing, who need the records. Patients routinely authorize disclosure to health insurers to obtain reimbursement. Records are used for research, often with patient identifiers so they can be linked with other records, although without further use or publication of patient identifiers. Some conditions are required to be reported to health authorities, to permit intervention for public health purposes.

Society and individuals are willing to have records used in these ways because such uses are necessary to the overall functioning of health care delivery and public health systems. Even in these contexts, however, there is the risk of invasion of legitimate privacy interests.

The need for privacy protections

For all these reasons, legal and ethical confidentiality controls are essential to protect the privacy interests of patients. They prevent disclosures that are not appropriate or necessary. They reassure patients that there are orderly processes for dealing with their information, even if there is not absolute secrecy. They can ensure that patients see their own records if they wish, and can provide remedies for patients whose records have been improperly disclosed.

Careful protections become even more important with the wide-spread computerization of records. Computerization can provide great benefits both for the patients and for management of the system. The effect on the privacy interests of patients is mixed. Computerized records present certain new vulnerabilities, such as the possibility that an unauthorized user may get access to them through the communications system. At the same time, computerization can enhance privacy protection in many ways. For example, when disclosure of records is necessary, it may be easier to pick out and disclose only information actually needed, rather than a patient's whole record. Further, a more careful watch may be kept on disclosures of information, through recording and auditing mechanisms built in to computerized record systems.

The health security act

Let me describe the information system and the privacy provisions in the Health Security Act (S. 1757), that will protect the confidentiality of the records. We look forward to discussions with the Congress on the President's proposals. In the system as proposed, there would be an administrative data system to identify persons who are enrolled. The Health Security Card would contain basic information on each person enrolled, including a unique identity number and the health plan in which the person is enrolled. Information about patients needed for the operation of the system would be transmitted electronically, in uniform data sets meeting national standards. These minimum data sets would be developed for enrollment and for claims and encounter information for all covered health services. As part of the information system, the National Health Board is to establish an electronic data network, with regional data centers.

The National Health Board would establish standards, and determine the information to be collected. This would be done with wide public discussion, and consultations outside the government.

It is essential that there be clear and strong protections for the information that the system has about individual people. A comprehensive national policy for protecting the confidentiality of health information is needed, and the Health Security Act outlines such a policy. It includes provision for protecting the information to be gathered by the new system, as well as, ultimately, national legal protections for information held by all health care providers. This comprehensive policy will provide our people with much greater protection and control over use and disclosure of information in their health records than they enjoy now.

Privacy protections in the act

There are several elements to the safeguards proposed in the President's bill. Let me mention four principal features, and then give more detail:

- First, the National Health Board would be required, within two years, to promulgate standards for confidential—treatment of the individually-identifiable information in the system. The standards would have to comply with principles and requirements set out in the bill.
- Second, there would be controls, with sanctions, on improper use of the Health Security Card or the unique identifying number chosen for the system.
- Third, within three years, the Board would have to produce a detailed proposal for a comprehensive scheme of Federal legislative protection for health information. This would cover records, for example, of physicians and hospitals.
- Fourth, there would be ongoing monitoring and advice, from people outside the government, to assure that privacy concerns are carefully considered. The National Health Board would have an advisory council on privacy and health data, that would include members distinguished in data protection and privacy, ethics, civil liberties, and patient advocacy.

I will describe some of these in more detail.

Governing principles

The bill sets out basic standards that the Board would have to include in its rules:

Disclosure outside of the system would be carefully restricted to purposes authorized by the individual, or for purposes of operating the system, or for purposes meeting criteria established by the board.

Disclosure would be restricted to the minimum necessary to accomplish the purpose of the disclosure.

No identifiable information about an individual could be disclosed to set premiums based on risk adjustment factors, nor could it be used to make employment decisions.

There would be technical and administrative safeguards, such as computer and communications security measures, to prevent unauthorized persons from getting information.

Individuals could always see information about themselves and get a copy, and they could correct erroneous information.

Individuals would have a right to know what entities hold or use information about them, and for what purposes.

The bill does not alter the existing powers of courts with respect to health care information, nor does it alter existing requirements for reporting of disease, child abuse, birth, or death.

The bill does not distinguish between records maintained in computerized form and records maintained in paper form.

The number and the health security card

Each person enrolled in the health care system would have a unique identifier. What the number will be is not specified in the Act; its design is left to the National Health Board. The Board would be required to make regulations to ensure that the number would not be used to connect individually-identifiable information from the health care system with information outside the system, except when necessary to administer the health program. To require anyone to give his or her number, or to use the number, for any purpose other than the health program, would be a criminal offense, and would also subject the offender to civil money penalties.

Each person enrolled would have a health security card. The Act spells out what kind of information would be included—the identity of the individual, the unique identifier, the health plan, and any supplemental insurance. The card could be used only for the purposes of the health syatem; to require a person to show it, or to otherwise use it, for another purpose, would be a criminal offense, and would also subject the offender to civil money penalties.

Comprehensive health record privacy protection

The Board would be required to develop a proposal, for the consideration of the President and the Congress, to provide comprehensive confidentiality protection for all health care records in the country. Such protection would provide a common rule, with a uniform level of protection through the country, to protect records that are now subject to varying and often inadequate State laws.

The effect of the proposal

Let me conclude by putting the information aspects of the President's proposal in a broader perspective. The President's proposal will reduce health care costs for individuals and businesses by reforming the health care payment system, with the information system necessary to operate that system effectively. That system would

be surrounded by legal and operational confidentiality safeguards—built in at the beginning and basic to its operation—to protect the privacy of the people it serves. At the same time, the President proposes to use this opportunity to devise protections for all health records, in providers' offices and in many other places. Those protections will be stronger than the present protections. This combination of legal and other protections will offer the public assurance that individually-identifiable information will be used respectfully and carefully.

Thank you, Mr. Chairman. I will be happy to answer any questions.

NAN D. HUNTER,
DEPARTMENT OF HEALTH AND HUMAN SERVICES,
Washington, DC, May 2, 1994.

Hon. PATRICK J. LEAHY,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY: I am happy to transmit to you answers to questions you posed following my testimony at your hearing on high-tech privacy issues in health care on January 27.

It was a pleasure to testify before you. We will be happy to work with the Subcommittee in its further work on these important issues. If we can help, please let me know.

Sincerely,

NAN D. HUNTER,
Deputy General Counsel.

Enclosure.

NAN D. HUNTER'S RESPONSE TO QUESTIONS SUBMITTED BY SENATOR LEAHY

Question 1. The 7 members of the National Health Board are appointed by the President, with the advice and consent of the Senate, and will have the power to decide the type of health security card we all carry and the information about us that will be on the card. This non-elected Board will also have the power to collect computerized information about us, decide where that information will be sent, and how it will be protected. The power this Board will have over each Americans medical information will be immense. Do you think the Board should be given more guidance in the Health Security Act about how to exercise power over personal medical information?

Answer. The National Health Board would be an Executive Branch agency, with public accountability, and would conduct its activities under the Administrative Procedure Act.

In making its decisions, the Board would consult widely with concerned groups, including plans, providers, consumers, public health authorities, researchers, privacy advocates, and others.

We are considering what more precise guidance could be given to the Board in the statute about use and disclosure of information, and we look forward to working with the Congress on this issue.

Question 2. The Health Security Act calls for the creation of an advisory council called the National Privacy and Health Data Advisory Council, which will help the National Health Board formulate the privacy standards and legislation. Could you explain whether the Advisory Council has a longer-term role after the standards and privacy legislation are recommended?

Answer. The Health Security Act does envision an ongoing role for this Council. How it will be employed-depends on the Board, but we believe that it could be of great help to the Board in addressing data and privacy issues that arise in the health care system once it is operational. It could also be of help in advising the Board on the research and technical support activities, and education and awareness programs, with respect to privacy that the board may conduct. (§5121).

Question 3. The Health Security Act has drawn some criticism from privacy experts because the National Health Board is not required to submit a proposal for comprehensive privacy legislation for protection of health information until *3 years* after enactment, even though the Board's implementation of a national health information system and issuance of privacy and security standards for that system will be on-line within *2 years* of enactment.

If the privacy legislation is passed after the national medical information system is already in place, there is a risk that the system might have to be reworked to

comply with new legislative requirements. Would it be more cost effective to have the privacy legislation in place before the information system is implemented?

Answer. We believe the Act envisions that the rules governing information to be gathered in the new health care system will be prepared by the Board within the two years it will take to establish the information system. That system and its privacy rules will be developed simultaneously. Thus, there should be no need to rework the system to accommodate rules made later.

The Board is given three years to recommend legislation to the Congress to apply to health care records more generally—i.e., to records that already exist in the offices of providers and payors.

We do appreciate that there would be value in having even these rules developed at the same time as the basic health care information system is being designed, and we welcome conversations with the Congress on this.

Question 4. Vermont already has an effort underway to implement a state-wide medical information database. The Vermont Health Information Consortium (VHIC) has a confidentiality and privacy working group that is working to identify confidentiality, privacy and security standards for the system.

Will the National Health Boards privacy and security standards for the national medical information system preempt any state guidelines, even if those guidelines are more protective of privacy and security?

Answer. We are studying the issue of preemption. It is a complicated issue, and we will be happy to work with the Congress on this.

Question 5. Could you explain what types of records will not be covered under the Board's standards? For example, would computerized medical records maintained at a hospital or in doctors' offices be covered by the National Health Board's privacy and security standards?

Answer. The Health Security Act envisions that the Board's standards will cover the health information system that will be established to support the payment and management mechanisms under the Act (§5120). Those standards would not cover the medical records, used for patient care, maintained at a hospital or in a doctor's office. The Act calls for, within three years, the Board's recommendation for legislation covering such records. (§5122)

Question 6. The Republican response to the President's State of the Union message characterized provisions of the Health Security Act as a "compromise of privacy none of us can accept." Does the Health Security Act provide for health and treatment information to be sent to a national database without the patient's approval?

What does it, in fact, provide for?

Answer. There will not be a single comprehensive data base. We are creating a national network of data systems that can serve a variety of data needs at all levels of the health care system from consumers to the Federal government. It is important to distinguish enrollment and encounter data.

There will be a select set of enrollment information that will be available at the national level which is needed for purposes of coordinating care, coverage and payment. There is no need for a nationally centralized identifiable encounter data base. Most national analytic needs do not require identifiable data at all. They can be served through anonymous linked files of enrollment and encounter files.

Question 7. There has been a lot of attention focused on the Health Security Card that will be used under the Clinton reform plan. At the Subcommittee's last hearing on high-tech privacy issues in health care on October 27, 1993, we saw demonstrations of two types of cards—the smart card and laser optical card—that could be used to hold many pages of health records.

The Health Security Act does not specify the type of card that will be used if the plan is enacted, but leaves up to the newly created National Health Board to decide standards for the form of the card. Could you explain why the bill does not specify the type of health security card everyone will carry?

Answer. The design of the health card is left to the Board, so that it will have the flexibility to adopt the best technology—for protecting privacy and for fulfilling the operational functions of the card—at the time the card is developed.

Question 8. The alliances will issue the health security cards to all its covered members. Will each alliance have the freedom to decide on the type of card it issues, so long as the card it chooses to use works on the health system?

If so, does the plan allow individual alliances to choose more high-tech types of health security cards with better security features and with more capacity to hold information than a magnetic strip card?

Answer. The Health Board will determine the form of the card, in light of privacy considerations, available technology, and the operational needs of the system. There are several available technologies, and the magnetic strip card is only one of them. There is nothing unacceptable in principle with the choice of different cards, as long

they meet minimum standards set by the Board to insure that the card works for the basic operational purposes of the system.

Question 9. Do you think it is important for the health plan to give alliances and consumers a choice of the type of health security card they use, so long as whatever card they choose works on the information system?

Answer. This will be up to the Health Board, in light of the considerations mentioned in No. 8, above.

Question 10. Will use of a health security card rely on the storage of the medical information in a central database? Could you explain how extensive the information in the central database will be?

Answer. The use of the health security card will not rely on the storage of the medical information in a central database. The purpose of the card is to identify the holder as enrolled in a particular health plan, and to assist in the administrative transaction attendant to receipt of health care. That might possibly involve communicating with a regional data base, but to retrieve the administrative information, not medical information.

Storage of medical information on a card, or retrieval of medical information from a central location through use of a card, are among the possible uses of card technology. But they are not part of the basic use of the card in the program proposed in the Health Security Act.

The nationwide enrollment data base would contain information such as the unique identifying number of the enrollee, and the plan in which the person is enrolled. It could also include information about other insurance coverage.

Question 11. The Act says that the National Health Board will determine the information contained in the health security card. This information will include identity information, the plan in which the person is enrolled, any supplemental policy, and any additional information the Boards finds necessary "for the purpose of providing or assisting the eligible individual in obtaining covered health services (Sec. 5105).

Could you give us an idea of what other information may be required to be on the card?

Answer. It will be up to the Board to determine what other information may be required on the card, and it is difficult to predict what other administrative information may be needed.

One possibility would be for the Board to require on the card only the basic information mentioned in the Act, and leave to personal choice whether an individual wanted the card to carry medical information or to be a means of access to centrally stored medical information.

Medical information on the card, or accessible through it, could be of great benefit to an individual, and some people may want that benefit. Others may prefer that the card not be used this way.

Question 12. We already have situations in this country where employers can get information about the medical condition of prospective employees to use against them in hiring decisions. With medical information literally at your fingertips with the health date card, what is to prevent an employer from demanding the card before making a hiring decision. The Act proposes to deal with this situation by prohibiting an employer from doing this but it puts a prospective employee who wants a job in the position of turning the employer in. Is there any way to address this problem?

Do you know of any technological features that could limit an employer's access to private medical information on the health data card?

Answer. The card as envisioned in the Act will not provide "medical information literally at your fingertips." For its basic purpose, it will not contain medical data.

In any case, there is an explicit prohibition in the Health Security Act against use of health care information from the health care system in making employment decisions (§5120(c)(9)). Additionally, use of information for employment decisions is restricted by the Americans With Disabilities Act.

It should be noted that the possibility of demanding access to a health record for an inappropriate purpose is not necessarily increased by carrying the information on a card. It is possible to ask an individual to authorize disclosure of a medical record in the hands of a health care provider, or to ask an individual to get a copy of his or her own record and provide it to the employer.

If there were health information on the card (at the individual's choice, as discussed in No. 11), it is possible to design a smart card with several memory zones, each with different levels of security and requirements for access. Health care providers, or health alliances, might maintain the controls on access to the several levels, while securing the individual's permission to access the material.

Question 13. Sec. 5101 of the Health Security Act requires, within two years after enactment, that the National Health Board implement a health information system to collect and disseminate health information "consistent with policies established as part of the National Information Infrastructure Act of 1993.' Could you explain the interrelationship, if any, between the information system that is contemplated in the Administrations health care reform bill and the information superhighway?

A. The information superhighway will consist of many highly effective technical means of communication, and it may carry many types of information. It can be expected that health care information will be carried over this system, and the data system contemplated in the Health Security Act can certainly make use of it. The main interrelationship is most likely to occur in the areas of new technologies for communication, and transmission standards.

The bills now pending ("The National Information Infrastructure Act of 1993," H.R. 1757, and "Information Technology Applications Program Act of 1993," title VI of S. 4) call for projects to develop high performance computing and high speed networking technologies for use in the health care sector. We envision that these authorities, if enacted, will be helpful in supporting development of elements of the data system envisioned in the Health Security Act.

Question 14. As part of the information system envisioned in the Act, regional centers will be created to collect, compile and transmit medical information. Could you give us any additional details about these regional centers, such as the number contemplated or where they will be located?

Answer. At this time we are not proposing the number or location of regional data centers. It is quite possible that regional data centers will be configured in a number of ways. Centers could be single discrete entities run by public or private interests. A center could also be a consortium of interests that either runs a single data system or a network of geographically dispersed data systems. This flexibility would make it easier to build upon the existing data systems in a given region. Regardless of the configuration, all data centers would provide a minimum set of services and would be subject to the same privacy standards. Regional data centers would be electronically linked to facilitate access to information.

Question 15. Information will be transmitted from regional centers to the National Health Board in order for the Board to get set both national health standards and a national health budget, and to evaluate the performance of different plans and alliances. Does this mean there will be a huge, national database of medical information centralized with the National Health Board?

Answer. There will not be a single comprehensive data base. We are creating a national network of data systems that can serve a variety of data needs at all levels of the health care system from consumers to the Federal government. The functions you describe do not require access to identifiable encounter information at the national level.

It is important to distinguish enrollment and encounter data. There will be a select set of enrollment information that will be available at the national level which is needed for purposes of coordinating care, coverage, and payment. There is no need for a nationally centralized identifiable encounter data base. Most national analytic needs do not require identifiable data at all. They can be served through anonymous linked files of enrollment and encounter files.

Question 16. I am interested in how the enforcement mechanisms of the Health Security Act are designed to protect personal privacy. If a privacy standard promulgated by the National Health Board is violated, sec. 5141 provides that the Secretary of HHS can impose a civil penalty of $10,000 per violation. It would be wrong, however, to require the public disclosure of private information in order to prove a violation of a privacy standard. What procedures govern that the Secretary's determination of a privacy violation and what protections are there in those procedures to protect personal privacy interests?

Answer. We agree that there can be no effective vindication of privacy rights if it is necessary to have a public proceeding with, perhaps, disclosure of the very information that is meant to be kept confidential. There are procedural mechanisms available, such as use of a pseudonym (e.g., Jane Doe) to identify the aggrieved person, that can assure that this does not happen.

The precise procedures would be developed later. We note that there is an established body of procedure governing the imposition of civil penalties, and that our Office of Inspector General has been effective in having penalties imposed for violations of rules in Federal health care payment programs.

Question 17. Is the civil penalty provided by section 5141 intended to preempt in any way a person's rights or remedies for an invasion of privacy?

Answer. No, we believe the civil penalty would not preempt other rights or remedies for an invasion of privacy. The bill as written provides the stated penalties "in addition to any other penalties that may be prescribed by law."

Question 18. Does the Administration intend for the privacy standards promulgated by the National Health Board to be used to immunize what might otherwise be an invasion of privacy or to act as a defense to such a claim?

