(date)

The Honorable Michael O. Leavitt
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Leavitt:

The American Health Information Community (AHIC) members identified and prioritized several "breakthroughs", health information technology applications and uses that could produce a specific tangible value to healthcare consumers and which could be realized within one year. The AHIC Chronic Care Work Group's breakthroughs are defined by both a broad and a specific charge as follows:

- **Broad Charge for the Workgroup:** Make recommendations to the Community to deploy widely available, *secure technology solutions for remote monitoring and assessment of patients* and for *communication between clinicians* about patients.
- **Specific Charge for the Workgroup:** Make recommendations to the Community so that within one year, widespread use of *secure messaging*, as appropriate, is fostered *as a means of communication between clinicians and patients* about care delivery.

While concentrating on deployment of the specific charge, the Workgroup identified five significant issues which could either preclude or enable successful implementation of both charges. The Workgroup's recommendations presented in this letter to address these five issues:

- Reimbursement
- Medical Liability and Licensure
- Consumer Access and Consumer-Clinician Workflow
- Standards for Embedding Secure Consumer-Clinician Messages into EHRs
- Standards for Patient Identifications, Authentication and Security

Chronic Illness and Consumer-Clinician Secure Messaging

Approximately 50-60 million Americans live stably with at least one chronic condition -- most have more than one. This 20% of the US population interprets care which is safe, effective, efficient, timely, patient-centered, and equitable (the aims of the Institute of Medicine) broadly -- given that most of the care management occurs outside of the professional setting. Patients with stable chronic conditions manage a good part of their care themselves while monitoring diets, controlling weight, checking blood sugars, adjusting blood thinners, titrating asthma medications, etc. This population, above and beyond almost any other, requires frequent and easy communication with their clinicians for guidance and timely decisions so that their chronic condition can be better and more tightly managed in their home, work, and school environments with minimal disruption. Further, as technology continues to find new and better ways to gather and transmit information through monitoring and communication devices, there will be even greater opportunity to meet patients' needs for care wherever and whenever they require the time and expertise of their physician or clinician. (See Appendix 1 -- populations and opportunities.)

Technology alone, however, will not lead to better care and outcomes. How it is adopted and used are critical components of success, as are the financial and social policies which either incent or disincent the adoption and use. The following recommendations which address technical, financial, and social policies are specific to secure messaging between patients and their physicians and clinicians. They are, however, applicable to all types of telehealth communications.

Secure Messaging Definition and Common Functionalities
Secure patient-clinician messaging refers to communications between patients and clinicians who have an explicit measure of responsibility for their patient's care. In addition to online consultation, secure messaging between patients and their clinicians may be used for:

- Requesting Prescription Refills
- Scheduling Appointments
- Requesting Referrals
- Receiving Routine Test Results
- Receiving Reminders & Instructions

Secure messaging may occur through a secure unique portal, may be part of a shared electronic health record system, may be accessed through a delivery system's architecture or may be part of encrypted attachments to traditional email. Independent of the vehicle, secure messaging is characterized by clear guidelines for use, published by the AMA and AMIA, and a clear methodology for assessing value developed by the IOM and the American Telehealth Association.

Adoption by the practicing clinical community has, however, been limited. The following recommendations address the major barriers.

Key Recommendations

Reimbursement

While up to 80% of chronic care management takes place out side of the practitioner's office, he/she is only reimbursed for time and expertise if the patient makes the effort to make and keep an appointment for an office visit. Explanations on how to best manage the changing patterns of atrial fibrillation, advice on how to modulate insulin in a brittle diabetic, monitoring of blood pressure and titrating its medications all require office visits in order for clinicians to be compensated, much of this information and guidance could be provided through direct communication. Lack of reimbursement for clinician time and expertise rendered outside of the office setting is the major barrier to widespread adoption of the use of secure messaging between clinicians and their patients.

In situations where lack of compensation is not a barrier (salaried clinicians or fee for service reimbursement) both a positive return on investment (ROI) and improved quality of care have been noted by the entity holding responsibility for the costs of care. (See Appendix 2.)