Answer. The exact content of the standards will be up to the Board. We believe that the standards should provide strong privacy protection, and should not be used to "immunize" what might otherwise be an invasion of privacy.

However, we would recommend that once a standard for use and disclosure of information has been established, those acting in good faith under it should not be subject to suit or prosecution for actions taken in accord with that standard.

Question 19. Section 5138 of the bill would make criminal only the misuse of the health security card or unique identifier number. Does the Administration think that misuse of personal and private health information required to be maintained on the computerized health information system should also be subject to criminal penalties?

Answer. The bill would not, as written, provide criminal penalties for improper disclosure of information maintained in the health information system. The standards set out in the bill are not, of themselves, precise enough to base a criminal penalty on.

We believe that, once standards for disclosure are defined with specific precision, criminal penalties should attach to their violation. We would welcome discussion with the Congress on the possibility of criminal penalties.

Question 20. According to section 5120 of the Health Security Act, the National Health Board is to promulgate privacy and security standards in two years. With respect to disclosure of personal medical information there is a catch-all provision that authorizes disclosure otherwise consistent with the Act and criterion established by the Board. What prevents this authority from becoming a giant loophole to our privacy protection?

Answer. The intent of the bill is to allow broad flexibility for uses of identifiable information necessary to operate the health system, while providing strong protections against any use of information for purposes inconsistent with that goal.

We are considering proposing modifications that would further delineate within the statute specific standards for disclosure and use, and we would be happy to discuss this with the Congress.

Question 21. Sec. 1203 of the Act directs participating states to establish criteria for certifying health plans and includes by reference to other parts of the Act, criteria related to the confidentiality of health data. Should the Act give states more explicit direction about the privacy and confidentiality criteria that health plans must satisfy for certification?

Answer. The Act should probably not go into detail at that level. The Board may want to provide guidance or assistance to the plans in this regard. If Congress concluded that the Act should include more substantive confidentiality requirements, those requirements would of course apply to the plans, and States would have to assure themselves that the plans were complying with the requirements.

Senator LEAHY. Ms. Hunter, I know you feel as I do that protecting the privacy of individuals is something that we pride ourselves on in this country. You have worked both at your school and the ACLU on issues where privacy becomes very important.

It is going to be difficult enough to try to figure out what kind of a health care plan works. But you can understand the concern that Americans feel when you hear statements, very powerful statements like the Congresswoman just gave. You and I can go back and find hundreds of other experiences like that one, where personal medical information may not be on the front page of the Post, but it could be on the desk of an employer, or it could be a co-worker, or a neighbor, and what that does to the individual.

I looked at the Health Security Act, and I am concerned by some of the criticism I have heard that the national health board is not required to submit a proposal for comprehensive privacy legislation for the protection of this health information until 3 years after enactment, even though the board's implementation of a national

health information system would all be on-line 2 years after enactment. Does there have to be that kind of a delay, or is that criticism unfounded?

Ms. HUNTER. Senator, the plan calls for the health board to promulgate standards that will apply to all information coming into the new system based on the principles that are set out in the legislation within 2 years after enactment. The structure behind the President's proposal is that, first, and within 2 years, the board must promulgate standards that govern the new system from the beginning, from the start-up date of the new system. So those standards are looking prospectively and they do provide for penalties, civil money penalties and criminal sanctions in some cases for violations of those standards or violations of provisions that are in the bill.

The next stage to which you are referring would happen 3 years after enactment, and that is the proposal from the board for comprehensive legislation. We structured it in a two-stage process for several reasons. First, because the comprehensive legislation would cover all medical records, all preexisting medical records, all medical records that exist today and not simply the new records that come into the system. We thought that the opportunity to structure the standards and the rules and the safeguards for the new system would be a necessary first step, so that the new system is absolutely protected from the beginning and so that the legislation could build on the experience of formulating safeguards for the new system.

Senator LEAHY. An article appeared in the paper here a while ago about an IRS office where apparently there were a lot of IRS tax records of famous people—in this case, I think Hollywood stars. It turned out that some of the people who did the electronic filing, had fun just kind of waltzing through the electronic files and seeing how much particular persons made last year, what their tax deductions were and everything else. They would just talk about it in the office to a few co-workers, and they only talked about it to a few others, and to a few others. And of course, very quickly this was in the press.

Do you feel that we can keep medical data in this way—I mean, somebody has got to handle this stuff. Somebody has to actually, physically load it into the system, somebody has got to move it about. But to stop the person who violates a trust, and really their own condition of employment by going through it, can we prevent that?

You talked about moving information back and forth without people's name. I would assume what you are talking about is that we have done X number of open-heart surgeries at this kind of price or something like that, without identify the particular patient. But how do you stop it so that somebody cannot go through and find out what is in Pat Leahy's records, or Nan Hunter's records, or anybody else's?

Ms. HUNTER. There are a number of ways to stop it. One, of course, is to provide stringent penalties. At some level that is the best you can do because, as you said, Mr. Chairman, the data have to be transmitted. There is also the protection that names are not associated with data. And some of the kinds of situations that you

have just referred to where clerical employees might simply scroll through papers, or even electronic transmissions, it becomes much more difficult to do if the names are never attached to those records.

The kind of situation you talk about is one of the reasons that the President's bill attaches from the very beginning very stringent criminal and civil penalties for misuse of the identifier, because the identifier number ultimately has to be the code.

Senator LEAHY. But would you go further and make the same criminal and civil penalties apply not just to the misuse of the identifier but of the health information that is behind that?

Ms. HUNTER. The civil money penalties include a penalty for violation of any of the standards that are set up by the health board. So any unauthorized disclosure would lead, at a minimum, to a civil money penalty. And those sanctions are something that we are more than willing to work with you and others on.

Senator LEAHY. Let's go right to an actual case, Congresswoman Velazquez. Let us suppose all this had occurred after we are in some form of a national health system. And if they were able to find who it was that got into her records—it is obviously an unauthorized disclosure. She was not about to, in the middle of a campaign, authorize a disclosure like that to a newspaper. Should there be criminal penalties against the person who disclosed that?

Ms. HUNTER. I think that's an important question to explore. Right now under the President's bill for information coming into the system there would be a civil money penalty that could be assessed against anyone who would engage in such unauthorized disclosure. And there exist some legal remedies which I imagine the Congresswoman is exploring.

Senator LEAHY. While you are exploring it, just so they will know back at HHS, this chairman thinks that there should be criminal penalties, too. I really do. I feel strongly about that. I have had the advantage of both practicing law as a private practitioner and involving myself with civil remedies, and also for a number of years as a prosecutor being able to use criminal remedies. I think that this is something that calls out really for both. I think it should be a crime to disclose anybody's medical records in an unauthorized fashion.

I do not think, when we are able to maintain so much information, that we are going to have the confidence in this system as a Nation unless there is a criminal penalty for doing that. I know all of this is still in the formative stage and we are still deciding what to do, but I feel strongly that we should consider appropriate penalties because the advantages of being able to store so much of this information electronically is enormous.

For example, you are traveling in Arizona and you are in an automobile accident. With one of the cards I showed, you would be able to show, when you are brought into a hospital, that you have an allergy to this or that, or are allergic to this type of medication versus that, or you have got a preexisting heart condition or whatever it might be. I mean, you do not have to be an expert in the medical field to know how important that could be if somebody could just pop the card into a computer and you have got the information there immediately.

But that is also the down side of it, too, because once that card is put into a computer that information could also be copied into somebody's data bank in Arizona, or Vermont, or anywhere else, and it has to be protected. It is not like you are carrying around the suitcase of medical records with you, but in one sense, you will be. I think people have to know that this is inviolate. And in most cases it is. Most doctors, most medical personnel would be horrified to think that somebody would rifle through their patients' records.

But I do not want anybody to start thinking, well, maybe there is a little bit of information that could be used in there. Maybe some information could be used for help in selling life insurance, or non-prescription drugs, or this, that, or the other thing.

Ms. HUNTER. Senator, I just want to emphasize that the Administration is committed, as I said, to privacy as a first principle and to the need to protect the confidentiality of these records.

Senator LEAHY. I know it is. And I would note that without that, I do not think a health care bill can pass the Congress. I do not think it would, as much as people want it, because everybody wants health care but I think most people do not want us to give up our sense of privacy.

I have a number of questions that I will submit for the record. The one question I would like to ask is, employers today might seek medical information as a condition of hiring people. If you have got all your data on your health card, what is to stop an employer from saying, before I go any further on this job application, give me your card, I want to scroll through this?

Ms. HUNTER. There are several things that would stop an employer. The bill prohibits the use of information gathered as part of this health care system to be used by an employer to make employment decisions in that kind of situation. The bill also, as I said, imposes criminal as well as civil penalties for anyone who would try to do what you just suggested. That is, an employer would try to force someone to display or produce the card for any purpose other than obtaining health care.

And third, there is an existing statute, the Americans with Disabilities Act, that protects against job discrimination for people who have disabilities unrelated to the essential functions of their work. So all of those protections, in this bill and in existing law, would stop an employer from doing that. As I said, one of the reasons we wrote the bill this way is to protect against that very kind of abuse.

Senator LEAHY. It is going to require some enforcement though because I can still see at the time when somebody is trying like mad to get a job in a shrinking job market and the interviewer sits there and says, "you know under the law we cannot ask you about what is on your card, and I have been looking over your job application and I am still having a hard time making up my mind. You do not have to show me your health care card." And you know there is going to be those kind of situations.

We have got to find a way to prevent this situation. Part of that is going to be an educational process.

Ms. HUNTER. That's right.

Senator LEAHY. And in some instances where there are abuses, it is going to require some prosecutions. But the difficult part today

is the prospective employee that has to blow the whistle. And they are in a very difficult position because they can blow the whistle knowing I am never going to get that job while this goes on, or I can kind of gulp and say, I will get the job and pay my bills.

Ms. HUNTER. I understand. All I can say, Senator, is that we are very committed to preventing exactly that kind of abuse.

Senator LEAHY. I know you are, Ms. Hunter. I would just ask that you and your staff would keep in touch with us as we do this because we are all working to the same end. We do not want the situation we heard here today, or the situation we would have heard from Mrs. Ashe had she been able to testify.

Ms. HUNTER. Absolutely.

Senator LEAHY. Thank you very much. Thank you for taking the time and coming.

Ms. HUNTER. Thank you, Senator.

Senator LEAHY. Our next panel will have Carolyn Roberts, who is the chairwoman of the American Hospital Association. She is also the president and CEO of Copley Hospital and Copley Health Systems, which just coincidentally are in Morrisville, VT. Ms. Roberts, is also a good friend, and I must admit, one of the people that we are most proud of in Vermont because of what she has done in making a rural hospital in an area where it is certainly anything but a high income area, and she has made it into a model system.

And Janlori Goldman, director of the Privacy and Technology Project at the ACLU, and someone who is not unfamiliar with the Senate Judiciary Committee. She is somebody who has been very, very helpful to us.

I would tell a story, if I might—and I apologize for this, Ms. Roberts. Just so that anybody who is taking notes of the sense of privacy we have in Vermont. I would retell a story that was in the New York Times, as a little sidebar to an article they were doing in Vermont.

To put this in perspective I should point out, my wife and I and family have a small tree farm that is on a dirt road in Middlesex, VT. We have had it about 35 years or so. A neighboring farmer for most of those 35 years has kept an eye on the farm when we've been out of town and so on. He has known me since I was a child.

A driver pulled up to the dirt road and said, "Does Senator Leahy live up this road?" As the Times reported it, the farmer looked at the driver and said, "You a relative of his?" And the person said "No." The farmer said, "You a friend of his?" He said, "Well, not really." The farmer asked, "He expecting you?" The answer again was no. The farmer looked him right in the eye and said, never heard of him. [Laughter.]

So we have that kind of sense of privacy. I only mention this if anybody wonders what my motivation might be for this legislation. We want to keep it private.

Please go ahead, Ms. Roberts.

PANEL CONSISTING OF CAROLYN C. ROBERTS, CHAIRWOMAN-ELECT, AMERICAN HOSPITAL ASSOCIATION, AND PRESIDENT AND CEO OF COPLEY HOSPITAL AND COPLEY HEALTH SYSTEMS, MORRISVILLE, VT; AND JANLORI GOLDMAN, DIRECTOR, PRIVACY AND TECHNOLOGY PROJECT, AMERICAN CIVIL LIBERTIES UNION

STATEMENT OF CAROLYN C. ROBERTS

Ms. ROBERTS. Thank you, Mr. Chairman. Senator Leahy, I am really very pleased to be here today on behalf of the American Hospital Association and to have the opportunity to address what we feel is a very important topic of confidentiality and individually identifiable patient information. I would just say that I think we are all in this room with the same concerns and looking for the best solution.

I would like to make three main points in my oral statement this morning. First, as I think you are aware, Senator, the American Hospital Association has a vision for the reform of the health care system. We support the restructuring of the system to create community-based networks that integrate the delivery and the financing of care, not only to improve patient care, but to yield more efficient and appropriate utilization of the precious health care resources that we have.

The health information infrastructure is central to the reform vision. Better coordination of care, the provision of what we call a seamless system of care to people across time, across sites, and across providers will require that information also move smoothly throughout the system. This also requires, and I think the conversation previously underscores, that we balance the need for such information for improved patient care with the protection of patient's rights to privacy.

Second, accomplishing this protection must be done in a uniform fashion. In examining the current system, we find that laws are inconsistent from State to State, and at the very least this is an administrative burden, but at worst can preclude the transmission of crucial health care data across State lines. While the health care delivery system may be local, our population is mobil and many of our health care systems are multi-State. Some laws actually create obstacles to the legitimate flow of information, and some State laws do not go far enough to protect privacy or confidentiality.

So third, we believe that the best way to achieve the goal is through a Federal law that preempts all State laws on confidentiality of individually identifiable patient information. The President's health care reform bill provides for a comprehensive scheme of Federal privacy protection both with Federal legislation and with privacy standards within the health information system developed by the national health board. The American Hospital Association would go just one step further and provide for the preemption of State laws.

In addition, as you have brought up, Senator, with the earlier witness, we believe that consideration of the issue of confidentiality is far too important to be delayed until 3 years after the enactment of reform as provided in the Health Security Act. It must be dealt with, we feel, as part of the health care reform. Data flow is para-

mount to the health care reform. But it is a front-end issue, not something that we can put off until we have the system reformed.

Our proposal—and we have submitted a piece of model legislation with our written testimony—is ready to be considered along with the broader reform package. It would preempt State laws on the subject of privacy and confidentiality, and would serve as both a floor and a ceiling. That is, that no State could provide less protection nor more protection.

So in conclusion, Mr. Chairman, if our new health system is to provide both high quality care and consumer peace of mind, we believe that Federal law must occupy the field and preempt the application of State law as to the collection, storage, processing, and transmission on individually identifiable health care information. We look forward to working with the Clinton Administration and with this Committee to reach that goal. Thank you for being able to be here today.

[Ms. Roberts submitted the following:]

PREPARED STATEMENT CAROLYN C. ROBERTS ON BEHALF OF THE AMERICAN HOSPITAL ASSOCIATION

Mr. Chairman, I am Carolyn C. Roberts, president and chief executive officer of Copley Health System in Morrisville, Vermont and Chair of the Board of Trustees of the American Hospital Association (AHA). On behalf of the AHA's 5,300 institutional members, I am pleased to testify on our view of the need for federal legislation governing the confidentiality of individually identifiable health care information.

THE NEED TO PROMOTE THE HEALTH INFORMATION INFRASTRUCTURE

This country is on the verge of comprehensive health reform. We hope, as we work to reform the nation's health care delivery system, that we will emerge with a system of community-based health networks that integrate the financing and the delivery of care. We believe that by bringing providers together into health networks, we will provide incentives to integrate services and coordinate care, yielding more efficient and appropriate utilization of precious health care resources.

A health information infrastructure is central to our vision of an integrated delivery system. By such an infrastructure, we mean an interconnected communication network capable of linking all participants in the U.S. health system. For better coordination of care to occur, information about patients must move smoothly across times, sites, and providers of care. Each health care facility and practitioner would connect to and become part of a larger shared information network. When authorized, data from such a system could flow to health care managers, payers, purchasers, policy makers, and researchers to monitor the performance of the health care system and make key decisions for the future. By increasing the accessibility of patient information, this electronic information infrastructure can help improve quality, increase efficiency and control costs. However, because this information will be traveling through a variety of providers, payers and health data repositories, including processing vendors and clearinghouses, this information will become more vulnerable to unauthorized disclosures.

CURRENT PROBLEMS

As we move toward our goal, we are faced with the challenge of finding an acceptable balance between providing greater access to health care information and protecting patient rights to privacy. For all the enthusiasm among those within the health care sector for migrating toward computerized information systems, many Americans view the computerization of personal health information with suspicion, if not outright hostility. No obstacle to the development of this infrastructure looms larger than the public's concerns about safeguarding the flow of personal health information.

As we begin to build a nationwide information infrastructure, we must examine the currently inconsistent laws and regulations which govern the exchange of patient information. Many state and federal laws create obstacles to legitimate sharing of health information that could yield better patient care, administrative savings,

and more efficient patient management. For example, some states prohibit the use of computerized record systems by requiring that orders be written in ink, often referred to as the "quill pen" laws or by restricting the permissible health record storage media to the original paper or microfilm.

Moreover, payers and providers that operate in more than one state are required to comply with a multitude of different rules, which adds to administrative inefficiency. The obligation of complying with individual—often inconsistent—state laws and regulations is overly burdensome and costly.

Despite this plethora of state laws, most of which include some form of confidentiality protection, identifiable health care information still remains vulnerable to unauthorized disclosures. Furthermore, many state laws do not address key issues, like the patient's right to see, copy, and correct his or her own records, and the obligations of anyone who comes in contact with individually identifiable health care information—including but not limited to, payers, providers, processing vendors, storage vendors and utilization review organizations—to protect confidentiality. As a result, the current system promotes confusion over confidentiality rights with varying requirements from state to state.

At the same time, because many of these state laws were written in the context of the paper records of yesterday, they frequently do not offer sufficient security for today's world of electronic data interchange (EDI). The shared information networks of the future will require explicit and uniform confidentiality requirements for handling health care data. Identifiable health care information traveling in an EDI environment is more vulnerable to unauthorized disclosures. Special protections need to be in place for thia type of information in order to provide appropriate incentives for providers and payers to move toward EDI while assuring confidentiality. Therefore, a uniform federal law must ensure that individually identifiable health care information be maintained confidentially as it travels from place to place.

SOLUTIONS

AHA believes that in order to reap the benefits of electronic information exchange while still protecting patient privacy and confidentiality, there must be federal legislation to preempt state laws regarding the collection, storage, processing, and transmission of individually identifiable health care information. All personally identifiable health care information, regardless of where it originates or where it is transmitted should be handled under the direction of a uniform federal law. Additionally, federal law must create a system where confidentiality rights no longer vary from state to state—in other words the federal law should serve as both the "floor" and the "ceiling," such that no state could provide less protection or more protection.

President Clinton's proposed Health Security Act includes a section entitled "Information Systems, Privacy and Administration." This section would provide uniform and comprehensive privacy and confidentiality protection for individually identifiable health care information, including a uniform national standard which would simplify compliance for organizations that operate nationwide and are linked or potentially linked to other data systems.

It appears that the President intends this federal law to occupy the field and preempt all state laws on the subject. However, the proposed legislation does not specifically include such preemptive language. In order for a federal law to be comprehensive, it must contain a preemption clause which would create uniform protection and in fact make the law serve as both a floor and a ceiling.

In addition, the Health Security Act contemplates congressional consideration of the comprehensive federal privacy legislation "not later than three years after" enactment of health care reform itself. AHA believes this issue is too important for a three-year time lag.

Confidentiality protections are an integral part of health care reform and legislation guaranteeing these protections must be considered within that context.

PRINCIPLES GOVERNING THE PROTECTION OF ELECTRONIC HEALTH RECORDS

The issue of the protection of confidentiality of patient information is not a new one; rather, the government has been active in this arena for many years.

In 1973, the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems set out the following principles to govern electronic data systems (many of these principles have been incorporated into the attached model legislation and are part of the Clinton plan as well):

- Existence of personal data record keeping systems must be identified and not kept secret;

- Individuals should be able to find out what information is in their records and how it issued;
- Individuals should be able to prevent information that was obtained for one purpose from being used or made available for other purposes without their consent;
- Individuals should be able to correct or amend a record of identifiable information;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must take precautions to prevent misuse of the data.

Currently, a Department of Health and Human Services (HHS) Task Force on the Privacy of Personal Health Records is preparing another report based on two years of research and deliberations, for delivery to the Secretary in 1994. We look forward to the publication of this report.

In November 1991, HHS Secretary Sullivan convened a forum of national health care leaders to discuss the challenges of reducing administrative costs in the U.S. health care system. At the forum, several health care industry-led workgroups were created—including the Workgroup for Electronic Data Interchange (WEDI) and the Workgroup on Computerized Patient Records. Both of these Workgroups submitted reports to the Secretary' recommending ways the health care industry could begin reducing administrative costs associated with the delivery of and payment for health care, and recommended that national standards be established for protecting the confidentiality of individually identifiable health care information. The American Hospital Association participated in both groups and strongly supports the recommendation that Congress enact federal preemptive legislation governing the confidentiality of individually identifiable health care information.

WEDI, a public/private partnership consisting of health care leaders from all segments of the health care delivery and payment communities, believes that national legal standards for the protection of the confidentiality of personal health information should:

- Establish uniform requirements for the preservation of confidentiality and privacy rights in electronic health care claima processing and payment;
- Address the collection, storage, handling and transmission of individually identifiable health care data, including initial and subsequent disclosures, in electronic transactions by all public and private payers, providers of health care, and all other entities involved in the transactions;
- Ensure that preemption will not supersede state public health reporting laws which address the particular health safety needs of a community;
- Delineate protocols for secure electronic storage and transmission of health care data;
- Specify fair information practices that ensure a proper balance between required disclosures, use of data, and patient privacy;
- Require publication of the existence of health care data banks;
- Encourage use of alternate dispute resolution mechanisms, where appropriate;
- Establish that compliance with the Act's requirements would serve as a defense to legal actions based on charges of improper disclosure;
- Impose penalties for violation of the Act, including civil damages, equitable remedies, and attorney's fees, where appropriate; and
- Provide enforcement by government officials and private, aggrieved parties.

WEDI reconvened in January 1993 and set up a Workgroup on Confidentiality/ Legal Issues to draft model legislation. This model legislation is included in a report delivered to Secretary Shalala in November of 1993 and is attached to this statement. The requirements of this legislation are intended to apply to all entities, including public and private third-party payers and providers, that collect, store, process, or transmit such information in electronic form. The legislation would protect individually identifiable health care information, but would not affect federal and state laws that require reporting of identifiable information to public health authorities. It would also place oversight authority in an independent national privacy commission.

CONCLUSION

The American public is concerned about the development of a new health information system, where their personal health information will easily travel through a variety of health repositories. The public must be assured that the benefits of computerizing their health information substantially outweigh the potential risk of any unauthorized disclosures.

AHA applauds President Clinton for giving this issue a place of prominence in his health care plan. The steps he outlines would do much to ensure confidentiality and privacy of health care records and clinical encounters. But his proposal falls just short of providing complete and comprehensive protection for individually identifiable health care information, because the proposed legislation would not clearly preempt existing state laws. Moreover, the three-year delay in instituting new and stronger confidentiality protectiona ia far too long.

AHA believes that it is essential that federal law occupy the field and completely preempt the application of state law to the collection, storage, processing and transmission of individually identifiable health care information. If our new health care system is to protect unauthorized disclosures of individually identifiable health care information and preserve its privacy and confidentiality, comprehensive legislation must be enacted—at the aame time as the enactment of the new health care system itself—that will ensure uniform and confidential treatment of identifiable health care information.

We appreciate the opportunity to present our views to this subcommittee and look forward to working with you as the issues of reform and confidentiality move forward.

Addenda

Addendum 1: Text of Proposed "Health Information Confidentiality and Privacy Act of 1993"

MODEL FEDERAL LEGISLATION

CONFIDENTIALITY OF ELECTRONIC HEALTH CARE INFORMATION

A BILL

To provide for the preservation of confidentiality and privacy rights in the collection, storage, processing and transmission of individually identifiable health care information (including initial and subsequent disclosure) in electronic form; to preempt state laws relating thereto, except public health reporting laws; to establish a regulatory mechanism for delineating protocols for securing electronic collection, storage, processing, and transmission of such health care information, and for fair information practices; to require publication of the existence of health care data banks; to encourage the use of alternative dispute resolution mechanisms, where appropriate, for resolving disputes arising under this Act; and to establish penalties for violation.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1 - SHORT TITLE

This Act may be cited as the "Health Information Confidentiality and Privacy Act of 1993."

SECTION 2 - SCOPE

A. Applicability. This Act shall apply to the collection, storage, processing, and transmission of individually identifiable health care information (including initial and subsequent disclosures) in electronic form by all persons, including but not limited to public and private third-party payors and providers of health care.

B. Protection. The protections of this Act shall extend to individuals who are the subject of individually identifiable health care information that is collected, stored, processed or transmitted in electronic form.

C. Exemptions. This Act shall not apply to federal or state laws or regulations that require reporting of individually identifiable health care information to public health authorities.

SECTION 3 - DEFINITIONS

For purposes of this Act:

A. "**Disclosure**" includes the initial release and any subsequent redisclosures of individually identifiable health care information.

B. "**Electronic form**" means all mechanical, non-paper formats, including fiberoptic transmission and laser disc storage.

C. "**External Disclosure(s)**" means:

(1) All disclosures of individually identifiable health care information to person(s) who are not employed or credentialed by, or who do not have an independent contractor relationship with a payor or provider; and

(2) Which are made on behalf of the individual and are directly related to either the adjudication of a claim, coordination of benefits, or to the medical treatment of an individual.

D. "**Health care**" means:

(1) Any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service or procedure provided by a provider:

(a) with respect to an individual's physical or mental condition; or

(b) affecting the structure or function of the human body or any part thereof, including, but not limited to, banking of blood, sperm, organs, or any other tissue; and

(2) The prescription, sale or dispensing of any drug, substance, device, equipment, or other item to an individual or for an individual's use for health care.

E. "**Individual**" means a natural person who is the subject of individually identifiable health care information, and includes the individual's legal representative.

F. "**Individually identifiable health care information**" means any data or information that identifies or can reasonably be associated with the identity of an individual, either directly or by reference to other publicly available information, and:

(1) Relates to the individual's health history, health status, health benefits, or application therefor; or

(2) Is obtained in the course of an individual's health care from a provider, from the individual, from a member of the individual's family, or from a person with whom the individual has a close personal relationship.

G. "**Person**" means a government, governmental subdivision, agency or authority, natural person, corporation, estate, trust, partnership, association, joint venture, and any other legal entity.

H. "**Provider**" means a person that is duly authorized, or that represents itself as being duly authorized to provide health care.

I. "**Secretary**" means . . .

SECTION 4 - PREEMPTION

Unless otherwise provided in Section 2 C, upon the effective date of regulations implementing this Act, no effect shall be given to any provision of state law that requires individually identifiable health care information to be maintained exclusively in written rather than electronic form or to any provision of state law to the extent it relates to the matters covered in this Act, including the preservation of confidentiality and privacy rights in the collection, storage, processing, and transmission of individually identifiable health care information (including initial and subsequent disclosures) in electronic form by all involved in such transactions.

SECTION 5 - STANDARDS FOR INFORMATION PRACTICES

A. The Secretary shall, by regulation, establish appropriate levels of security, standards, and controls including but not limited to passwords, access codes, restrictions on access, limitations on networking and electronic data sharing, and protocols and procedures for preventing computer sabotage, for collecting, storing, processing and transmitting individually identifiable health care information in electronic form so as to ensure the

privacy and confidentiality of such information, taking into consideration the nature of the information and relative risks of disclosure.

B. The regulations promulgated pursuant to Section 5 A shall incorporate the following principles:

(1) The individual shall have the right to know that individually identifiable health care information concerning the individual is collected, stored, processed or transmitted by any person, and to know for what purpose such information is used.

(2) Individually identifiable health care information shall be collected, processed, stored and transmitted only to the extent necessary to carry out a legitimate purpose for which the individual has granted consent.

(3) Each person collecting individually identifiable health care information from an individual shall notify the individual of his or her right to receive a statement, in the style and form prescribed by the Secretary, summarizing the individual's rights pursuant to this Act.

(4) The individual shall have a right of access to individually identifiable health care information concerning the individual from the person collecting such information, the right to have a copy of such information after payment of a reasonable charge, and the right to have a notation made with or in such information of any amendment or correction requested by the individual.

(5) Persons collecting, processing, storing or transmitting individually identifiable health care information shall implement or cause to be implemented as the case may be, the appropriate security standards and controls promulgated by the Secretary to assure the accuracy, reliability, relevance, completeness, timeliness and security of such information.

SECTION 6 - DISCLOSURE

A. Disclosure. Except as authorized in Section 6 D, no person other than an individual shall disclose individually identifiable health care information to any other person without the individual's valid authorization as provided in Section 6 C. No person shall disclose such information except in accordance with the terms of such authorization, unless otherwise authorized under Section 6 D.

B. Record of Disclosures. Each person collecting or storing individually identifiable health care information shall maintain a record of all external disclosures made on behalf of a provider, payor or individual of such information.

C. Individual Authorization: Requirements for Validity.

(1) To be valid, an authorization to disclose individually identifiable health care information must –

(a) Identify the individual;

(b) Describe the health care information to be disclosed;

(c) Identify the person to whom the information is to be disclosed;

(d) Describe the purpose of the disclosure;

(e) Indicate the length of time for which the individual's authorization will remain valid;

(f) Be either,

(i) In writing, dated and signed by the individual; or

(ii) In electronic form, dated and authenticated by the individual using a unique identifier; and

(g) Not have been revoked under Section 6 C (2).

(2) Revocation of Individual's Authorization. An individual may revoke the individual's authorization at any time, unless disclosure is required to effectuate payment for health care that has been provided to the individual, or other action has been taken in reliance on the individual's authorization. An individual may not maintain an action against a person for disclosure of individually identifiable health care information made in good faith reliance on the individual's authorization, provided the disclosing person had no notice of the revocation of the individual's authorization at the time disclosure was made.

(3) Record of Individual's Authorizations and Revocations. Each person collecting or storing individually identifiable health care information shall maintain a record of each individual's authorization and revocation thereof, and such record shall become part of the

individually identifiable health care information concerning such individual.

(4) No Waiver. Except as provided by this Act, an authorization to disclose individually identifiable health care information by an individual is not a waiver of any rights an individual has under other federal or state statutes, the rules of evidence, or common law.

D. Disclosure Without An Individual's Authorization. A person may disclose individually identifiable health care information without the individual's authorization required in Section C if:

(1) The disclosure is by a family member or by any other person with whom the individual has a close personal relationship, unless such disclosure is expressly limited or prohibited by the individual;

(2) The disclosure is only to the extent necessary for the disclosing person to carry out its lawful activities and is to the disclosing person's agent, employee, or independent contractor who is under an obligation to hold the individually identifiable health care information in confidence and not to use such information for any purpose other than the lawful purpose for which the information was obtained by the disclosing person;

(3) The disclosure is to a provider who is providing health care to the individual except as such disclosure is limited or prohibited by the individual;

(4) The disclosing person reasonably believes that disclosure is necessary to avoid or minimize imminent danger to the health or safety of any individual, but only to the extent necessary to avoid or minimize such danger or emergency;

(5) The disclosure is to a member of the individual's immediate family, or to any other individual with whom the patient is known to have a close personal relationship, if such disclosure is made in accordance with good medical or other professional practice, unless such disclosure is expressly limited or prohibited by the individual;

(6) The disclosure is to a successor in interest to the person maintaining the individually identifiable health care information, provided, however, that no person other than a provider or the estate of a deceased provider shall be considered a successor in interest to a provider;

(7) The disclosure is to federal, state, or local government authorities, to the extent the person holding the individually identifiable health care information is required by law to report specific individually identifiable health care information:

(a) when needed to determine compliance with state or federal licensure, certification, or registration rules or laws; or

(b) when needed to protect the public health;

(8) The disclosure is to a person solely for purposes of conducting an audit, if that person agrees in writing:

(a) to remove or destroy, at the earliest opportunity consistent with the purpose of the audit, information that would enable identification of the individual;

(b) not to disclose in any report any individually identifiable health care information; and

(c) not to further disclose the information, except to accomplish the audit or to report unlawful or improper conduct involving health care fraud by a provider or the individual or other unlawful conduct by a provider;

(9) The disclosure is for use in a research project that:

(a) is of sufficient importance to outweigh any potential harm to the individual that would result from the disclosure;

(b) is reasonably impracticable without the use of the individually identifiable health care information;

(c) contains reasonable safeguards to protect the information from redisclosure;

(d) contains reasonable safeguards to protect against identifying, directly or indirectly, any individual in any report of the research project;

(e) contains procedures to remove or destroy at the earliest opportunity, consistent with the purposes of the project, information that would enable identification of the individual, unless retention of identifying information is required for purposes of another research project that also satisfies the requirements of this Section; and

(i) the person agrees in writing:

(I) to remove or destroy, at the earliest opportunity consistent with the purpose of the research information that would enable identification of the individual;

(II) to not disclose individually identifiable health care information, except as necessary to conduct the research project;

(10) The disclosure is in accordance with a discovery request:

(a) Before service of a discovery request on a person maintaining individually identifiable health care information, an attorney shall provide advance notice to the person and to the individual involved or the individual's representative or attorney through service of process or first class mail, indicating what information is sought, and the date by which a protective order must be obtained to prevent the person from complying. Such date shall give the individual and the person adequate time to seek a protective order, but in no event be less than fourteen days after the date of service of such notice;

(b) Without the individual's authorization, a person may not disclose the information sought under paragraph (a) if the requestor has not complied with the requirements of paragraph (a). In the absence of a protective order issued by a court of competent jurisdiction forbidding compliance, the person shall disclose the information in accordance with this section. In the case of compliance, the request for discovery or compulsory process shall be maintained by the holder thereof with the individual's health care information;

(c) Production of individually identifiable health care information under this section, in and of itself, does not constitute a waiver of any privilege, objection, or defense existing under other law or rule of evidence or procedure;

(11) The disclosure is to federal, state or local law enforcement authorities to the extent required or permitted by law;

(12) The disclosure is directed by a court in connection with a court-ordered examination of an individual; or

(3) The disclosure is based on reasonable grounds to believe that the information is needed to assist in the identification of a deceased individual.

E. Obligations of Legal Representatives.

(1) A person authorized to act as an individual's legal representative may exercise the rights of the individual under this Act to the extent necessary to effectuate the terms or purposes of the grant of authority; but an individual who is a minor and who is authorized to consent to health care without the consent of a parent or legal guardian under State law may exclusively exercise the rights of an individual under this Act as to information pertaining to health care to which the minor lawfully consented.

(2) An individual's legal representative shall act in good faith to represent the best interests of the individual with respect to individually identifiable health care information.

SECTION 7 - PUBLICATION

Persons collecting individually identifiable health care information shall, pursuant to regulations, periodically publicize the existence of the information and provide information regarding procedures for obtaining and correcting the information.

SECTION 8 - AMENDMENT OF INDIVIDUALLY IDENTIFIABLE HEALTH CARE INFORMATION

A. Within thirty (30) business days from the date of receipt of a written request from an individual to amend any individually identifiable health care information about the individual within its possession, a person collecting, storing or processing such information shall either:

(1) Amend the portion of the recorded individually identifiable health care information identified by the individual, or

(2) Notify the individual of:

(a) Its refusal to make such, amendment;

(b) The reasons for the refusal, and

(c) The individual's right to file a statement as provided in Subsection 8C.