- *HHS should develop the evidence base for informed reimbursement policies with respect to secure messaging between clinicians and their patients.*

- *HHS should be charged to develop a description of reimbursement methods suitable for secure messaging. These methods would need to address the heterogeneity of practice setting from traditional fee for service to the variety of capitated systems (IPA and integrated staff models) as well as newer, innovative proposal like the American College of Physicians Advanced Medical Home. (Timeline - six months) To develop these descriptions, HHS should utilize the experience of existing secure messaging systems to learn different reimbursement strategies and to identify current best practices regarding existing specific and auditable guidelines for reimbursement of secure messaging. (Concurrent - six months)*

- *HHS should identify opportunities to leverage existing programs using secure messaging between clinicians and their patients to:*
  - *reflect the diversity of current physician practices*
  - *reimburse only for internet based physician/patient encounters that qualify under CPT code 074T*
  - *used in accordance with guidelines as developed by the American Medical Informatics Association, the American Medical Association and the Massachusetts Health Data Consortium for secure messaging*
  - *coincide with existing or planned HHS demonstration programs designed to promote health IT adoption, consumer directed healthcare, and/or pay for performance efforts*

- *HHS should monitor and report on ongoing electronic communication experiences in various practices and in pilot studies to determine the effects of online communications on cost, quality, especially for chronic disease outcomes, medical legal concerns and patient and caregiver satisfaction.*

Medical Liability and Licensure

Since the use of communication technologies, such as secure messaging, to exchange medical information between a patient and his/her care provider is a critical/essential component of the healthcare delivery process which can impact the diagnostic and therapeutic decisions for the patient, as well as provide a convenient, cost effective means of accessing that care, any barriers to its use need to be addressed. One such restriction, based on existing state licensing laws, would prohibit a practitioner licensed in one state from giving advice/care/education to his/her patient using a communication modality if that patient resided in another state.

Although the focus of our efforts is to establish both continuity and quality in the Chronic Disease Care process by integrating electronic communications as a vital means of health information transfer, it should not be forgotten that this type of information exchange will be equally critical in the event of a man-made (smallpox) or natural (H5N1) bio-event.

Immediate access to information to effect diagnostic, therapeutic and isolation decisions needs to be made to avoid further spread, but local, state-based expertise may not be available, or if available, too distant to access quickly. In the same manner that biological agents as they spread and infect people are not going to respect state boundaries, we cannot let state licensing laws prohibit our ability to diagnose and treat those individuals who have been exposed. (See Appendix 3.)

- *Given that existing state licensing laws did not anticipate secure messaging as an integral part of the healthcare process, it is recommended that the Secretary of HHS working with such stakeholder groups as the National Governors' Association, the Federation of State Medical Boards, and the National Council of State Boards of Nursing, explore new licensing alternatives to address the ability to provide electronic care delivery across state boundaries while still ensuring compatibility with individual state requirements in terms of licensing fees, CME, etc. Some alternatives could include licensure by reciprocity, similar to what exists between states in Australia, or utilizing a model comparable to a driver's license in which if you have a valid license from one state you are permitted to drive in any other state. Key stakeholders to include in discussions might include the American Medical Association, the American Nurses Association, and the American Bar Association.*

Consumer-Clinician Workflow

As we consider enhancing the consumer-clinician experience via communication beyond face to face interactions in traditional care settings (e.g., physician offices, clinics, hospitals and assisted living homes), we begin by addressing the question of consumer value. Key areas of value include time savings, improved access, and an “unquantifiable” piece of mind that patient users get from the system. Indeed, there is a “sense of social interaction” that secure messaging provides patients, especially elderly patients. The value proposition for clinicians for secure messaging with their patients includes office efficiency, clinical productivity, revenue potential, patient satisfaction, and interoperability with other IT systems.[1] [2]

The value of secure messaging to both consumers and physicians, however, depends on the ability of this communication media to successfully transmit concepts. Sometimes this will be facilitated by online templates. Other times, free text will be more appropriate depending on the complexities of the medical situation being addressed and the comfort of the consumer with using the various online choices inherent in free versus structured text in the message. In general,

[1] Colella, Relay Health, AHIC Chronic Care Testimony, March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

[2] Sands, M.D. Beth Israel Deaconess Medical Center and Harvard Medical School, Zix Corporation, AHIC Chronic Care Testimony, March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

technology connections without consideration to improved processes would only accelerate bad processes and hence fail to reinvent dialog between physician/care giver and patient/consumer.

Additionally, "one can't separate workflow issues from reimbursement issues, for the nature in which physicians are reimbursed drives how they perform. In particular, if you do not get to a secure-messaging use rate among patients of at least 20 to 30 percent, it creates additional workflow… It is really the power users who find secure messaging beneficial, because they actually change the way their office work flows to accommodate and use the new technology… Physicians who effectively use secure messaging find that their work with patients who come into the office become more focused, because they are handling many of the less significant issues via secure messaging."[3] (See Appendix 4.)