B. If the person amends information in accordance with Subsection 8 A above, the person shall provide the amendment to:

(1) The individual;

(2) Any person specifically designated by the individual who may have, within the preceding two (2) years, received such information;

(3) Other persons who have systematically been provided such information within the preceding seven (7) years; provided, however, that the amendment or fact of deletion need not be furnished if the other person no longer maintains such information about the individual; and

(4) Any person that provided the information that has been amended.

C. Whenever an individual disagrees with a person's refusal to amend individually identifiable health care information, the individual shall be permitted to file with such person:

(1) A concise statement setting forth what the individual believes to be correct, relevant or fair information; and

(2) A concise statement of the reasons why the individual disagrees with the refusal to amend such information.

D. If an individual files either statement as described in Subsection C above, the person shall:

(1) Include the statement with the disputed individually identifiable health care information and provide a means by which anyone reviewing such information will be made aware of the individual's statement and have access to it;

(2) With any subsequent disclosure of the information that is the subject of disagreement, clearly identify the matter or matters in dispute and provide the individual's statement along with the information being disclosed; and

(3) Provide the statement to the persons and in the manner specified in Subsection 8 B above.

E. The rights granted in this section shall not apply to individually identifiable health care information that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving the individual.

SECTION 9 - ALTERNATIVE DISPUTE RESOLUTION

The Secretary shall promulgate regulations that will promote the resolution of disputes arising under this Act through alternative dispute resolution mechanisms.

SECTION 10 - PROMULGATION OF REGULATIONS

A. In promulgating regulations under this Act, the Secretary shall follow the procedures authorized under the "Negotiated Rulemaking Act of 1990," 5 U.S.C. §§ 581-590.

B. If the Secretary determines that a negotiated rulemaking committee shall not be established as permitted by 5 U.S.C. § 583, the Secretary shall appoint and consult with an advisory group of knowledgeable individuals. The advisory group shall consist of at least seven (7) but no more than twelve (12) individuals from the following areas: (1) health care financing and reimbursement; (2) health care delivery, including representatives of health care professionals and health care entities; (3) third party payors/administrators, network administrators; and (4) health care consumers.

C. The advisory group shall review all proposed rules and regulations and submit recommendations to the Secretary. The advisory group shall also assist the Secretary: (1) in establishing the standards for compliance with rules and regulations; and (2) in developing an annual report to the Congress on the status of the requirements set forth in this Act, their cost impact, and any recommendations for modifications in order to ensure efficient and confidential electronic data interchange of individually identifiable health care information.

SECTION 11 - CIVIL REMEDIES

A. An individual aggrieved by a violation of this Act may maintain an action for relief as provided in this section.

B. The district courts of the United States shall have exclusive jurisdiction in any action brought under the provisions of this section.

C. The court may order a person maintaining individually identifiable health care information to comply with this Act and may order any other appropriate relief.

D. If the court determines that there has been a violation of this Act, the aggrieved individual shall be entitled to recover damages for any losses sustained as a result of the violation; and, in addition, if the violation results from willful or grossly negligent conduct, the aggrieved individual may recover not in excess of $10,000, exclusive of any loss.

E. If an aggrieved individual prevails in an action brought under this section, the court, in addition to any other relief granted under this section, may award reasonable attorneys' fees and all other expenses incurred by the aggrieved individual in the litigation.

F. Any action under this Act must be brought within two years from the date on which the alleged violation is discovered.

SECTION 12 - CIVIL MONEY PENALTIES

Any person that knowingly discloses health care information in violation of this Act shall be subject, in addition to any other penalties that may be prescribed by law –

A. to a civil money penalty of not more than $10,000 for each violation, but not to exceed $50,000 in the aggregate for multiple violations; and, in addition -

B. to a civil money penalty of not more than $100,000 if the Secretary finds that violations of this Act have occurred with such frequency as to constitute a general business practice.

SECTION 13 - IMMUNITY

It shall be an affirmative defense in actions brought for improper disclosure of individually identifiable health care information that such disclosure was in accordance with the requirements of this Act and regulations promulgated pursuant to this Act.

SECTION 14 - CRIMINAL PENALTIES FOR OBTAINING INDIVIDUALLY IDENTIFIABLE HEALTH CARE INFORMATION THROUGH FALSE PRETENSES OR THEFT

A. Any person who, under false or fraudulent pretenses, requests or obtains individually identifiable health care information shall be fined not more than $50,000 or imprisoned not more than six months, or both, for each offense.

B. Any person who unlawfully takes, or under false or fraudulent pretenses, requests or obtains individually identifiable health care information and who intentionally uses, sells or transfers such information for remuneration, for profit or for monetary gain shall be fined not more than $100,000, or imprisoned for not more than two years, or both, for each offense.

SECTION 15 - SEVERABILITY

If any provision of this Act or its application to any person or circumstances is held invalid, it shall not affect other provisions or applications of this Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 16 - EFFECTIVE DATE

Except as provided in Section 4, this Act shall become effective upon enactment.

Senator LEAHY. Thank you very much. I appreciate you being here.

Ms. Goldman, why don't we have your statement, too, and then I will go to questions for both of you.

STATEMENT OF JANLORI GOLDMAN

Ms. GOLDMAN. Thank you very much for inviting me to testify here today on this issue. I just want to say at the outset that the ACLU really appreciates your continued commitment to privacy issues and we look at you really as kind of a bedrock here in the Senate on these issues.

The privacy project thinks that there is no more critical issue today, the privacy issue, than protecting health care records of individuals. As we heard from the Congresswoman earlier, there is no more personal or sensitive information in this country than health care records. Protecting the information is not a new issue. Here we are talking about getting Federal legislation to protect these records. It is really shocking that we do not have such legislation today. It is not a new issue. It was an issue 20 years ago.

The Congress looked at enacting legislation 15 years ago. They were not ultimately successful. There was a change in administrations just as momentum was getting going here. But I think we have an opportunity, because health care reform is the number one issue, we have an opportunity, and I believe a responsibility, to take up this issue today. It is clearly a bipartisan issue, as Senator Dole mentioned after the State of the Union address. This issue is something that people care about across the board.

I also want to underscore that even if we do not have health care reform this year, we need Federal legislation to protect these records. Health care reform only gives us an opportunity to take this step.

The Adminstration's plan clearly has some laudable goals: universal coverage, lowering cost, improving quality of care, and we do not want to interfere with those. We want to ensure that whatever electronic data system is put into place, whatever system is put it into place that that will foster those goals.

We also want to acknowledge up front that HHS and the Administration as a whole has taken a really big step in acknowledging the need to protect personal information. But it has failed, and I think fatally so, to put forth a statutory proposal in the Health Security Act. It reads like a statement of principles, which it is, and very good principles and strong principles.

But all the policymaking is delegated to a national health board. This board is not in place. We do not know to what extent they would turn the principles into statutory protections, and I do not think we can afford to wait for that to happen. Certainly, we cannot put a system into place and then enact the privacy protections to safeguard the information. Any security expert will tell you that that is certainly a backwards way to do the job, and a very dangerous one. Some would even tell you that it is unworkable; that you cannot——

Senator LEAHY. Doesn't it also have the problem that if you do it after the fact you may find yourself having to either re-work some of the health legislation itself or be locked into a situation

where you do not have as much ability to put in a security system; is that a fair statement?

Ms. GOLDMAN. Absolutely. Most people will tell you—in fact, I do not find anyone in the security area who will tell you otherwise—that many of the privacy policies are put into place as software design matters. That you design a system based on the policy that is set forth.

So here we are working kind of with these amorphous standards and nothing that really makes it happen. So I think that the Administration needs to take another crack at this and draft some statutory principles. As difficult as that may be, I certainly do not think we need 3 years to do it. They have had a year really to do this and I would like to see them come back with a statutory proposal.

I think many of these issues have already been pointed out. We are looking at the creation of an electronic data network. The act calls for that; a card, some kind of a unique identifier. These are the kinds of things that are going to make the American public extremely nervous about participating in a system if they are not assured that the information will be protected.

It is all well and good to say that we are only going to use the card for one very limited purpose. But it is another thing if you are a historian and you look back on how information systems have developed in this country. The Social Security number was created for an extremely limited purpose. Some may remember that. It said that on the card. We now know that it is a de facto national identifier. The criminal history records system in this country was developed for one limited purpose: to assist law enforcement. It is now used primarily—certainly when a fingerprint is sent to the FBI—primarily for non-law enforcement purposes.

So information which is collected by the Government and the public is given assurance it is only going to be used for a limited purpose, the temptations to use it for other purposes become irresistible. And I submit to you that this will happen in the health care area. So I am extremely nervous, even though I recognize that we have some very laudable goals here, I am very nervous about the large scale creation of a data base, a card, a number.

There are some in my organization, particularly in the immigration context, who say a card should not be created at all because it will become not only a de facto national ID card, but it will be used in the immigration context, it will be used in a way which will discriminate against people of color, people with foreign-sounding names, people with accents, and that this is a very real concern. We have already heard calls for a national ID card in other contexts, and if this card is used for all Americans who are eligible for benefits I think you will see real abuses and probably Congress at some point—not with your support, I understand—but Congress will at some point legitimately authorize the use of the card for other purposes.

Again, I don't think we can wait in the legislation for legislative standards. The ACLU is working closely with a coalition currently of consumer groups, industry groups, health care professionals to craft legislation and to have the proposal considered by Congress. Out of a series of conferences, meetings and hearings this last year

and the year before a consensus is emerging, and I think you are hearing it here today, that we need strong statutory protection.

The National Academy of Science's Institute of Medicine just issued a report calling for Federal legislation, strong Federal legislation that restricts disclosure of personal health records. The Office of Technology Assessment just issued a report calling for the same kinds of recommendations. I think the public will not tolerate a delay. If they do not believe that they can trust the health care system, that they have confidence in the health care system, they will not participate.

So while we are providing universal coverage, I'm not sure that everyone will seek it under this kind of a scheme. We heard that again from the Congresswoman.

To conclude, we recognize that the technology here does present some tremendous opportunities, but it also presents threats. The technology is neutral, it is the policy that will guide how the technology is used.

The Supreme Court has held, in a decision called *Whelan* v. *Roe,* that there is a constitutional right to privacy in health records, it is just a question of whether the state can adequately protect the information. It is up to Congress to make sure that that happens. I think most poignantly—and it has been overstated, but most poignantly, Congresswoman Velazquez said that it is easier to get access to someone's medical records than to get a copy of their video rental list. That is a tragedy.

The only reason that is so is because there was an unethical disclosure of Robert Bork's video rental list, as you will recall, during his confirmation hearings.

Senator LEAHY. I wrote the law to block disclosure after the hearing. I did not know you could get it before that hearing.

Ms. GOLDMAN. That is interesting. Most people do not know that you can get copies of health care records. I do not think the Congresswoman anticipated someone could get a copy of her health care record. It is not something you think about when you seek health care.

So we do not want to wait for more situations, more tragedies, like the Congresswoman's, before we act here. I think we know that there is a problem and we can act to remedy it.

[The prepared statement of Ms. Goldman follows:]

PREPARED STATEMENT OF JANLORI GOLDMAN ON BEHALF OF THE AMERICAN CIVIL LIBERTIES UNION'S PRIVACY AND TECHNOLOGY PROJECT

I. OVERVIEW

Chairman Leahy and Members of the Subcommittee: I very much appreciate the opportunity to testify before you today on behalf of the American Civil Liberties Union (ACLU). The ACLU is a private, non-profit organization of over 275,000 members, dedicated to the preservation of the Bill of Rights. The ACLU's Privacy and Technology Project was established in 1984 to evaluate the impact of new technology on individual privacy. Over the years, the Project has worked to develop strong privacy policy in numerous areas, including credit reporting, electronic communications, video rental lists, and criminal justice information systems. We have often worked closely with this subcommittee on these privacy issues, and we look forward to continuing to assist you in crafting legislation to protect health records.

The Project's primary goal for the 103rd Congress is the passage of federal legislation that establishes enforceable privacy protection for personal health information. We believe that the need for such legislation is the most critical privacy issue facing

this country today. The absence of a strong federal law to protect peoples' health records is troubling. In fact, a recent Louis Harris survey found that most people live under the mistaken belief that their health records are protected by the law. Protecting the privacy of people's health records must be at the heart of any health care reform plan.

The Project has been working with a diverse coalition of industry representatives, consumer advocates, and health policy specialists to develop a consensus on a privacy policy for health records.

The societal impact of technological innovations—including those that allow medical records, data and images to be transferred easily over great distances—will continue to be staggering. The development of a national information infrastructure and the information superhighway are changing the ways we deal with each other. While the information revolution holds great promise for enhancing the way we communicate with each other, we must ensure that new technologies operate within enforceable privacy rules.

There is no doubt that the collection and use of personal health information will eventually take place in an electronic networked environment. Traditional barriers of distance, time and location are disappearing as information and transactions are computerized. Few relationships in the health care field will remain unaffected. As these changes are taking place, there is a conflict between individuals' need to keep health information confidential and the economic opportunities posed by the computerization of health records, from lowering the cost of processing insurance claims to selling personal medical records for marketing purposes.[1]

We applaud this Subcommittee and its Chairman for holding this hearing. Our statement today outlines the imminent need for federal legislation that creates an enforceable privacy right for personal health records, the public's support for such a measure, and our recommendations for essential components of the legislation.

II. THE HEALTH SECURITY ACT

Recent proposals to reform this country's health care system rely heavily on the automation and linkage of personal health information as a means to reduce costs, improve efficiency and quality of care, and extend universal coverage.[2] The Administration's Health Security Act, would require the creation of a national, linked electronic data network containing vast amounts of biographical and health information on virtually every American. Under the Act, people will be required to carry a Health Security Card to verify identity and eligibility, and to access and exchange health information. The Act requires the creation of an "electronic data network consisting of regional centers that collect, compile and transmit information." (Sec.5103) The Health Security Card, with a unique identifier, (Sec. 5104, Sec. 5105) would be issued to all eligible individuals. The Act leaves open the question of whether the unique identifier will be the Social Security Number or some other identifier.

In its bill, the Administration does address the need to protect the confidentiality of personal information held in health information systems (Title V, Subtitle B), but, we believe, inadequately. All of the responsibility for developing privacy standards and a legislative blueprint is delegated to the National Health Board. From the date of enactment, the Board is given two (2) years to promulgate standards for the privacy and security of individually identifiable health information (section 5120(a)), and three (3) years to submit a legislative proposal to provide a comprehensive scheme of federal privacy protection (section 5122).

The Act requires that, in developing legislation and standards, the Board must incorporate principles of fair information practices. The principles outlined in the Act are strong and can provide the base for an enforceable, effective privacy law. Under the principles, disclosures of personal information would be strictly limited. People could retrieve their own information, and consent to disclosures of third parties. Law enforcement is given access for limited health-related functions. Use by

---

[1] For instance, in a television advertisement from last year, a phone company promises a medical service * * * that could improve the quality of health care for millions of Americans. A doctor in a small town can transmit relevant information about a patient to leading experts in the field. This is just one example of how Americans will benefit from recent breakthroughs. Many more advanced services could be available if your local phone companies are allowed to offer their customers the fullest range of services that technology allows.

Or consider, for example, the medical implications of AT&T's Hobbit, a handheld personal communicator that combines the functions of a cellular phone, fax machine, and personal computer. With it, a doctor could communicate with colleagues across town or across the country, send and receive medical data and x-ray images, and fax a prescription to a pharmacy.

[2] *See* S. 1494 and H.R. 3137, bills to establish an electronic health care information network.

employers would be absolutely barred. Further, individuals would be given notice of how information would be collected, used and shared.

While the Administration is to be commended for acknowledging the need to protect the privacy and confidentiality of medical records. The Act lacks a legislative proposal to accomplish its privacy goals. We do not believe the overall Act can be implemented without statutory privacy policy in place from the outset. It is very difficult, if not impossible, to build privacy and security protections into a system once it is already in place. Privacy policy that requires certain protections must be the guide that shapes the creation of health information systems. For instance, the Act requires the creation of a electronic data network that will link regional centers that collect, compile and transmit information. Such an amassing of the most sensitive, personal information will seriously jeopardize peoples' privacy if legal requirements are not in place form the outset.

Further, the Act requires the creation of a health security card and a unique identifier system for individuals. The Board is given substantial discretion in determining the identifier and type of card. We believe these issues should be resolved in the initial legislation.

We support the provision in the Act limiting the use of the card to the health care context. The personal information collected for inclusion into the electronic data network should not be used for any non-health related purpose. It is important to recognize, however, that such a comprehensive, linked database will pose a great temptation to others in the private and public sector who will want access to the information for a variety of purposes, ranging from marketing to law enforcement. Once the network is in place it will be very difficult for Congress to limit its use.

The history on this issue is replete with information systems being created for a limited purpose, only to be expanded in the future due to pressure. We have seen this pattern with the social security number, created for a limited purpose, sixty years ago and now a de facto national identifier, and the FBI's criminal records systems, initially developed for law enforcement use but now used primarily by the non-law enforcement community. To prevent the expanded use of the electronic data network, Congress must be committed to maintaining the Act's initial objectives.

More importantly, we are concerned about the creation of a card which will be especially vulnerable to use and misuse for purposes other than health care. It is not hard to imagine the Health Security Card burgeoning into a national ID card. The pressure to move in this direction —once the card is linked to a national database on all Americans—will be irresistible. We urge Congress to move cautiously in this area and consider seriously whether a card is needed at all.

Finally, we urge that the social security number not be selected as the method of individual identification due to its widespread use for both public and private purposes, the use of the social security number will jeopardize the privacy and security of personal health information maintained under the Act. The Social Security Administration has testified before Congress that the number is not a reliable identifier due to the high percentage of duplicate, fraudulent and inaccurate numbers. Currently, there is no way to verify the accuracy of existing numbers or that the number holder is who he or she claims to be. Finally, because the social security number has become the most widely used identifier—even on most driver's licenses—health records would become vulnerable to abuse.

The Act should require the board to develop a new unique identifier, limited to the health care context. To build a new system that's success hinges on absolute security, the existing shaky system will put American's health records at risk. The better approach, albeit more costly in the beginning, is to devise a new identification scheme unique to the individual and the health care system.

III. THE NEED FOR FEDERAL PRIVACY PROTECTION

Currently, at the state and local level, employers, insurers, and health care providers are forming coalitions to develop automated and linked health care systems containing lifetime health histories on millions of Americans. Again, the goals are cost reduction and improved quality of care. Attempts are being made by some in these state coalitions to address the privacy, confidentiality and security of health data by crafting internal guidelines, regulations and contracts. In states where the automation of health care information is seen as a key component of the state's health care reform package, the state legislatures and public agencies are attempting to enact legislation that establishes a right of privacy in personally identifiable health care information. The states are also attempting to design effective enforcement penalties and oversight mechanisms to monitor the information practices of these newly created health data systems.

The outcome of this piecemeal, state by state, approach to protecting the privacy and security of health care information will be conflict amongst the states and a setback for the overall goals of privacy protection. Relegating the protection of health care information to the states' different guidelines, policies and laws leaves individuals subject to wavering degrees of privacy protection depending upon where they receive their health care. In some instances, this means that individuals traveling across county or state lines to receive necessary medical treatment may lose their ability to control how their personal medical information is used. Further, such a patchwork approach to health information privacy will hamper national health care reform. The various states and local governments with rules governing the use of health care information may be prevented from sharing health care information contained in their systems with neighboring states that insufficiently protect privacy.

Health care records, in both paper and electronic form, are deserving of privacy protection, but the vulnerability of the information to unauthorized use grows exponentially as the computer makes possible the instant sharing of information. As a recent study pointed out: "The paper medium is cumbersome and expensive . . . Ironically, it is the 'negative' aspect of the paper medium . . . that has minimized the risk of breaches of confidentiality. Although a breach could occur, if someone gave access to health records or insurance claim forms, the magnitude of the breach was limited by the sheer difficulty of unobtrusively reviewing large numbers of records or claim forms."[3]

Nevertheless, technology is not the evil. Information systems can be designed to promote the confidentiality and security of personal information. For instance, a health security card could be used as a means of giving individuals greater control over their medical records, allowing them to determine and control the access to and exchange of personal information. The key here is to recognize technology's potential to enhance privacy, not just undermine it.

There is widespread agreement among privacy and security experts that protections must be built in on the front-end; it is too difficult and risky to try to add them once a system is already in place. Privacy and security must be viewed as the foundation on which health information networks are created. Health care reform is more vulnerable to failure if privacy protections are not in place from the outset. Americans must have confidence that their personal health information will be guarded before they will fully and willingly participate in a new system.

IV. PUBLIC DEMAND FOR PRIVACY PROTECTION

A consensus is emerging that federal legislation is needed to protect the privacy of personal health care records. At a conference in Washington, D.C. this past November co-sponsored by the U.S. Office of Consumer Affairs, the American Health Information Management Association, and Equifax, nearly every panelist and member off Congress supported the need for making privacy an integral part of health care reform. Both the Chairman of this Subcommittee, Patrick Leahy (D–VT) and Representative Pete Stark (D–CA) insisted that privacy must be the cornerstone of any health care reform plan. In agreement were panelists from the American Medical Association, CIGNA Health Care, the U.S. Public Interest Research Group, Computer Professionals for Social Responsibility and IBM.

At the conference, Louis Harris and Associates released their *Health Information Privacy Survey,* prepared with the assistance of Dr. Alan Westin, of Columbia University. The survey found that the majority of the public (56 percent) favor the enactment of strong comprehensive federal legislation governing the privacy of health care information. In fact, eighty-five percent say that protecting the confidentiality of medical records is absolutely essential or very important in national health care reform. Specifically, most people want penalties imposed for unauthorized disclosure of medical records (96 percent), guaranteed access to their own records (96 percent), and rules regulating third-party access. In addition, most people support the need for an independent, neutral Board to issue regulations and enforce standards on privacy matters (86 percent).

More broadly, the Harris survey found that a large majority of Americans (80 percent) are concerned or very concerned about threats to their privacy. A 1992 Harris survey showed that while a large majority of people recognize the benefits to society of innovative technology, nearly nine out of ten people also believe that computers make it easier for someone to improperly obtain confidential personal information. As a result, over two-thirds of the public support tough restrictions on the use of computers.

---

[3] Workgroup for Electronic Data Interchange, *Report to the Secretary of the U.S. Department of Health and Human Services,* July, 1992, Appendix 4, pp. 3–4.

Health care reform cannot move forward without assuring the American public that the highly sensitive personal information contained in their health care records will be protected from misuse and abuse. As the most recent Harris survey reveals, individuals are highly suspicious of large scale computerization and believe their medical records are in dire need of privacy protection. If people are expected to embrace a reformed health care system, the price of their participation must not be a loss of control over the sensitive information contained in their health care records.

The unauthorized disclosure of personal health information can have disastrous consequences. New York Congresswoman Nydia Velazquez won her House seat only after overcoming the results of an unauthorized disclosure. Her medical records—including details of a bout with depression and suicide attempt—were faxed to a New York newspaper and television station during her campaign.

More common—and in some ways more troubling than the well-publicized privacy invasions of political figures—are the consequences suffered against ordinary individuals whose privacy has been compromised by the disclosure of medical information.

In one instance, a journalist disguised himself as a doctor, obtained an actress' medical record and published that she had been treated for a sexually transmitted disease. In another case, a physician at a large New York City medical school logged on to a computer system, discovered that a nurse was pregnant, and proceeded to publicize that information. Finally in Colorado, a medical student sold medical records to attorneys practicing malpractice law. These are stories that are known; undoubtedly there are millions of similar breaches that occur without knowledge of the individuals harmed. The 1993 Harris survey found that nearly 50 million people have suffered the unauthorized disclosure of medical information.

Further, errors in peoples' medical records have been difficult to correct and control. For instance, Mary Rose Taylor of Springfield, Massachusetts went without health insurance for a year and a half because of a computer error at the Medical Information Bureau (MIB), a huge medical database kept by insurance companies. MIB reported that Ms. Taylor had an abnormal urinalysis, even though she'd had only a blood test. She was forced to go to the insurance commissioner of her state to have the error corrected so that she could finally receive health insurance.

Despite the horror stories—both public and private—many Americans trust that the information they share with their doctor is kept private. The traditional nature of the doctor-patient relationship is intended to foster trust and to encourage full disclosure. However, once the patients's information is submitted to a third-party payor, or to any other entity, the ethical tie between doctor and patient evaporates. In fact, in a particularly telling statistic, 93 percent of those termed "leaders" in the Harris survey, including hospital CEOs, health insurance CEOs, physicians, nurses, and state regulators, believe that third party payors need to have detailed confidentiality and privacy policies.

Within our current health care system, people are trying to protect themselves against potential privacy violations. Some people routinely ask doctors to write down a false diagnosis because they fear their employer may see their records, or some people don't even tell their doctors everything about their condition for fear of losing control over this sensitive information. In psychiatric practices, it is common for many patients to ask that the doctors not take notes during sessions out of fear they could be leaked or even obtained legally with a subpoena. Also, some people try to avoid the creation of a record altogether by paying for medical services out of their pockets, even though they are entitled to insurance coverage.

A few insurers have been candid enough to concede that their economic, business relationship is with the employer and not the patient. They might be reluctant to disclose individually-identifiable information requested by an employer, but they will comply if pressed. No federal law prevents disclosures by insurers to employers. Most patients, of course, think the fiduciary relationship is with them, and don't realize that a third-party with no direct relationship to their medical treatment, "owns" the information. It is intolerable to support a system in which an employer's payment of a portion of employees' health care premiums, a normal part of most American employee's compensation packages, amounts to employers owning their employees' health records.

In the end, any system that fails to win the public's trust will fail to win the public's support. Once the public recognizes that their right to control information about themselves within a health information system is weak, they will withdraw from full and honest participation. To allow individuals to fall through the cracks because their privacy is not protected, is as serious as health care coverage that does not extend far enough.

In essence, people should not be forced to give up their privacy and their right to control information about themselves as the cost of participation in society—and especially as a cost of receiving quality health care.

Presently, a great deal of attention is being focused on establishing a privacy law to protect personal health records. In October 1993, this Subcommittee held hearings on "High Tech Privacy Issues in Health Law." The next month, the House Subcommittee on Government Information, Justice and Agriculture of the Committee on Government Operations held a hearing on the confidentiality of health care records. The House Subcommittee, chaired by Gary Condit (D–CA) is in the process of drafting a health information privacy bill.

The Office of Technology Assessment (OTA) recently issued a report entitled "Protecting Privacy in Computerized Medical Information," which addresses the effects of the computerization of medical records on people's privacy. In recommending comprehensive federal legislation, OTA found that:

> (t)he expanded use of medical records for nontreatment purposes exacerbates the shortcomings of existing legal schemes to protect privacy in patient information. The law must address the increase in the flow of data outward from the medical care relationship by both addressing the question of appropriate access to data and providing redress to those that have been wronged by privacy coalitions. Lack of such guidelines, and failure to make them enforceable, could affect the quality and integrity of the medical record itself. (OTA Report, p. 44).

Further, the National Academy of Science's Institute of Medicine just released a study that focused on the risks and opportunities associated with protecting the privacy and confidentiality of personally-identifiable health data. The IOM report recommenda that the U.S. Congress enact preemptive legislation that will "establish a uniform requirement for the assurance of confidentiality and protection of privacy rights for person-identifiable health data and specify a Code of Fair Health Information Practices that ensures a proper balance among required disclosures, use of data, and patient privacy." (Recommendation 4.1). The Committee also recommended that a responsible administrative unit or board be established. Also, the Department of Health and Human Services Task Force on the Privacy of Private Sector Records sponsored a conference last year on the confidentiality of health records. All of these efforts represent a tremendous pulling together of the public and private sector to achieve a critical goal—the passage of a health records privacy law.

Over fifteen years ago, there waa similar pressure to craft such a privacy law. In 1977, the federal Privacy Protection Study Commission issued a report recommending legislation to protect private sector records, including medical and insurance records. The Commission's recommendations sparked the only other Congressional effort to enact a medical records privacy bill. In 1980, due in part to pressure from the law enforcement community for unfettered access to health records, the legislative effort failed.

Given today's focus on reforming our nation's health care system, the opportunity to enact legislation in 1994 appears far more viable than it did 15 years ago.

V. RECOMMENDATIONS

Congress has enacted legislation that gives people expectations of privacy in certain information held by others, including credit,[3] education,[4] financial,[5] cable,[6] and video records.[7] In all of these instances, Congress created statutory rights of privacy in personal information. Congress has acted either to counter the refusal of the Supreme Court to extend privacy protections or to respond to new technologies overtaking current law.

The following are our recommendations for the key provisions we believe should be included in a federal health records privacy law:

> 1) Personally-identifiable health records must be in the control of the individual. Personal information may only be disclosed with the knowing, meaningful consent of the individual;

---

[3] Fair Credit Reporting Act, § 15 U.S.C. 1681 (1970).
[4] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232 (1974).
[5] Right to Financial Privacy Act, 12 U.S.C. § 3401 (1978).
[6] Cable Communications Policy Act, 47, U.S.C. § 551 (1984).
[7] Video Privacy Protection Act, 18 U.S.C. § 2710 (1988).

2) Limits on access and disclosure should apply to all personally identifiable health data regardless of the form in which the information is maintained;

3) Information that is not personally-identifiable may be provided for research and other purposes;

4) Health record information systems must be required to build-in securitymeasures to protect personal information against both unauthorized access and disclosure from within;

5) Employers should be denied access to personally-identifiable health records on its employees or prospective employees;

6) Individuals must have the right to see, copy and correct all information contained in their records. Individuals should be given notice of how personal information will be used and by whom;

7) Both a private right of action and a government enforcement mechanism should be established. Also, a federal oversight process should be put in place, to be conducted by a National Health Board or Data Protection Board.

8) It ia imperative that any card, such as the Administration's Health Security Card, only be used for identification purposes and be limited to the health care context. Any other use, such as by law enforcement or employers,should be strictly prohibited.

Finally, we urge this Subcommittee to re-examine the traditional reliance on individual consent as the linchpin of privacy laws. In many circumstances, particularly where the government is involved, consent is coerced and meaningless. Where consent is a condition of receiving benefits, people are forced to choose between providing information or receiving necessary benefits. In the health care context, we urge that impenetrable "firewalls" be erected to prevent disclosure in certain coercive situations, such as employment.

CONCLUSION

The ACLU believes that the protection of personal health information, must be central to all health care reform proposals. Even in the absence of health care reform, we believe that a comprehensive, enforceable federal law is necessary to create privacy protection for personal health information.

There is no more pressing privacy issue than the protection of peoples' health care records. With health care reform one of the top political priorities, we have an opportunity, and responsibility to make privacy an integral component of any new plan. No plan should be put into place unless the privacy and security of personal health information is safeguarded. We have come a great distance in achieving a broad consensus on the key principles. The more difficult task ahead will be to reach agreement on the details. We look forward to working with you on that process.

Senator LEAHY. Neither of you would disagree with the statement that the release of the Congresswoman's health records was totally unethical. I mean, whoever did that violated just about every medical ethics rule there is.

Ms. ROBERTS. It is absolutely unjustifiable and, in fact, you mentioned it was a compelling story to be brought to Congress. I think it is a compelling story to be brought to health care professionals, people who work in hospitals.

I do not know of any hospital that will allow the conscious release of medical records without approval of the patient, him or herself. But we are all aware that there are examples of how that happens unofficially, and we have to work very hard to prevent that from happening.

In many ways, I think the electronic system can almost aid us in that I think we can build in better protection.

Senator LEAHY. Audit trails, identifying of who went into the records at what time and so on would be helpful.

I was also struck with what Ms. Goldman said about the health security card being used as a national ID card. I have to tell you, I do worry about that. I had a situation where I was driving back

from Vermont after the August recess. My wife and I were driving across Lake Champlain, coming down the New York Northway, probably about 60 miles south of the Canadian border, and there was a road block by the Border Patrol.

I said why are we stopping? The guy said the authority is right there, pointing to his badge. I said that is not the question, why? He said can you prove you are an American citizen. I looked at him and I said no. He said what proof do you have of your citizenship? I said none.

So we sort of sat there for a while and I am not sure what would have happened, but he went around and checked the license plate. It is number one from Vermont. I explained it was number one because we are a small state and do not have many cars.

But I am a law-abiding person. I was the chief law enforcement officer in my county for 8½ years. I still bridle at the idea in this country of having to prove who I am, or prove I am a citizen. I mean, we take our rights and our ability to travel and our constitutional right to travel, so strongly.

I do want a good health care system for all of us. We cannot have tens of millions of Americans without easy access to health care and without the ability to pay for it. I do see some of the enormous advantages both in cost containment and in better health, to be able to have the smart cards or other health data cards to carry records.

We are a mobile society. It is no longer the case that you grow up in the same town where the local doctor knows you and everything else. You do travel about. With the changes in medical practice, if they know that you had a particular disease in your teens, that may affect you in your thirties, or forties, or whatever else. And that is fine. But I do not want it to be available to anybody who knows how to tap into a data system.

Would you agree with me that it is important to get the security system worked out quickly, not after the fact?

Ms. ROBERTS. I had said that in my testimony. I think that is critical and I would agree that we do not need to wait for health care reform to have that in place. I think, on the issue of the card, what is on that card and whether it actually has all the information on the card or is an access card for certain appropriate people to be able to access the very critical information that is important for your health, still needs to be developed. And we need to be able to have access to the information, the system, the health care system needs to be able to take care of us.

But having the information that is available to all, I would point out that Vermont is one of the few states that does not use the Social Security Number for the driver's license, but I would also point out that since we do not have pictures on them, it is hard to prove that you really are who you say you are.

Senator LEAHY. One time I actually had to show an ID card with my picture and the only thing I had in my pocket was my Senate ID card. You are right, the Vermont driver's license does not have it. They said do you have anything with a picture, so I showed them my Senate ID and they said well, it does not have a number. I said there are only 100 of us. They said well, which one are you? So that was fine. I was trying to rent a car in California and they

had a Congressional discount and they looked down and said we have it for the Congress but not for the Senate, so that was the end of that.

You are trying to be serious Carolyn, and I apologize.

Ms. ROBERTS. It is not easy.

I am here on behalf of the American Hospital Association, but it is hard to get away from Vermont as well. As you well know, we have been very active in the area of health care reform in the state of Vermont. I would point out, as a potential model, is the Vermont Health Information Consortium which is working in tandem with health care reform on the development of the appropriate health care information system. It has a very active subcommittee that is working very intently on the issue of patient confidentiality and confidentiality of information.

Ms. GOLDMAN. Senator, if I may just make a comment on the security issue that you raise, what we call for—in our testimony we have a list of recommendations for legislation—while we call for strong security measures, whether they are audit trails, encryption as information is sent across the information highway, strong penalties, those security measures are never going to be 100 percent. You will always have a situation where someone can figure out how to hack into the system, where someone on the inside either sells information or—as in the case of the Congresswoman—gives out the information for some other political purpose.

So we are taking a risk in putting together an electronic data network. It is a risk. I am not saying we should not take it, but we have to at least recognize that no system is going to be 100 percent foolproof, even if we take all the right steps.

Senator LEAHY. Sure. The fact is the system is there so that people can go into it. You are in the hospital or you are in for medical treatment and the person who is treating you is going to want to get as much information as possible, in order to give you the best treatment, and second not to make mistakes. So somebody can access the information.

And somebody can breach that if they are unethical. There is no way you can totally stop that. But I think that we can devise a system where you can limit greatly who has access and then do as many safeguards as possible, by putting in indicators of who accessed the information, so that you make it much easier to identify who went in, so that if something is released—even though that has happened after the fact—you can go back into the system to find out how it occurred.

You do not have the situation we have with the Congresswoman: they are still having to investigate and are having a difficult time finding out who might have done it. Those steps can be taken. I think we all agree on that.

Ms. Roberts mentioned Vermont. We do have the Vermont Health Information Consortium looking at security and identity issues. You said from your association that the national legislation should be able to preempt the state guidelines. What if those state guidelines are more protective of security?

Ms. ROBERTS. I think we have to have a standard. I think the Federal law should preempt state laws, both from the ceiling and

from the floor. I think we have to have a standard set of guidelines which are all accountable to, through a Federal law.