- *Enable clarity around intangible value to consumer and value in consumer-physician work-flow*
  - *AHRQ should investigate the impact of secure messaging on improved workflow by identifying successful patient care models that leverage secure messaging*
  - *AHRQ should quantify and qualify intangible ROI, e.g., peace-of-mind, for patients within these usage models*

Standards for Embedding Secure Consumer-Clinician Messages into EHRs

Secure technology solutions for communication about chronic care delivery between clinicians, and between clinicians and patients, and for remote monitoring and assessment of patients, must be based on standard transactions before they can be widely deployed as a means of chronic care improvement. The solution will only be effective if the clinical data can be appropriately shared between parties with legitimate needs for the data. Web portals currently offer feasible solutions for secure messaging among clinicians and patients, however, their effectiveness is limited by a lack of standardization and interoperability. Certification of secure message transactions and portals by a recognized certification body has the potential to encourage more widespread utilization. (See Appendix 5.)

- *The Office of the National Coordinator for Health Information Technology (ONC) needs to ask the Health Information Technology Standards Panel (HITSP) to prioritize harmonization of standards relevant to secure messaging that could be used by the Certification Commission for Health Information Technology (CCHIT) in certification criteria for systems supporting secure messaging.*

- *ONC needs to ask CCHIT to establish certification criteria for patient-physician secure messaging.*

[3] AHIC Chronic Care Workgroup Discussion, February 23, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

Cross Cutting AHIC Workgroup Recommendations

Consumer Access & The Healthcare Digital Divide

The benefits of HIT, particularly transactional functions, are of recognized value to consumers. However, several studies have documented evidence of a digital divide (see Appendix 6). In addition, there are a number of barriers, including financial, technical, personal preferences, access and ability to use and understand the technology that must be overcome if all are to benefit from secure messaging in health care. It is necessary to reconfirm the barriers and identify strategies to address those barriers, as well as determine whether secure messaging is a viable technology for all population groups.

- *AHRQ should conduct a synthesis of current knowledge from existing studies of computer use by elderly and underserved populations including an analysis of barriers and drivers. The barrier and driver analysis should elucidate for which subpopulations, barriers can be overcome and how they can be overcome.*

Patient Identification and Authentication

(Note that this area cuts across all workgroups and will be considered in an integrated fashion among workgroups)

Accurate, verifiable, unique patient identification and authentication is a foundational requirement both for supporting secure messages between patients and clinicians as well as incorporating the documents created into electronic health records, both those maintained by healthcare organizations as well as personal health records which may be maintained by patients. Methodology for identifying and authenticating patients must be constructed in such a way as to promote patient trust in the process, transparency in the use of information provided, and adequate patient control over who may or may not access this information. Ideally, patient identifying components and the method for cross-matching these components between systems should be standardized to facilitate matching patient identification across multiple systems, as long as patients have a full understanding of the potential risks and benefits of this capability and voluntarily chose to allow this level of interoperability. (See Appendix 7.)

- *HHS, HITSP and the private sector should set as their top priority the ability to match patient identification across multiple systems. This is the single most important first step for nationwide interoperability. The standard should be ubiquitous across all healthcare environments such as long term care, ambulatory, acute, chronic or generated from an individual. Additionally, the standard should be ubiquitous across all healthcare sectors such as payer, provider, individual.*

- *HHS, HITSP and the private sector should set as their second priority the requirement of initial in-person authentication as the requirement for e-authentication and the use of a secure messaging portal for actual exchange of information between patients and providers. The e-authentication industry is advanced and is an existing technology widely used in industry that healthcare can leverage. Because of the sensitivity of* *health information, authentication should be in-person. This recommendation is not focused on the technology of e-authentication; instead it is focused on the minimum requirement to obtaining e-authentication (i.e. digital certificate etc). Authentication is the first step to enabling a patient, or their proxy, access to their health information electronically and having a high level of assurance that the sender of health information is in fact the authoritative source for the information. A secure portal rather than common e-mail facilitates the identification/authentication process, provides a more acceptable level of security, and creates opportunities for structured data entry not routinely available in common e-mail systems.*

Sincerely yours,

(signature)	(signature)
Craig Barrett, Ph.D. Co-Chair, Chronic Care AHIC Workgroup	Mark McClellan, M.D., Ph.D. Co-Chair, Chronic Care AHIC Workgroup

Appendices

Appendices

Appendix 1: Targeting Opportunity for the U.S. Healthcare Consumer & U.S. Healthcare Costs

1.01 Background

As the Chronic Care Workgroup makes recommendations regarding what aspects of secure messaging should be implemented within one year, a number of considerations must be addressed. These are outlined below as recommendation areas for the specific charge, with each recommendation area containing brief background and rationale for the recommendation followed by the recommendation itself (including appropriate detail to clarify the specifics of the recommendation).