Senator LEAHY. Your association proposed to HHS privacy legislation. Do you think that that was stronger than what so far has come out of the administration?

Ms. ROBERTS. Yes.

Ms. GOLDMAN. On preemption issues, I think while we would support preemption under certain circumstances, those circumstances would probably be if the Federal legislation was really tough, if it was enforceable and it was strong. We do not want to be setting such a low floor, I think you would agree with me.

Ms. ROBERTS. Absolutely, that's exactly it.

Ms. GOLDMAN. We need to make sure the legislation is strong.

Ms. ROBERTS. I think we are saying the same thing. Our concern is both for strong legislation but also so that it goes across state lines to ensure the portability of the coverage, as well as——

Senator LEAHY. And don't you have to be careful, also, to make sure that the individual's right to take action against anybody who has so invaded their privacy is not limited? I mean, we do not want to set up an immunization of people from invasion of privacy. I want to be able to sue the pants off of somebody who invades my privacy. I want to really go after them.

Ms. ROBERTS. Being surrounded by lawyers, I understand.

The thing I want to stress, we have an opportunity to improve efficiencies in the system. We also have an opportunity to improve care of people and in doing that we have to maintain the balance of improving the care with their right to confidentiality of their own information.

But as we set up these networks of care, which are part of the President's bill and part of the American Hospital Association's vision, we are going across providers. It is not the hospital record, the home health record, et cetera. It is across the full episode of care, and that is a whole new challenge for us.

I think if we start thinking in terms of how do we protect confidentiality today, as we are moved forward into this new system, we have a greater chance of really being able to protect that.

Senator LEAHY. I would assume that the health security card is going to have to have certain basic information to identify the person, and also certain information for billing. Again, whether you are in Vermont or you are in Texas, and you have a health problem or whatever else, we can understand all of that.

Should the health security administration, or whatever it may be called, design just one card or should we have something available if consumers want to have more information on their cards? Suppose I have some chronic condition and I want to carry around a great deal more information on the card than whatever is set up as the basic. Should I have that ability to do that or that right to do that, even if it means I've got to pay something extra to put it on the card?

Ms. ROBERTS. It would seem to me, as a non-lawyer person, that people should have the right to decide whether they want to have information that pertains particularly to them or not. If you have an allergy and you are concerned about your health in another area

if that allergy is not recognized, you should have the right to put that information on.

If you are willing to be accountable for not having that information on your card, then you should be able to assume that responsibility for yourself.

It seems to me—and I am not a technical data person—but it seems to me that card can serve as an access and that information as to who you want to have access could be included on that card. The details of it, I guess we can work out. The principles of it is what we need to establish and all be committed to.

Ms. GOLDMAN. I think first, Mr. Chairman, we really need to question the need for a card. We need to really discuss whether we actually need a card in order to make health care reform work, because I think there are dangers inherent in having a card.

Senator LEAHY. You think primarily the national identification card is a danger?

Ms. GOLDMAN. Absolutely. I mean, the story that you tell, while it is a humorous story, it might not have turned out so humorously for somebody else.

Senator LEAHY. And I admit, it is a little bit different because I sit there and think if push comes to shove, my wife is going to quiet me down enough to say just tell them who you are, Pat, and let's get out of here.

Ms. GOLDMAN. But if there were a card that people knew everyone who was eligible for health care in this country had this card, whether they carried it with them or they had it at home, I think you would find people asking for it as proof of citizenship, as proof of eligibility for benefits. So I think it is a real concern.

And I am not saying we absolutely should not have them, but there has not really been a very good discussion in this country about it. The President has held up his card on TV and people keep carrying their prototypes of the card around as though it is a done deal, and I think it is worth having a pretty serious discussion about the dangers.

Senator LEAHY. Let me ask this question to both of you. If there is a card with an identification number, what are the pros and cons of using the Social Security Number for the identification number? Ms. Roberts, do you want to go first? Ms. Goldman?

Ms. ROBERTS. Speaking for the American Hospital Association, it is not a policy decision that we have had a chance to deliberate on or come to a statement on. I can tell you, though that we are all very concerned about a single number that carries as much power as a Social Security Number does. I do not know how that discussion would end up, but I have a sense that the Social Security Number being used as a number would not fare well.

Senator LEAHY. Ms. Goldman.

Ms. GOLDMAN. The Social Security Number should absolutely not be used as an identifier if there is a card. This issue is extremely controversial and that is why the administration did punt this again to the health board. It is extremely controversial and for really kind of conflicting reasons.

One, the Social Security Number is a de facto national identifier. It is on more than half of the driver's licenses in this country. It is a number that is most commonly requested when you get admit-

ted to a school, even at the elementary school level. When you open up an account at a bank, when you do almost any kind of a transaction, when you go to the doctor, when you get a credit card, they want your Social Security Number. So it is very commonly used.

But the conflicting reason of why we should not use it is that it is not a reliable identifier. There is nothing which allows you to verify that the Social Security Number is tied to that individual. The Social Security Administration does not issue the number tied, in any way, to an identification system. So they do not necessarily verify identity when the number is issued.

The Social Security Administration testified a number of years ago, when the work authorization card was being debated in the House, that this is not a reliable identifier and they do not want to see it become a national identifier. They know that there are a very high number of fraudulent numbers out there, duplicate numbers, that the number is misused. People forget and they give the wrong number.

So we would really be building what we need as a very secure system on a very shaky system and I think we should start fresh. I do not think the costs to do that are particularly high. There have not been any numbers on it, but we would just start fresh and use something that is secure, something we can encrypt, that has a pass code.

Senator LEAHY. Would you agree that as far as security is concerned, it does not make any difference whether the medical record is on paper or in a computer-bank? Even though the record can be moved instantaneously, electronically from place to place, the need for security and privacy remains exactly the same, is that correct?

Ms. GOLDMAN. I think that the issue is the same, in terms of our ultimate result. We want to protect both the paper records and the electronic records. It is one of, I think, the flaws in the WEDI legislative recommendation, is that it only would protect electronic records. It does not protect the paper records.

So in the case of Congresswoman Velazquez, she would not be covered under the WEDI recommendation, because it turns out there was probably a paper record that was then faxed. So I think we need to protect the information, regardless of the form that it is in, but there are things that are possible when information is computerized, when information is electronic, that is not possible when it is kept in paper form. There is just an added risk, an increased risk.

Senator LEAHY. I think that with electronic records, of course, there are different problems. I think that the privacy issues remain the same, no matter how it is done, whether it is a handwritten note in a record or whether it is electronic.

We had an earlier hearing and Jeffrey Rothgater, who wrote the book "Privacy For Sale," testified. He talked about a freelance artist who could not get health coverage. He kept going from place to place and could not get health coverage.

He found out that a hospital he had been in had been one that was selling information to companies for marketing services or other purposes. Somebody had put somewhere in his records erroneously that he had AIDS. This got into a data bank and it went out to a number of insurance companies and he kept getting turned

down for insurance. He found out why: the mistake was traced all the way back to his records.

It was not just the fact that the mistake was made, but of course the question obviously comes up, why in heaven's name was that being disseminated anyway.

I just mention that it is so much easier to send all this information around if it is electronic. I think that we ought to be able to check into this.

And also, of course, you have the problem of what happens if a computer hacker gets in. We joke about the bright young college student who did not show up for exams but gets into the school data base and all of a sudden he or she is on the dean's list. That is kind of funny, I suppose. But what if somebody goes into a medical data bank and puts in that everybody has tuberculosis, or everybody has AIDS, or whatever else it might be, or says that they have been cured? There are problems either way. I think these are things that we have to guard against.

Ms. ROBERTS. Your statement is absolutely correct. The issue of confidentiality should be paramount regardless of what the system is, whether it is paper or electronic. We are in an electronic age now, and that is not going to go away. The work of your Subcommittee is to be applauded and I would certainly look at any way that I could to help you continue in your work.

I do not think we want to go back in our opportunity to move forward in improving health care for the people in our society, but the issues that you raise are with us in all area of data that flows in our society and we need to be looking at ways that we can protect that information for all of us, in all areas of our life.

Clearly, health care is a very personal issue that has people very concerned. Knowing that the information is only going to help them and not harm them will be, I think, paramount to get good legislation passed.

Senator LEAHY. I do not expect to come up with all the answers here today, any more than we did in the earlier hearing that I had on this issue, and we will have more. I would like to be able to call on both of you as we go on about how we should work this out.

Again, I think most Americans have this sense of privacy. We have spent 200 years refining our sense of privacy in this country. We all know how easily it can be violated, with the ability to keep data on people.

We will keep the record open here until February 14 for any further testimony that comes in. I have longer statements which will be included in the record, too.

Let's just keep working together on it. I do not want us to wait until after we have a health system to start fully addressing the security part. I think it has to be done together. Frankly I think most people feel as we do in my own state, that unless you can guarantee their privacy, they are not going to be too eager to have the system. So they are going to have to be done together.

I thank you both for taking the time to be here today.

[Whereupon, at 12:11 p.m., the subcommittee was adjourned.]

APPENDIX

ADDITIONAL SUBMISSION FOR THE RECORD

STATEMENT OF THE AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

Mr. Chairman and Members of the Subcommittee: The American Health Information Management Association (AHIMA) appreciates the opportunity to submit written testimony to the Subcommittee to present our views on privacy and confidentiality and the need for federal legislation.

The American Health Information Management Association represents 35,000 credentialed professionals who are responsible for managing the health care information which has become an increasingly important component of our nation's health care delivery system.

On a daily basis, health information management professionals ensure that an individual's right to privacy is protected. Our members must handle requests for health information from third party payors, employers, researchers, attorneys, other health care providers, local, state and federal agencies. Health information management professionals ensure that information is disclosed pursuant to valid authorizations from the patient or their legal representative or pursuant to statute, regulation or court order. This responsibility is not taken lightly and is complicated by lack of uniform national guidelines or legislation.

The recently released Office of Technology (OTA) report, *Protecting Privacy in Computerized Medical Information,*found that current laws do not, in general, provide consistent, comprehensive protection of health information confidentiality. Focusing on the impact of computer technology, the report concluded that computerization reduces some concerns about privacy of health information while increasing others. The report highlights the need for enactment of a comprehensive federal privacy law.

The public's concern about the confidentiality of health information was identified in a poll conducted by Louis Harris and Associates for Equifax, Inc. The results of the *Health Information Privacy Survey 1993* were released at a conference sponsored by AHIMA and Equifax in conjunction with the U.S. Office of Consumer Affairs on October 26, 1993. There was strong support for comprehensive federal legislation to protect the privacy of medical records.

Currently, there is little uniformity among state licensure laws and regulations regarding confidentiality of health information. It has been recognized that there is a need for more uniformity among the 50 states. In recent years, the National Conference of Commissioners on Uniform State Laws developed the Uniform Health Care Information Act in an attempt to stimulate uniformity among states on health care information management issues. Presently, only two states, Montana and Washington, have enacted this model legislation. Clearly, efforts must be directed toward developing national standards on privacy and confidentiality.

The development of the national information infrastructure is a key component of the President's health care reform plan. The increasing need for data highlights the need for federal preemptive legislation to protect the confidentiality of health information.

During the past two years, AHIMA has taken a leadership role in addressing privacy and confidentiality. In July 1992, Arthur Ashe was a keynote speaker at AHIMA's first annual confidentiality symposium. Mr. Ashe spoke eloquently of his

decision to disclose his medical condition and his concerns regarding invasion of privacy. During that conference, both Mr. Ashe and other speakers highlighted the need for federal legislation to ensure that individuals have access to their health information and to protect the confidentiality of their medical records.

In order to address the need for federal legislation, the American Health Information Management Association (AHIMA) drafted model language in February and March of 1993 with input from AHIMA members, members of the Computer-Based Patient Record Institute Workgroup on Confidentiality, Privacy and Legislation and individuals from other professional associations.

This model language was presented to members of The White House Task Force on Healthcare Reform on April 29, 1993. Copies of the model language have also been shared with staff to this Subcommittee. The model language was also included in the OTA report.

There are a number of key provisions in AHIMA's model language which we believe are essential elements of any legislation to govern the collection, use and disclosure of health care records. These include:

- Disclosure—No person other than the patient or the patient's representative may disclose health care information to any other person without the patient's authorization, except as authorized in this act.

No person may disclose health care information under a patient's authorization, except in accordance with the terms of such authorization.

The provisions of this section apply both to disclosures of health care information and to redisclosures of health care information by a person to whom health care information is disclosed.

- Record of Disclosure—Each person maintaining health care information shall maintain a record of all external disclosures of health care information made by such person concerning each patient, and such record shall become part of the health care information concerning each patient. The record of each disclosure shall include the name, address and institutional affiliation, if any, of the person to whom the health care information is disclosed, the date and purpose of the disclosure and, to the extent practicable, a description of the information disclosed.
- Patient's Authorization; Requirements for Validity—To be valid, a patient's authorization must——

1) Identify the patient;
2) Generally describe the health care information to be disclosed;
3) Identify the person to whom the health care information is to be disclosed;
4) Describe the purpose of this disclosure;
5) Limit the length of time the patient's authorization will remain valid;
6) Be given by one of the following means——

a) In writing, dated and signed by the patient or the patient's representative; or
b) In electronic forms dated and authenticated by the patient or the patient's representative using a unique identifier.

The AHIMA model also includes the following principles of fair information practices:

- Patient's right to know—The patient or the patient's representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purpose the health care information is used.
- Restrictions on collection—Health care information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected.
- Collection and use only for lawful purpose—Health care information must be collected and used only for a necessary and lawful purpose.
- Notification to patient—Each person maintaining health care information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy of the statement of a person's fair information practices and should receive an explanation of such fair information practices upon request.
- Restriction on use for other purposes—Health care information may not be used for any purpose beyond the purpose for which the health care information is collected, except as otherwise provided in this [ACT].

- Right to access—The patient or the patient's representative may have access to health care information concerning the patient, has the right to have a copy of such health care information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such health care information of any amendment or correction of such health care information requested by the patient or patient representative.
- Required safeguards—Any person maintaining, using or disseminating health care information ahall implement reasonable safeguards for the security of the health care information and its storage, processing and transmission, whether in electronic or other form.
- Additional protections—Methods to ensure the accuracy, reliability, relevance, completeness and timeliness of the health care information should be instituted. If advisable, additional safeguards for highly sensitive health are information should be provided.

The AHIMA model language also contains provisions for civil and criminal penalties to protect against unauthorized use or disclosure.

CONCLUSION

Health care information is personal and sensitive information, that if improperly used or released, may do significant harm to a patient's interests in privacy and in health care, and may affect a patient's ability to obtain employment, education, insurance, credit, and other necessities. Persons maintaining health care information need clear and certain rules for the disclosure of health care information. The movement of patients and their health care information across state lines, access to and exchange of health care information from automated data banks and networks, and the emergence of multi-state providers and payors creates a compelling need for federal law governing the use and disclosure of health care information.

AHIMA believes that it is critical for legislation to be enacted in the coming year. AHIMA applauds the Subcommittee for their concern regarding this issue and looks forward to working with the Subcommittee.

STATEMENT OF ANNA FORBES, M.S.S.

Thank you for giving me the opportunity to address this Committee. I am a social worker by training and an AIDS policy analyst by profession. I have been working in the field of HIV/AIDS since 1985 and am a civil libertarian by conviction. For all these reasons, I have become intensely concerned with the issues of confidentiality and accuracy in HIV reporting systems. This concerns has led me and my colleague, Walter Cuirle, to engage in an extensive investigation of unique identifier systems as tools for the safe and thorough collection of HIV-related information.

Walter Cuirle is a physicist by training and a computer software designer by profession. He and I have been working on this issue since 1991. Although we have focused on this from an HIV/AIDS perspective, our findings are applicable to any situation in which unique identifiers are being used for data collection. The central issues in any case are accuracy, non-duplication, reproducibility and confidentiality protection.

Attached here are two documents written by Walter Cuirle; a "Glossary of Unique Identifier Terms" and "How To Design and Test A Unique Identifier System." Other policy makers have found these useful and we hope they can serve as tools to facilitate this Committee's deliberations.

Two principles are essential to consider in selecting the best possible unique identifier system for public health data. They are:

1) High quality data collection and privacy are not antithetical goals. They have been unnecessarily placed in opposition to each other in public debate. These goals are achievable in tandem and the implementation of a system that accomplishes both should be the standard to which we hold ourselves.

2) A list is never created is a list that does not need to be protected. Figuring out how to eliminate the need for name bearing records is more productive than developing mechanisms to safeguard the confidentiality of such records.

This is not to suggest that data should not be collected. Accurate, comprehensive, client-based information about health care service delivery is unquestionably needed because it directly informs the planning, funding and monitoring of those services. Such data also play a key role in our epidemiological understanding of disease progressions and health care needs.

But we must think of data collection as a function completely separate from the maintenance of records that identify individuals. The two need not and, in fact, should not be linked. Creating a system in which there is absolutely no need or occasion for them to be linked should be the goal.

Once that is achieved, the issue of privacy violation becomes moot because the records that need privacy protection are not linked in any way to data bases maintained by the federal government. This is what we mean when we say that a list that is never created is a list that does not need to be protected. Application of this principle is far more effective in terms of protecting individual privacy than any elaborate series of confidentiality protection steps can ever be.

If I were you, I would say at this point that all this is a nice idea but totally unrealistic. Fortunately, it's not. Walter Cuirle and I have co-authored two unique identification systems that adhere to these two principles. The first one, called the Client Key System, was field tested with federal funding from HRSA in ten AIDS service provider sites across Pennsylvania in 1993.

The second system, called DoubleLock, is an improvement of Client Key in some ways, since we were able to incorporate the lessons we learned during the Client Key field test into its development. We are seeking funding with which to field test DoubleLock.

I mention these here only because they serve as examples of the systems that explicitly incorporate non-duplication and reproducibility, two characteristics that are essential to making a system in which storage of identifying information is neither necessary nor desirable. I'm sure there must be other unique identifier systems that also fully incorporate these characteristics.

As indicated in the Glossary attached here, duplication can be defined as the extent to which input elements belonging to different individuals will generate the same identifier code. Duplication is usually stated as a percentage or rate.

Name-based reporting, which is the first preference of epidemiologists, has been referred to by the CDC as the "Gold Standard" for elimination of duplicates. The CDC has not yet determined, however, the exact level of duplication that occurs in name based reporting. That duplication is (to expand the analogy) the alloy in the gold standard. It can actually be refined out to some extent by the inclusion of a private data element. There may be two John J. Smith's, for example, and they may even have the same birth date. But it is highly improbable that they also have the same hand size.

In any event, name based reporting is certainly not free of duplication. All of us can think of instances in which two individuals have, or are shown in public records as having, the same name.

Only a few systems, such as those based on fingerprints or DNA typing, are free of duplication in a practical sense. In general, the lower the duplication rate is in the raw data elements fed into the computer, the less duplication will occur among the unique identifiers that come out of the computer. But the duplication rate is never zero.

Understanding how duplication occurs is essential to the selection of a unique identifier system with minimal duplication rate. Soundex, a popular phoneme encoding scheme designed for quite other purposes, has been used by several states for generation of health-related unique identifiers. It has a duplication rate of 10 percent-20 percent. This has already been assessed by HRSA as being unacceptably high. An efficient unique identifier system is one that generates or verifies the unique identifier code by processing data elements that:

1) are as specific to the individual as possible
2) demonstrably belong to that individual (so as to minimize fraud or duplication of records as a result of "passing around" ID) and
3) that do not vary over time. For example, use of address as an input data element is inadvisable. So is hair color.

Another characteristic of a good unique identifier system is reproducibility; the ability to regenerate the same unique identifier from the same set of input elements every time.

This appears to be a trivial factor until one looks at it in action. Let's consider reproducibility in light of the following scenario. It is now 1997 and I am going to my local clinic. I have just enrolled in the government's new Health Insurance program. A unique identifier number was assigned to me when I enrolled and the clinic, of course, needs that number in order to bill for my services. But how does the clinic know what that number is?

One possibility is that I could produce a Health Access Card of the type President Clinton held up when he unveiled his administration's health care reform plan on television last year. But what assurance is there that the Card I produce really be-

longs to me? What if I borrowed it from my sister? What if I bought the Card on the black market because I am an illegal immigrant and don't qualify to get my own Card?

Another possibility is that the number assigned to me could simply be regenerated on the spot. I could be asked, for example, to produce some standard form of ID from which public record data elements (such as certain letters from my name and my birth date) could be selected. Then I could be asked to provide a specific private data element, such as a standardized measure of hand size, that is unique to me.

Using these data elements, the clinic staff could make one phone call, punch the data elements into a touch tone phone, and receive my unique identifier number on the spot from a computer that re-encrypts my data elements on command.

The computer could also indicate whether this unique identifier number matches one already assigned to a national Health Insurance participant. If it does, then I will have demonstrated two things:

1) that I am who I say I am (since my private data element, hand size, cannot have been stolen or borrowed for presentation by someone claiming to be me) and

2) that I am enrolled in the federal Health Insurance plan and qualified to receive services under it.

That, in a nutshell, is the DoubleLock unique identifier system that Walter Cuirle and I have developed. We believe it provides a safe, reliable method of generating unique identifiers because it incorporates non-duplication and reproducibility. The data elements used to generate my unique identifier meet the criteria outlined above for minimizing duplication. And the ease with which the unique identifier can be regenerated on the spot minimizes fraud and automatically protects against confidentiality violation.

Since my number can be regenerated by any service provider, there is no need for me to carry a Health Insurance ID card. Since I do not carry a card, my ID number cannot be stolen or misused by someone trying to obtain confidential information about me without my permission.

A unique identifier working group convened by the Maryland Department of Health and Mental Hygiene estimated that a code, to be used efficiently, should take no longer than 90 seconds to generate. We calculate that the DoubleLock code can be generated in less than 60 seconds.

Let me use DoubleLock as an example of how a system can address the two principles I cited.

I. ONE CAN ENGAGE IN FULL DATA COLLECTION WITHOUT COMPROMISING PRIVACY

Under DoubleLock, an individual's unique identifier number can be generated by any service provider at any time. All you need is a touch tone phone. Although computer encryption is involved, the provider does not need to have either a computer on hand or any computer experience.

This means that all providers, from the largest metropolitan hospital to the most impoverished, rural public health nurse, are equally capable using the system to report the services they provide.

Privacy is protected by the inclusion of a private record data element in the mix of input elements. Systems that rely solely on public record data elements are susceptible to confidentiality violation through cross matching. Precedent already exists for systematic confidentiality violation through computer facilitated cross matching of data bases.

This is how it's done. Here I am again in 1997, having just enrolled in the national Health Insurance program. This time let's imagine that I'm a health care worker and that my employer, a multi-hospital corporation, decides to find out which of its employees are HIV positive. Since the corporation can't legally require employees to be tested for HIV, it decides to go through a back door for this information.

It manages, somehow, to get access to a list of national Health Insurance identifier codes for people who have had extremely low CD4 blood test results. Perhaps it obtains these through a local laboratory with which it happens to have a large contract.

Since CD4 blood test results below 200 almost invariably indicate active HIV disease, the corporation can answer its question by determining whether any of its employees have ID code numbers on this list. To do this, it takes the required data elements from its personnel files. Then it feeds these data elements through the unique identifier software, which it has on hand because it develops ID codes for patients all the time. The computer generates pseudo-identifiers for all employees,

which the corporation then cross matches against the list of real identifiers obtained from the lab. Wherever a match occurs, the corporation has identified an employee who almost certainly has active HIV disease.

The threat of confidentiality violation through cross matching cannot be completely eliminated unless one of the data elements is not a matter of public record. Think of what a difference it would have made, in terms of this scenario, if one of the data elements needed to produce my unique identifier number were a private data element, something that is never a matter of public record. This could be something as simple as hand size, foot size or a private word I select, myself. My private data element will never be recorded in my employee records, my Social Security file or on my drivers license. It simply will not be available without my consent and participation. This eliminates the danger of confidentiality violation through cross matching.

Once that risk is eliminated, data can be stored, transported and compiled with impunity. This is why we contend that a confidential unique identifier system (one that includes a private data element) can actually facilitate data collection. Since names are not used and names cannot be accessed through cross matching, there is no need for restrictions on who can obtain data, how it is stored or how frequently it is transferred from one public entity to another. Privacy is already assured.

Now I'd like to use elaborate just a little on the second fundamental principle we have identified, which is:

II. A LIST THAT IS NOT CREATED IS A LIST THAT DOES NOT HAVE TO BE PROTECTED

Let's go back one more time to my 1997 persona. Suppose I did come into my local clinic proudly carrying my new federal Health Insurance identification card. You, as the clinic staff, are faced with the task of determining whether my Card really belongs to me. One way you could do this is by getting out a master list of all the unique identifier numbers assigned to Card holders.

Then you'd ask me to produce a second form of identification for confirmation and you'd compare the name on my second ID to the name and number on my Card and the number as it appears on the master list.

The problem with this solution, of course, is that it requires maintenance of a master list. Who's going to be in charge of protecting the master list? And how will they do it?

As you know, state legislation gets introduced all the time proposing to attach penalties or restrictions to particular behaviors. Suppose my state passes a bill saying that everyone with a history of alcohol abuse will be issued a bright red drivers license, so that police can tell at a glance if someone they pick up has ever had a drinking problem. Now suppose that I was treated for alcoholism two years ago. I don't drink at all now but, once they pick up the master list and cross match it against alcoholism treatment records, the Department of Motor Vehicles will know that I did drink before and they will issue me a red license.

If the state has a master list that connects unique identifier numbers with names, then it has information that it can be forced to turn it over as new legislative mandates are passed. If the state only has unique identifiers, however, and no master list, then it has nothing of use to those wishing to violate individual confidentiality.

Use of master lists at any level automatically raises the question of "Quis custodiet ipsos custodes" or "who guards the guardians". This is a question that, as politicians know, has endless ramifications and is almost never answered to the satisfaction of the public. Why engage it unnecessarily? If full, accurate, verifiable data collection can be achieved without master lists, why have master lists?

I would like to conclude on a note that should be pleasing to Vice President Gore and his colleagues. The creation of a national confidential unique identifier system of the type I have described would require very little by way of new record keeping systems. In other words, no new paper.

A service delivery tracking system will have to be created for a national Health Insurance system, anyway. But, beyond that, the only thing the system we've described would require is maintenance of a data base of all approved, enrolled unique identifier numbers. That data base would be maintained electronically through the existing telephone networks and accessed electronically by service providers.

The public record data elements needed for this system can be obtained from uniform types of identification already in common use such as driver's license, voter registration card, citizenship papers, passport, etc. No new paper, no new networks.

Thank you again for the opportunity to present these ideas to you today. Regardless of the outcome of these hearings, I hope you will bear the principles I have outlined in mind. All too often, public health and civil liberties are portrayed as nec-

essarily oppositional interests. Walter and I have tried to show that this need not be the case with regard to confidential unique identifiers.

Senator Dole, in his Minority Response to the State of the Union message last Tuesday night, indicated great concern about the privacy of citizens' health care records. We applaud his concern and agree that careful consideration should be given to the question of how our health care records are to be transported on the Information Superhighway. It is not unreasonable to want the confidentiality of those records to be fully protected.

Neither is it unreasonable for health policy analysts to want data that completely and accurately describe what health care services are consumed in the country, how, with what frequency and under what circumstances.

Confidential unique identifiers are the key to meeting both of these needs. They allow us to improve upon the old "Gold Standard" of name reporting and move to a system that is simultaneously more efficient and more protective. By advancing our definition of what is needed, we also redefine what is achievable.

Thank you.

THE GLOSSARY OF 'UNIQUE ID' TERMS BY W. CUIRLE

(An earlier version of this document was prepared for the AIDS Institute of the New York State Department of Health 11/08/93)

Algorithm—A set of rules or a formula. For example, the algorithm for representing x as a percentage of y is: "Divide x by y then multiply by 100."

Checksum—An encoding algorithm that creates an identifier by performing some summing function on the input elements Checksums were invented as a technique to determine whether two blocks of text are the same. Imagine a simple system in which there are only capital letters and they are assigned values A=1, B=2 and so on. Punctuation is ignored and the checksum is computed by simply adding up the values of the letters. In this system, the checksum for "APPLE" is 40 and for "APPLES" is 59. Most checksum methods are far more sophisticated than this, but all have the same basic purpose and all are inherently non-reversible. HRSA's algorithm for the proposed URN is a checksum method. See 'Reversibility.'

Client Key—Name for an encryption system that creates unique identifiers. Client Key was created by Alainn Design and field tested by HRSA in Pennsylvania in 1992/93 as an alternative to the URN in per-unit service tracking. It is a reversible encryption assignment method that uses a client-selected word, phrase or number as an encryption key. The key can be of any arbitrary length up to 26 characters. Keys are verified through either existence or reversal. It relies on there being some incentive for the client to use the same key at every encounter.

Confidential Unique ID—See 'Public Element,' 'Private Element' and 'Reversibility.'

DoubleLock—Name for an encryption system that creates unique identifiers. DoubleLock was created by Alainn Design to answer the CDC's perceived need for the reporting of HIC and CD4 test results by laboratories and the real need for client confidentiality. It is a reversible encryption method using as an encryption key some a stable body measurement, such as a ratio of hand measurements. It has the necessary advantage in this application of being verifiable by demonstration and reversibility and it is independent of incentives to the client. The cost of this benefit is that the range of the encryption key is much less than in Client Key.

Duplication—The extent to which input elements belonging to different individuals will generate the same identifier. Also, a measure of the occurrence of many-to-one correspondence in a system that is supposed to be one-to-one. Duplication is usually stated as a percentage or rate. No system is theoretically free of duplication. Only a few systems, as those based on fingerprints or DNA typing, are free of duplication in a practical sense. The minimum duplication rate of a system is a function of the input elements and the selection rules for both list and encryption assignment systems. If an encoding assignment system uses a non-reversible algorithm, it increases the minimum duplication rate. Minimum duplication rate is never zero.

Encode—Any process that transforms a set of inputs (a message) into some other form. All encryption techniques are also encoding techniques. Not all encoding techniques are also encryption techniques. The distinction is that encryption techniques are inherently reversible and therefore do not lose any input information.

Encrypt/Decrypt—To hide or conceal/to reverse the process Properly speaking, a message is said to be encrypted if and only if the process can be fully reversed to obtain the original message. Messages that are merely transformed in some way but cannot be reversed are encoded. In the context of identifiers, "encrypt" and "encode" have, unfortunately, been used interchangeably.

Encryption key—The knowledge necessary to decrypt a message A key could be as simple as knowledge of the encryption algorithm (see 'Transposition') or it could be knowledge of a particular input element (see 'Private Element').

Reversibility has nothing to do with security; it has everything to do with uniqueness.

Encoding/Encryption assignment—An ID generation method in which assignments are made without direct reference to a master list. Instead, a set of selection rules is applied to the set of input elements with the presumption that the result (the input string) is as unique to the individual as the input elements. The input string is passed through an algorithm that generates the final ID. (If the algorithm is reversible, the method may be called 'encryption assignment.') Encoding assignment methods that use only public input elements are ultimately no more secure than the algorithm that generates them. Given the algorithm, any comparable list of public elements can be used to regenerate the IDs and this list can be compared against the list of real IDs to identify the individuals by name.

Identifier—A string, typically of fixed length, made up of letters, numbers or a combination of them. Identifiers are generated by list or encryption assignment. When there is a one-to-one correspondence between individuals and their identifiers, the identifier is unique.

Input element or data element—A characteristic that helps to identify an individual. For example: name, address, gender, birthdate and so on. An identification code, regardless of the method of generation, can be no more unique than the sum of its input elements.

Lifetime of an element—The average time over which an input element retains the same verifiable value. With the exception of just a few possible input elements like fingerprints or DNA type, all input elements have a finite lifetime. This is entirely a function of population and behavior. Take, for example, an urban population between the ages of 18 and 30. Within that population there will be a certain non-zero number of changes in every public element: name, gender, address, even birthdate may change as a matter of public record. Of the elements used to create an ID, the shortest lifetime of any element determines the lifetime of the ID. A differently defined population will have a different set of lifetimes for the component elements. Absent any incentive (in the sense of direct personal benefit, not punishment) to report these changes AND a method to track them, all identifier systems will erode over time.

List assignment—A generation method in which identifiers are assigned by direct reference to some master list. Each entry in the master list is a set of public data elements. Assignment is typically serial: to generate a new ID, the set of elements for the individual is compared against the master list and the new set determined to be or forced to be unique; then, the next number in the ID sequence is assigned. Prisoner or military IDs backed by fingerprints are one such system that works well; social security is similar but more vulnerable to fraud; telephone numbers are a one-to-many list assignment. List assignment methods are very efficient in that they maximize the use of selection space. On the other hand, the necessary existence of the master list makes them impossible to keep confidential.

Many-to-one correspondence—Several different sets of elements correspond to the same identifier. This is a useful property in identifying groups; for example, several family members at one address or several patients at one clinic. In the context of uniquely identifying an individual, it represents a design flaw. Non-reversible encryption assignment methods all have an inherent risk of many-to-one correspondence—the trick is in measuring that risk. Many-to-one cannot be unique.

One-to-one correspondence—One set of input elements corresponds to one and only one identifier. An encryption assignment method that is reversible is provably one-to-one and therefore as unique as its inputs. List assignment methoda may or may not be, depending on intent. For example, by design telephone numbers are unique but not one-to-one; social security is supposed to be both unique and one-to-one. One-to-one is always unique, but unique is not always one-to-one; however, in the context of identifiers for individuals, unique and one-to-one are synonymous.

One-to-many correspondence—One set of input elements corresponds to several different identifiers. Whether or not this is a good thing depends on intent and method. It is a good thing for telephone numbers, a problem with social security numbers. One-to-many may also be unique, as with telephone numbers.

Private or non-public element—an input element that is not collected into a public list. This could be almost anything: ratio of hand width to hand length; model of television in the living room; name of first pet. To be practical, an ID system that uses private elements must use verifiable private elements.

Public element—An input element that is already collected as part of some public list. For example: name, address and birthdate are all together as elements in all

drivers' licenses, so all three are public elements. If all of the input elements that comprise a unique identifier system are part of any one public list, the ID system cannot ever be confidential since individuals can always be identified by cross matching to the public list. This is true regardless of generation method.

Range or variability—The number of mutually exclusive values a particular input element can have. For example: gender has a range of 2; birth month plus birth day has a range of 365. A design goal is to use elements with a broad range or high variability (see 'Selection Space'). (Note that both these terms have quite different meanings in other contexts.)

Reproducibility—The extent to which a set of elements from a particular individual will generate the same ID every time. On the face of it, this is a trivial issue; it would seem that a particular individual will always have the same set of input elements. As a practical matter though, this is not the case. People change their names and addresses or they may have perfectly valid forms of public ID with different names; for example, 'Bill' and 'William' or 'Betty' and 'Elizabeth.' Failure to reproduce an ID from verifiable inputs is sometimes called "the Betty/Elizabeth Problem." See also 'Lifetime.'

Reversibility—The ability to regenerate input elements correctly from the identifier. An encryption assignment method (one that uses a reversible algorithm) is provably one-to-one and therefore has an incremental duplication rate of zero due to the algorithm. A list assignment method is reversible if and only if the master assignment list is available. An arbitrary encoding technique may not be reversible at all. Reversibility has nothing to do with confidentiality.

Selection rules—techniques used to reduce the length of input elements while minimizing the effect on uniqueness. Input elements frequently have a much larger selection space than their range. Selection rules attempt to maximize the ratio of a variable's range to its selection space without a significant loss of range or increase in duplication. The degree to which a given set of selection rules succeeds in this goal can only be determined empirically. For example, HRSA's proposed URN uses the selection rules: "1st and 3rd letter of last name plus 1st and 3rd letter of first name." Client key uses "first four letters of last name plus first letter of first name." There is no analytical means to judge between them.