It's useful to segment the health consumer according to how they experience their health challenges and the costs those challenges represent. For example from among the US population as whole, we see the chronically ill segment in numbers and costs fit in as follows:[4]

Population	Number	$/person/yr	Total $ billion/yr
1. Healthy	~170 million	~$700	~$120
2. Moms and babies	~6 million babies, moms	~$10,000	~$60
3. Acutely ill	~60 million	~$10,000	~$600
4. Chronic	~50 million	~$7000	~$350
5. Serious disability	~7 million	~$35,000	~$250
6. EOL, Short decline	~½ million	~$40,000	~$20
7. Erratic & sudden death	~1 million	~$45,000	~$50
8. Long dwindling	~5 million	~$50,000	~$250
TOTALS -	300 million		$1.7 trillion

[4] Lynn, Rand Corporation & CMS, AHIC Chronic Care Testimony , March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

To drill down into the chronically ill segment, 17 million Americans have been diagnosed with Asthma, 16 million with diabetes, 13.5 million with coronary obstructive pulmonary disease (COPD), 13 million with coronary artery disease (CAD) and 4.9 million with congestive heart failure (CHF). Against this background of large human costs and an ever increasing financial burden on our nation, the most tragic point is that much of this suffering and cost is preventable. For example, a recent Rand Report found that on average patients receive recommended care only 54.9% of the time.[5] To put this in concrete terms, consider that sixty percent of non-traumatic amputations occur in diabetics (82,000 in 2002).[6] As one health insurance company put it, approximately 40,000 amputations associated with diabetics could be prevented.[7]

As we look for opportunities to improve the rate at which chronically ill health consumers receive appropriate care, we segment the population along the dimensions defined by the IOM Quality Aims and explore what opportunities for leveraging enhanced communication exist for the chronically ill as follows:[8]

Aim	**Interpretation**	**HIT Opportunities**
Safe	No medication errors; safe devices,	PHR with CDS, EHRs
Effective	Secondary prevention, RX to goals	Reminder systems, EHRs
Efficient	Coordinated DX services, successful RXs, no admin bur	EHRs, patient centric PMS, care communities
Patient Centric	Individual care plans attentive to circumstance, ability to self-manage	PHRs, shared care plan management, monitoring device
Timely	Access to care from remote settings	E-visits, e-prescribing, e-scheduling
Equitable	Respect for cultural differences, geography	Multi-lingual, telecommunications

Secure consumer-clinician messaging is a part of each of the above HIT opportunities. In particular, the key theme is to leverage HIT to mitigate for the chronically ill the onset of acute episodes of heart and lung failure. For once these begin, the patient experiences steady function decline marked by instances of sharp drops and rebounds in function representing

[5] McGlynn EA, Asch SM, Adams J, et al. The quality of health care delivered to adults in the United States. *N Engl J Med*. Jun 26 2003;348(26):2635-2645. http://www.nextlogical.com/pdf/research/Patients_Have_5050_Chance_of_Right_Care_NEJM_062603.pdf

[6] http://www.cdc.gov/diabetes/pubs/pdf/ndfs_2005.pdf

[7] R. Tuckson, Presentation to The Council of State Government's State Officials Summit, Chronic Illness and Disease Management, 2003.

[8] Ibid. Lynn 2006.

hospitalizations which have both a large toll in human suffering as well as a large financial toll as exemplified by the following 2004 hospital costs:[9] [10]

- CAD inpatient charges of $39.6 billion ($25.6 billion of which was Medicare)
- CHF inpatient charges of $19.8 billion ($15.2 billion of which was Medicare)
- COPD inpatient charges of $8.2 billion ($6.2 billion of which was Medicare)
- Diabetes inpatient charges of $7.4 inpatient charges ($3.8 billion of which was Medicare)
- Asthma inpatient charges of $3.3. inpatient charges ($1 billion of which was Medicare)

These are sizable savings targets and remote monitoring has been shown to make an impact on these hospitalization costs. For example, one study [11]of a tele-homecare project in California that focused on a patient population with chronic illnesses showed that the difference in cost for home care between the test group using tele-homecare services and the control group not using the technology was not significant. However, the overall medical costs of the test group were approximately half those of the control group during the study period. The cost savings was attributed to a "dramatic reduction in hospitalization" among members of the test group.[12]

Finally, we must also realize that secure messaging is one component of the remote communication channels available to clinicians and patients as outlined below:[13]

- Secure messaging (as outlined above)
- Incorporating readings for the in home tests such as glucose level, blood pressure, cholesterol and weight in the above asynchronous messaging
- Video conferencing and messaging
- Asynchronous messaging mixed with patient encounters attached to the EHR
- Patient Access to Notes and Reports
- Multimedia Educational Material

Hence, even though we are currently focused on secure messaging in the specific charge, we should remember the context of broader communication channels that lead us on the path to achieving the broad charge.