Selection space—The total number of possible values that could be represented in the number of characters allocated for a particular element within an ID. This depends on the length and structure of the ID string. For example, one hundred things can be represented with two digits. A social security number is always nine digits, so it has a selection space of one billion values. If capital letters were allowed as well, the same nine character string would have a selection space of ten thousand billion. Pure list assignment methods have a range equal to the selection space and are therefore compact and efficient. Encoding assignment methods will always have a variability less than the selection space. A design goal is to minimize this difference.

Soundex—Name for a common phoneme-encoding algorithm that generates a code equivalent to English phonetic spelling Soundex was invented to allow someone to search a list of names using an uncertain spelling as an input. It generates the same four-character code for all names that sound alike, regardless of spelling. Its strength lies in its ability to generate many-to-one codes. For example the Soundex code is "C640" for all of these: "Curley," Curly," Curle," "Curlae" and "Cuirle." It is a very useful addition to any name-lookup or spell-check application and has long been used by the US Census for that purpose.

Transposition—A simple encryption system based on the substitution of one letter for another according to a fixed set of rules. This is perhaps the simplest form of encryption, but it illustrates all the properties of a reversible algorithm as a basis for an encryption generator. Rules can be as simple as "Substitute B for A, C for B * * * A for Z." Toys like the Captain Midnight Decoder Ring are common examples.

Unique identifier—A characteristic of an identification system designed for one-to-one correspondence. The identifiers created by a system can be no more unique than the input elements used to create them. No practical set of input elements is 100 percent unique and the generation process invariably introduces more duplication. A unique identifier is a goal, not a reality. (See 'Duplication,' 'Lifetime,' 'Reproducibility,' 'One-to-one Correspondence').

Uniqueness—See 'One-to-one Correspondence,' 'Reversibility'

URN—Unique Record Number. A unique identification system proposed by HRSA, a part of DHHS, as a component of its Universal Reporting System (URS). URS is a client level reporting system designed to support Ryan White funding. In the URS, clients are identified by the URN rather than by name. The URN is a non-reversible encoding assignment technique using a form of checksum algorithm.

It was field tested throughout the country in 1992/93. The final report is in preparation.

Variability—See 'Range'

Verification—The act of confirming that an ID or elements of an ID in fact belong to the individual that claims them. Input elements and IDs can be verified by demonstration, existence, or reversal. Demonstration means that the person presents some standard form of public ID, such as a driver's license. Verification by existence means that the ID is generated from the presented elements and then checked against a list of IDs. Verification by reversal means that the person supplies the encryption key needed to reverse the ID and the composite public elements. If the decryption process generates the same public elements, the key is verified. (See 'Client Key' and 'DoubleLock')

HOW TO DESIGN AND TEST AN IDENTIFIER SYSTEM BY WALTER F. CUIRLE

(An earlier version of this document was prepared for the AIDS Institute of the New York State Department of Health 11/08/93)

Some of the debate over unique identifiers centers on the security of various algorithms, as if that were the only important aspect. The simple fact is that any system using only public input elements can be circumvented without any knowledge of the algorithm at all.

Other aspects concentrate on the cost of implementation, asserting high or low figures depending on the agenda but in both cases without much substantiation.

Some have called plain text name reporting the 'gold standard' of reporting, denying the error and duplication in all public records and implying that no identifier system could perform as well. In fact, appropriately designed private element systems can improve on the reliability of public records and refine that uncertain standard.

The fact is that the entire debate is taking place in a quantitative vacuum. No one has measured the base alloy in the so-called gold standard. No one has measured the performance of an ID system against such an assayed standard. No one has stated performance standards and substantiated them in any meaningful way. Everyone is stretching and polishing analogies, trading assertions instead of test results and debating with credentials and titles instead of fact.

Thia test suite can help fill that vacuum. It is simple, straight-forward, relatively quick and provides a numeric basis for comparison of any unique ID generation system. It is not perfect, but it is a start. As Lord Kelvin once pointed out, "If you cannot say a thing in numbers, your knowledge is of a meager and unsatisfactory kind."

1. *Define the system's performance*

Transcription—Will you want to transcribe IDs to paper? If so, look to systems that minimize transcription errors. Capital letters only or numbers only are best, but generate longer IDs than a combination of the two. Systems that include arbitrary punctuation or lower case letters lead to transcription errors.

Length—Will you want people to be able to remember IDs? Old telephone company tests demonstrated that the maximum length most people can remember easily is between five and seven characters in groupings of three and four. (That's why telephone numbers are seven digits long and were initially a mnemonic plus five digits.)

Longitudinal tracking—Do you want to track individuals over time? Over location? How long a period of time and how wide a geographic area? If the answer is no to both, almost any verifiable system will do. To the extent that the answer is yes, you must determine the lifetime and geographic scope of both the IDs and its component elements.

Lifetime of identifier—Decide on a lifetime for your identifier. Be practical—in the absence of any positive incentive that will induce people to report changes, you cannot have an inexpensive ID system that remains 100 percent reproducible for all time for every person of any age in all geographic areas. Represent lifetimes by dividing the target population into age groups: for example, 0–5 years, 6–15 years, 16–22 and so on. This is a rough cut. Base your decisions on your deaire for stability over a entire range, your estimates for possible changes in verifiable input sources across ranges and your guess at the utility of having the range identified within the population. Actual measurements of stability are taken later and the ranges can be refined.

Selection of input elements—The average lifetime of the input elements must be greater than or equal to the selected lifetime of the identifier and each element must be verifiable and reproducible. There are not too many choices—last name, first name, middle name, gender and birthdate are about it for public verifiable ele-

ments. Address is a possible element if you have a short ID lifetime or don't care about longitudinal tracking.

Consider the variability of the element as well; for example, gender is only two-valued and is unlikely to have much practical effect if first and last names are used as well.

Reproducibility and Verification—Reproducibility: How will you determine the correct way to make the input entry so that the same element is entered the same way every time? Do you include suffixes such as "Jr" or "III" with the last name? What is the first name in "H. Ross Perot," H or Ross? Make up some fixed set of rules, but don't try to cover every exceptional case.

Verification: How will you determine whether the input elements belong to this individual? While it may be reasonable to rely on some kind of picture ID for persons over 18 who are likely to have driver's licenses or some similar ID, how will you verify pediatric cases? What is the preferred form of verification?

You need a definite answer to these questions for each input element in each age range selected.

One overlooked question is this: In the case of hyphenated last names, which is the "last" name? In Anglo usage, choice of the first of the two might provide continuity of ID for women through marriage but it may not appear on all forms of ID. The hyphenated usage is also beginning to appear in some records for Anglo children. In some Hispanic and Russian usages, hyphenated last names have long represented paternal and maternal lines that can be interchanged or dropped depending on circumstance.

Selection rules—Decide on a set of selection rules. These may be and probably are dictated by the algorithm you intend to use. In those cases where an algorithm accepts the entire length of a name, be sure that you are thorough in your 'reproducibility' decisions.

2. *Measure raw input reproducibility*

This requires access to a large database of public records. You will repeat the test for each selected age range. Suppose that we want to measure reproducibility within the age range 0 through 5.

Use a set of closed public records. Select a sample of, say, 50,000 from birth records of, say, 1985. Follow the public record of these individuals through 1990, tracking changes in input elements. Suppose that by 1990, 500 members of this cohort have had their names changed through adoption or other means. Five have had the public record of their birthdates changed to reflect the correction of some clerical error. (If the information is available, adjust the numbers for migration out of the area and death. For the sake of argument, suppose that 2,000 in this age range leave the jurisdiction.)

500/48,000	1.04 percent changed names as recorded
5/48,000	0.01 percent changed birthdates
100 percent	1.05 percent = 98.95 percent Maximum rate of reproducibility

Adjust the sum as necessary for other input elements and all possible changes. For example, if address is one of your input elements and there are 5,000 changes of address within the cohort *and within the jurisdiction*, then

200/48,000	1.04 percentchanged names as recorded
5/48,000	0.01 percentchanged birthdates
5000/48000	10.42 percentchanged address
100 percent	11.47 percent = 88.53 percent Maximum rate of reproducibility

3. *Measure raw input uniqueness*

This requires access to a large public database in which records contain more elements than those that will be used as input elements. The extra elements will be used to identify duplicates.

Select a sample limited to the age range under consideration for some single instant in time. A sample taken from current records will do.

Sort or index the sample based on all the input elements plus any other existing element that will serve to distinguish among duplicates. If, for example, you are using birth records for this month then the mother's name might be sufficient to break a tie. Check that the resulting sample is a unique list when the tie-breaker is included.

Within the sorted sample, count the number of unique occurrences of the sums of the full-length of the selected input elements. Be careful. If, for example, the

input elements are last name and first name and a record reads "Franklin W. Smith Jr." then the sum of the input elements is "SmithFranklin" since middle initial and suffix are not designated input elements.

The rate of duplication is ratio of the second count to the first. Suppose, for example, that you select 50,000 current birth records and demonstrate based on internal evidence that 49,900 of these are unique as you define that for this purpose. (The 100 might be incomplete or could be indistinguishable based on available data.) When you count unique occurrences of designated input element sums in this list of 49,900, suppose that you find 49,500. Then:

(49,900–49,500)/49,900	0.80 percent raw rate of duplication or
100 percent—0.80 percent	99.2 percent raw rate of uniqueness

4. *Compute the maximum reliability*

Reliability can be expressed in words this way: Select an individual at the beginning of the age range specified and record the input elements. At some time later, equal to the age interval specified, record the input elements for the same individual. What is the probability that the input elements are the same both times AND are unique to this individual?

Mathematically, this is just the combined probabilities (the product) of the reproducibility and the uniqueness or Reliability, reproducibility, uniqueness. Using the examples above,

Reliability without addresses	98.95 percent	99.2 percent	98.16 percent
Reliability with addresses	88.53 percent	99.2 percent	87.82 percent

Error rate is just 100 percent minus reliability, another measure of the same thing:

Error rate without addresses	100 percent—98.16	1.84 percent
Error rate with addresses	100 percent—87.82	12.2 percent

NOTE: THESE RELIABILITY FIGURES ARE ENTIRELY THE RESULT OF POPULATION BEHAVIOR, THE QUALITY OF PUBLIC RECORDS AND THE SELECTION OF INPUT ELEMENTS. THEY ARE UTTERLY INDEPENDENT OF SELECTION RULES AND ENCODING OR ENCRYPTION ALGORITHMS. YOU MUST COMPUTE THE MAXIMUM RELIABILITY FIRST—IT IS THE BASE LINE AGAINST WHICH ALL CANDIDATE ID SYSTEMS ARE COMPARED.

5. *Compute the effect of the private element(s)*

If the system under test DOES use a private element or key, repeat item 2 above using the private key as an additional input element. A private element will have the net effect of decreasing duplication and increasing uniqueness. If the element is fixed, it will have no net effect on reproducibility. If it is not fixed, it will tend to decrease reproducibility.

To find the effect of a key on duplication and uniqueness, recompute the rate of duplication and maximum uniqueness with the key taken into consideration as just an additional field. The incremental effect of the private input element is the difference between the uniqueness computed there, without the key, and the uniqueness computed here, with it.

Suppose that, as in item 2, we start with 49,900 unique records and find a count of 49,500 unique combinations of input elements without the key and 49,800 unique combinations with the key.

Even if all of the keys were identical, the number of unique combinations with the key cannot be less than the number without the key. In other words, duplication is reduced or left the same and consequently uniqueness is increased or left the same.

(49,800–49,500)/49,900	0.60 percent	Correction in duplication rate due to key.

Corrections due to the key will always REDUCE the net duplication rate or INCREASE the net uniqueness.

If the key or private element is variable, do a similar recomputation of reproducibility. A variable key will tend to DECREASE reproducibility.

6. *Compute the effect of selection rules*

If the system under test does NOT use a private key, start with the second list created in item 2 above, the list which has only full length input elements but in which every record is known unique. (The count in that example was 49,500.) If the

system DOES use a private key, start with the list created in item 4 above, the list which has both full length input elements and keys and in which every record is known unique. (The count in that example was 49,800.

Apply the selection rules as stated for the system under test to every record in this test list to create still another list. Count the number of unique occurrences of each record, taken as a whole, in this new list. Suppose, for example, that you start with 49,500 known unique sets of full input elements. After applying the selection rules, suppose that the count of unique strings in the result is 49,300. This means that 200 duplicates were introduced solely because of the selection rules. Then:

200/49,500	4.0 percent	Correction in duplication rate due to selection rules

Corrections due to selection rule will always INCREASE the net duplication rate or DECREASE net uniqueness.

7. *Compute the effect of the encoding or encryption algorithm*

Corrections due to the encoding algorithm used will always INCREASE the net duplication rate or DECREASE net uniqueness.

A reversible encryption algorithm transforms inputs one-to-one so that there is no net loss of information. The correction due to such an algorithm is zero.

The effect of a non-reversible encoding algorithm may be zero, but this can only be determined by testing. Start with the known unique list from item 2 (if there is no key) or item 4 (if there is a key).

Apply the algorithm to the list overall and count the number of unique occurrences in the resulting list of identifiers. The difference between this number and the total number of input records, divided by the total number of input records, is the correction to the net duplication rate.

For example, suppose that the input list is 49,500 unique records. After application of the algorithm, the count of unique IDs is 49,450. The correction to the duplication rate is therefore:

(49,500–49,450)/49,500	0.10 percent	Correction to duplication rate due to algorithm

8. *Compute the overall reliability of the system*

The overall reliability of the system is the product of the corrected reproducibility and the corrected uniqueness.

Raw reproducibility—Correction due to variable key. Corrected reproducibility

Raw uniqueness + Correction due to key—Correction due to selection rules—Correction due to effect of algorithm. Corrected uniqueness

---

AMERICAN HOSPITAL ASSOCIATION,
CAPITOL PLACE,
Washington, DC, April 15, 1994.

Hon. PATRICK J. LEAHY,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY: The American Hospital Association (AHA) is pleased to be able to respond to the additional questions forwarded by your staff in follow up to the 27 January hearing at which Carolyn Roberts, Chair of the Board of the AHA, delivered the Association's testimony.

Let me begin by stating that some of the areas encompassed by the questions are ones that AHA has only recently started to explore, and for which, therefore, we have no formal policy in place. I will try to provide you with the benefit of some of our thinking in those instances where our policy is still fluid. Moreover, I will try to group the questions together when this will provide for better answers.

Your Questions 1–3 concern the development and use of a health security card. The AHA has no formal policy on such a card but would like to share with you some of the issues we see as important. The primary purpose of a health security card is to function as a uniform entry point into the health care system via a database. A question arises here as to whether there should be a single database or a multitude of smaller community databases. At the least, it is important that inquiries, responses and updates to any database be maintained at the community level because that is where health care is delivered.

We believe that uniformity and simplicity are key goals; introducing multiple care styles, to allow for consumer choice, would not further these goals and could require providers to purchase multiple card reading devices, which could become costly and burdensome.

As far as the type of card to be chosen, the magnetic strip card is the most common form in use today, and probably the quickest and most convenient way to permit hospitals and other providers to be routed to the appropriate database. While a smart care can hold an individual's entire medical record through use of a computer chip in the care, the current process for updating the patient's record on to the chip is weak and imprecise.

In addition, a patient's health record is rarely complete at the time of a discharge or when services are rendered. Getting such information on to the card at that time would be impossible; requiring the patient to return simply to update the card would be difficult.

Any unique identifying number (Question 4) issued as part of a health Security card does have the potential to become, in effect, a national identification number. For this reason, it is important that those whose work brings them legitimately in contact with patient information understand their responsibilities as to the confidential nature of such information. Strict database protocols must be established with redundant safety features to prevent unauthorized access and provide an historic log to track organizations and individuals who view or receive patient information.

The need for privacy and confidentiality of medical records applies to both paper and electronic information (Question 5). However, the general public perceives computerized medical records to be more vulnerable because they are travelling along an electronic highway where it is conceivable that a greater number of unauthorized individuals can view or obtain the information. Therefore, the AHA believes incentives are necessary to protect individually identifiable health care information travelling in an EDI (electronic data interchange) environment. Thia does not, however, preclude a uniform confidentiality law protecting all individually identifiable patient information regardless of the medium.

As far as the types of medical records covered by National Health Board standards (Question 8), our reading of the language seems to indicate that all health related information, whether maintained in a hospital or an individual physician's office, would be covered by the standards.

Our written testimony addresses the issues raised by your Questions 9 & 10. We stated that there are only two major components of the Administration's bill that need strengthening in the area of privacy and security of medical information. First, we think there must be a federal preemption clause, which would allow a federal confidentiality law to occupy the field and completely preempt the application of state law to the collection, storage, processing and transmission of individually identifiable health care information. We believe the WEDI model legislation attached to our written statement is a workable model for this effort. Second, we believe that the three-year delay in instituting new and stronger confidentiality protection is far too long.

Questions 11, 12 and 14 all relate to the penalty provisions of the Health Security Act. The AHA believes that criminal penalties should be enforced against an individual who obtains individually identifiable health care information through false pretenses or theft and that civil monetary penalties should be assessed against any person who knowingly discloses confidential health care information. For a more detailed understanding of AHA's policy for inappropriate uses of identifiable health car information, please refer to the WEDI model legislation, Sections 12 and 14, attached to our written statement.

Questions 16 and 17 raise some interesting ideas about the use of advanced technology to maintain an accurate record of who has viewed information and for what purposes. Although this is another area where the AHA has no formal policy, we would like to address some issues. First, of course, is whether these technologies are affordable to the health care system. Second, it might be useful, in the technology envisioned in Q. 17, to know whether there could be an override in certain circumstances. Last, there would have to be a very careful definition of categories for access in Q. 17. For example, would "Physician" include attending physician, consulting physician, or utilization review company physician?

Finally, Question 18 looks at state criteria for confidentiality in health plan certification. We believe there should be one uniform federal law to occupy the field and preempt all state laws on confidentiality.

Thank you for the opportunity to present testimony and answer questions on what we believe in a very important series of issues to be decided in health care reform.

Sincerely,

PATTI ROBERTS GOLDMAN,
Senior Associate Director,
Congressional and Executive Branch Relations.

○