[9] *Chronic Care Improvement*, ITTA May 2004 (based on estimates from AHRQ 2001 Cost and Utilization Project)

[10] Composite data provided by Disease Management Association of America (based on data from AHA, ADA, ALA, NHLBI, CDC)

[11] Johnston, Wheeler, Deuser and Sousa, ARCH FAM MED, Vol 9, 40, Jan 2000

[12] AHIC Chronic Care Workgroup Discussion, March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

[13] Delbanco and Sands 350, NEJM , vol 17, 1705, April 22, 2004 http://content.nejm.org/cgi/content/full/350/17/1705#T1

Appendix 2: Reimbursement

2.01 Background

Overview on Reimbursement
Electronic mail and internet access are now a well-established part of everyday life. Not surprisingly, surveys now show that the vast majority of US adults would like to communicate with their own physician or other health care provider on line. After a rather slow start compared with industries like banking, investing and shopping, demand for and supply of electronic messaging in health care is rapidly gaining momentum.

The amount of electronic communications between doctors and patients consistently increases. Absent any standardization, electronic communication takes multiple forms: some occurs in carefully planned, secure settings after extensive work to build an infrastructure, policies and procedures to create a true "SYSTEM" of electronic communication which frequently involves incorporation of communication into the medical record. Other communication is occurring in more informal, unstructured, and possibly insecure settings. In more carefully devised and monitored settings as well as based on anecdotal reports, persons requiring ongoing chronic care are most likely to use electronic communications in health care. They probably gain the most in terms of convenience, increased access, possible cost and time saving and the potential to experience improved outcomes. Although some settings do provide reimbursement for electronic communications, there are no accepted guidelines or even less formal established standards of practice, and, in spite of increased supply and demand, overall adoption of electronic communication is still slow, with 70% of physicians citing reimbursement as critical in their decision and ability to adopt online communication with patients.

Private Sector Reimbursement and Adoption of Secure Messaging
In the private sector, multiple providers, payers and Integrated Delivery Networks are currently promoting the use of the above secure messaging functionalities. The ambulatory practices associated with UC Davis are early adopters on the provider side. On the IDN front, Kaiser and Group Health Cooperative are adopters. Group Health deployed secure messaging and a PHR capability before it launched its EHR capability. High Mark Health in Pennsylvania and BCBS of Florida[14] are just two of many payers supporting the first five secure messaging functionalities above. Other blues plans that are participating in secure messaging programs include: **Blue Shield of California, Regence Blue Shield of Idaho**, **Blue Cross Blue Shield of Massachusetts, Blue Cross and Blue Shield of Kansas City, Empire Blue Cross Blue Shield, Blue Cross Blue Shield of Tennessee, Regence Blue Cross and Blue Shield of Utah, Premera Blue Cross (WA) and WellPoint (online consultation programs in NH, CO, IN).** Indeed secure messaging is a relatively low cost investment with demonstrable return that can let a spectrum of providers, from small physician practices to large IDNs, get started with clinical Health IT applications.

[14] http://www.jacksonville.com/tu-online/stories/090104/bus_16521558.shtml

Government Sector Adoption of Secure Messaging

In the government sector, the Veterans Health Administration has deployed through its MyHealtheVet patient portal online prescription refills, online appointment scheduling, online patient reporting and tracking over time of cholesterol and pain as well as patient access to Medlineplus.gov to explore health topics, research diseases and conditions, learn about vet-specific conditions, understand medication and treatment options, assess and improve their wellness and view seasonal health reminders[15]. Online consultation, however, may take a creative approach to reimbursement in staff model IDNs such as the VA (e.g. the RVU credits that UC Davis gives to its staff physicians) if physicians are going to incorporate online consultation into their already busy work flows. As for DoD, they have deployed online appointment scheduling and appointment reminders and have stated that in the future they would like to support online consultations. However, there may very well be security and authentication concerns for DoD health information that goes even beyond the stringencies of HIPAA that may delay adoption of online consultation.

Modes of Financial Incentive

In terms of reimbursement, many models or combinations of models are in play. Models include the following:

- For payers not participating, consumers can message with their physician and pay by credit card a fee for the online consultation
- For payers that do reimburse the physician, consumers can either participate with no charge or may have a copay. However, in some payer supported trials, physicians have chosen to waive the copay altogether. Other payers cap the copay at $10 per encounter even if face to face encounters have copays increase yearly.
- A wild card for payer reimbursed messaging will be those patients in Consumer Directed Spending Accounts. Here, if the patient is in the cost stage where their HSA would take the full brunt of the face to face encounter (e.g. an $80 office visit) the savings associated with only a $20-$30 fee for an online consult is substantial
- For staff physician models such as at the VA, RVUs could be assigned to the various secure message services. (Note that to enhance the timeliness and efficiency of secure messaging, these applications may have the capability to route the communication between the patient and the physician's office to the appropriate non-physician clinician within that office freeing up the physician to focus on the higher RVU activity)
- Indirect reimbursement can occur through capitated disease management models that include the primary care provider in the disease management process
- Pay for performance programs that incorporate secure messaging could also be part of the financial equation for the physician
- Reimbursement based on alternative care models such as the "Advanced Medical Home"[16]

[15] Abstracted from Dr. Kolodner's testimony on June 30, 2005 http://commerce.senate.gov/hearings/testimony.cfm?id=1563&wit_id=4402

[16] Barr, American College of Physicians, AHIC Chronic Care Testimony, March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

Return on Investment

In terms of ROI for payers and providers, early promising results including the following:

- Financial ROI: In an April 2001 to May 2002 study (sponsored by Relay Health) involving 3,688 patients and involving BCBS of California and several high tech self-insured payers in Northern California, secure messaging resulted in total healthcare savings of $3.69 per member per month (pmpm) with costs of 0.31 pmpm. Of the $3.69 pmpm, $1.92 pmpm was related to savings in physician office visits.
- Quality ROI: The Columbia University Informatics for Diabetes Education and Telemedicine (IDEATel) Project is a four-year demonstration project funded by the Centers for Medicare and Medicaid Services with the overall goals of evaluating the feasibility, acceptability, effectiveness, and cost-effectiveness of telemedicine in the management of older patients with diabetes. The authors conducted a randomized, controlled trial comparing telemedicine case management (involving video conferencing with nurses) to usual care, with blinding of those obtaining outcome data, in 1,665 Medicare recipients with diabetes, aged 55 years or greater, and living in federally designated medically underserved areas of New York State. The primary endpoints were HgbA1c, blood pressure, and low-density lipoprotein (LDL) cholesterol levels. Telemedicine case management improved glycemic control, blood pressure levels, and total and LDL cholesterol levels at one year of follow-up

Evaluation

There are key points to evaluating remote monitoring approaches to patient care. However, it is difficult to address telemedicine as a whole, because there is significant variation among services that fall under the heading of telemedicine. Some types of telemedicine are supported by evidence demonstrating their efficiency and cost-savings while others are not. Key points for evaluation include:

- Three factors are typically considered when evaluating remote health service: access, cost, and quality. All three factors interrelate.
- There are four categories of cost that need to be considered with regard to secure messaging: patient cost, provider cost, payer cost, and community cost
- There are three factors for evaluating quality with regard to secure messaging: diagnostic accuracy, timeliness, and appropriateness.
- There are three factors for evaluating access: timeliness, contact with primary provider, contact with specialists.
- Rating the perception of secure messaging is critical in telemedicine. Evaluating perception involves looking at both patient and provider acceptance.
- There are critical questions to answer before beginning an evaluation of secure messaging related to what should be evaluated and how:
  - Evaluate the concept of secure messaging to decide whether the service should be reimbursable or evaluate ongoing secure messaging services to facilitate program improvements?
  - Evaluate secure messaging as a means of triage or as a tool for follow up care?
  - Should secure messaging be compared to traditional forms of delivery or is secure messaging distinct from these forms of delivery?
  - What about tradeoffs? It is dangerous to focus on cost alone because there can be tradeoffs between cost and quality of care.[17]

[17] Linkous, American Telemedicine Association, Chronic Care Testimony, March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

Appendix 3: Medical Liability and Licensure Issues

3.01 Background

Physician Medico-Legal Guidelines
In order to ensure that appropriate interactions take place across the growing spectrum of clinicians that may be engaged in the secure messaging process, a number of guidelines have been recommended by the AMA including the following.[18] (We note that wherever the term "email" is used below, in the context of this recommendation we interpret that to mean "secure messaging" as discussed above). We also note that certain guidelines pertain to actual emails as opposed to alternative forms of secure messaging such as via secure messaging web portals and/or the consumer-clinician communication component of an EHR.

Communication Guidelines:

a. Establish turnaround time for messages. Exercise caution when using e-mail for urgent matters.
b. Inform patient about privacy issues.
c. Patients should know who besides addressee processes messages during addressee's usual business hours and during addressee's vacation or illness.
d. Whenever possible and appropriate, physicians should retain electronic and/or paper copies of e-mails communications with patients.
e. Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) permitted over e-mail.
f. Instruct patients to put the category of transaction in the subject line of the message for filtering: prescription, appointment, medical advice, billing question.
g. Request that patients put their name and patient identification number in the body of the message.
h. Configure automatic reply to acknowledge receipt of messages.
i. Send a new message to inform patient of completion of request.
j. Request that patients use autoreply feature to acknowledge reading clinicians message.
k. Develop archival and retrieval mechanisms.
l. Maintain a mailing list of patients, but do not send group mailings where recipients are visible to each other. Use blind copy feature in software.
m. Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages.
n. Append a standard block of text to the end of e-mail messages to patients, which contains the physician's full name, contact information, and reminders about security and the importance of alternative forms of communication for emergencies.
o. Explain to patients that their messages should be concise.
p. When e-mail messages become too lengthy or the correspondence is prolonged, notify patients to come in to discuss or call them.
q. Remind patients when they do not adhere to the guidelines.
r. For patients who repeatedly do not adhere to the guidelines, it is acceptable to terminate the e-mail relationship.

[18] http://www.ama-assn.org/ama/pub/category/2386.html 2004

Medicolegal and Administrative Guidelines:

Develop a patient-clinician agreement for the informed consent for the use of e-mail. This should be discussed with and signed by the patient and documented in the medical record. Provide patients with a copy of the agreement. Agreement should contain the following:

a. Terms in communication guidelines (as stated above).
b. Provide instructions for when and how to convert to phone calls and office visits.
c. Describe security mechanisms in place.
d. Hold harmless the health care institution for information loss due to technical failures.
e. Waive encryption requirement, if any, at patient's insistence.
f. Describe security mechanisms in place including:
g. Using a password-protected screen saver for all desktop workstations in the office, hospital, and at home.
h. Never forwarding patient-identifiable information to a third party without the patient's express permission.
i. Never using patient's e-mail address in a marketing scheme.
j. Not sharing professional e-mail accounts with family members.
k. Not using unencrypted wireless communications with patient-identifiable information.
l. Double-checking all "To" fields prior to sending messages.
m. Perform at least weekly backups of e-mail onto long-term storage. Define long-term as the term applicable to paper records.

AMA Ethics Policy

a. E-mail correspondence should not be used to establish a patient-physician relationship. Rather, e-mail should supplement other, more personal, encounters.
b. When using e-mail communication, physicians hold the same ethical responsibilities to their patients as they do during other encounters. Whenever communicating medical information, physicians must present the information in a manner that meets professional standards. To this end, specialty societies should provide specific guidance as the appropriateness of offering specialty care or advice through e-mail communication.
c. Physicians should engage in e-mail communication with proper notification of e-mail's inherent limitations. Such notice should include information regarding potential breaches of privacy and confidentiality, difficulties in validating the identity of the parties, and delays in responses. Patients should have the opportunity to accept these limitations prior to the communication of privileged information. Disclaimers alone cannot absolve physicians of the ethical responsibility to protect patients' interests.
d. Proper notification of e-mail's inherent limitations can be communicated during a prior patient encounter or in the initial e-mail communication with a patient. This is similar to checking with a patient about the privacy or security of a particular fax machine prior to faxing sensitive medical information. If a patient initiates e-mail communication, the physician's initial response should include information regarding the limitations of e-mail and ask for the patient's consent to continue the e-mail conversation. Medical advice or information specific to the patient's condition should not be transmitted prior to obtaining the patient's authorization.

Appendix 4: Consumer-Clinician Workflow

4.01 Background

Care must be taken in which mode of secure messaging in employed based on the factors that follow (a comparison of free text versus structured text messages as highlighted in the following table):[19]

	Free Text Secure Messages	***Structured Text Secure Messages***
Comfort	High	Low
Best for	"Soft" issues	"Hard" issues
Problem types	Many/unclear	Single/clear
Encounter billing	May require extra step	May be automated

There are social and practical polices as well, including routing messages to appropriate personnel, informing patients that other staff or providers might read messages, establishing and enforcing message turnaround time, including prior communications thread in message replies, keeping one topic per message, and revoking access of patients who breech policies. Inappropriate uses of secure messaging include medical emergencies, time sensitive issues, communication of bad news, and sensitive issues. Finally, there are the medico-legal polices for secure messaging, including understanding the appropriate vs. inappropriate use of communications technology, using Web messaging or encrypted email when practical, providing e-care only to patients who agree to this form of communication, documenting patient agreements in record, saving messages in patient's record. An expanded discussion of legal issues occurs in the following recommendation as well. [20]

However, realizing the above value is not automatic. In particular, an already "broken" health care system could be further damaged unless behavioral shifts accompanying the advance of secure messaging occurred, allowing for the system to be "healed." Speeding up communication between patients and their providers does not necessarily improve the quality of the

[19] Ibid. Sands 2006
[20] Ibid. Sands 2006

communication.[21] In thinking about behavior changes needed to take place among consumers and providers to establish effective “e-visits” and traditional doctor’s office visits, “both patients and providers need to learn how to use secure messaging effectively, just as many providers have learned to use the telephone in their practices. Learning how to use secure messaging involves identifying situations in which it is useful as well as situations in which another approach would be more effective.”

[21] AHIC Chronic Care Workgroup Discussion, March 22, 2006. http://www.hhs.gov/healthit/ahic/cc_archive.html

Appendix 5: Standards for Secure Messaging Interoperability

5.01 Background

Several organizations currently utilize web portals for secure messaging about care delivery between clinicians and between clinicians and patients. However, these web portals use different standards and are not interoperable. The lack of interoperability limits their potential effectiveness.

To the extent that existing standards for secure messaging conflict, overlap, or are incomplete, the HITSP should harmonize those standards to produce a standards set that can be readily used by CCHIT to develop certification criteria for secure messaging. In the absence of such harmonization, CCHIT would need to conduct such a harmonization effort itself prior to establishing certification criteria, thereby lengthening the process of certification unnecessarily. If appropriately prioritized, HITSP could produce a harmonized standards set for use by CCHIT in time for CCHIT to produce certification criteria within twelve (12) months (see Recommendation below).

CCHIT has developed certification criteria for ambulatory electronic health records (EHRs), and is in the process of developing certification criteria for inpatient EHRs. Once certified, these products will have the "Good Housekeeping Seal of Approval", giving potential purchasers the confidence that they will contain the functionality needed for their intended purpose, including adequate technical safeguards for security. By developing certification criteria for web portals utilizing secure messaging, scheduling, prescription refills, and lab results functionality, CCHIT could provide both patients and clinicians the confidence they need to utilize certified web portals for secure messaging about chronic care delivery.

Appendix 6: Consumer Access & The Healthcare Digital Divide

(Note that this area cuts across all Workgroups and will be considered in an integrated fashion among Workgroups)

6.01 Background

A synthesis of documented evidence should be conducted to address the extent of deficiencies in health care quality that arise from lack of access or personal experience with health information technology for older persons and other vulnerable population groups and to determine whether it is feasible to ensure access to secure messaging for these populations directly or though family/advocates. In particular the synthesis should assess the feasibility of overcoming the digital divide for underserved and older populations, by determining whether secure messaging can be made available and used for their interactions with health care providers and others in their support community. This synthesis should include recommendations on how to educate and train vulnerable populations and their caregivers or family members about the advantages of secure messaging and to make those who lack personal experience aware of how and where to gain access to secure messaging. Areas to address include technology deployment issues and public policy approaches to them and how older populations and other vulnerable groups access and use health care services and decision support. Sample sources for the recommended synthesis include:

- Kaiser Family Foundation, *eHealth and the Elderly, How Seniors use the Internet for Health Information*, Jan. 2005
- Pew Internet and American Life Project
- Center for Applied Special Technology, CAST
- Technology & Innovation in an Emerging Senior/Boomer Marketplace[22]

[22] http://www.technology.gov/reports/2005/OTP_WHCOA.pdf

Appendix 7: Patient Identification and Authentication

(Note that this area cuts across all Workgroups and will be considered in an integrated fashion among Workgroups)

7.01 Background

Electronic communication between patients and providers is increasingly recognized as a needed and appropriate channel for exchange of information. More timely access to provider and support for increased patient participation in the care processes are just two of the aspects which contribute to improved health outcomes. Processes are needed to ensure that such communication occurs in a secure environment and that both patients and providers have confidence in the identity of those with whom they are communicating. Under existing HIPAA regulations, if an individual submits health information to the provider, which the provider then acts upon, the provider is required to store that information in the permanent legal medical record. As the patient becomes a more active participant in the care and management of their chronic condition, and as the ability to share information electronically becomes more of a staple of every day life, it is reasonable to expect that a patient can send to their physician personal health information via secure messaging which can then be stored as part of the permanent electronic health record.

At this time initial in-person authentication should be required as a prerequisite for e-authentication. The reasons include:

- Give the Patient the confidence that it is in fact their care provider with whom they are performing the secure messaging.
- Give providers the confidence that they can use secure messaging safely without the concern that the person at the other end of the secure message is not the patient.
- At this time while health IT is in its infancy, it is prudent to start with the safest step forward and then loosen this requirement as health IT use is better understood and if a lesser requirement is found to be just as effective.