Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information

December 15, 2008

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services

I. Preamble to the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information

PURPOSE

Electronic health information exchange promises an array of potential benefits for individuals and the U.S. health care system through improved clinical care and reduced cost. At the same time, this environment also poses new challenges and opportunities for protecting individually identifiable health information. In health care, accurate and complete information about individuals is critical to providing high quality, coordinated care. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to individually identifiable health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences. A key factor to achieving a high-level of trust among individuals, health care providers, and other health care organizations participating in electronic health information exchange is the development of, and adherence to, a consistent and coordinated approach to privacy and security. Clear, understandable, uniform principles are a first step in developing a consistent and coordinated approach to privacy and security and a key component to building the trust required to realize the potential benefits of electronic health information exchange.

The principles below establish a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the legal framework that may apply to a particular organization. The goal of this effort is to establish a policy framework for electronic health information exchange that can help guide the Nation's adoption of health information technologies and help improve the availability of health information and health care quality. The principles have been designed to establish the roles of individuals and the responsibilities of those who hold and exchange electronic individually identifiable health information through a network.

BACKGROUND

Numerous forces are driving the health care industry towards the use of health information technology, such as the potential for reducing medical errors and health care costs, and increasing individuals' involvement in their own health and health care. To facilitate this advancement and reap its benefits while reducing the risks, it is important to consider individual privacy interests together with the potential benefits to population health.

- Historical Perspective

The Federal government has long recognized the importance of privacy and security protections for the electronic collection, use, and disclosure of individually identifiable information and principles or practices to guide those actions. As early as 1973, the

U.S. Department of Health, Education, and Welfare (HEW) appointed the Advisory Committee on Automated Personal Data Systems to analyze the consequences of using computers to keep records about people. In order to benefit from computerization while providing privacy safeguards, the advisory committee developed the *Code of Fair Information Practice*, which addresses five practices: openness, disclosure, secondary use, correction, and security. These practices have influenced many U.S. laws at both the Federal and state levels and also numerous other national and international documents. For example, in 1974, the Privacy Act was passed, which protects certain personal information held by Federal agencies. In 1980, the Organisation for Economic Cooperation and Development (OECD), an international organization comprised of 24 countries including the U.S., published a consensus document, the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The purpose of the Guidelines was to decrease disparities and assist in harmonizing legislation that would allow the flow of data while preventing violations of what the OECD member countries considered fundamental human rights. In 1998, the Federal Trade Commission published *Privacy Online: a Report to Congress,* which among other conclusions stated that effective self-regulation is the preferred approach to protecting individuals' privacy. Most recently, the U.S. Department of Health and Human Services (HHS) built on these principles in developing the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

In 2004, the Office of the National Coordinator for Health Information Technology (ONC) was created by E.O. 13335, which charged the National Coordinator to the extent permitted by law, to develop, maintain, and direct the implementation of, a strategic plan to guide the nationwide implementation of interoperable health information technology in both the public and private health care sectors and to address in the plan, among other things, "privacy and security issues related to interoperable health information technology and recommend methods to ensure appropriate authorization, authentication, and encryption of data for transmission over the Internet…"

- Legal Environment

Over several decades, states have passed laws to protect the privacy of health information. These laws differ from state to state and often narrowly target a particular population, health condition, data collection effort, or specific types of health care organizations. As a result, states have created a patchwork of privacy protections that are not comprehensive or easily understood. Many states also have begun to consider information security related issues and have passed laws, for example, requiring various types of entities to provide notice of security breaches of individually identifiable information.

At the Federal level, there are also a variety of laws related to the privacy and security of health information, including the HIPAA Privacy and Security Rules, the Privacy Act of 1974, the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation (42 CFR Part 2), the Family Educational Rights & Privacy Act (addresses privacy of information held by certain educational institutions), Gramm-Leach-Bliley Financial

Services Act (addresses privacy of information held by financial institutions), and Federal Information Security Management Act of 2002 (FISMA).

The Privacy and Security Rules promulgated under HIPAA were the first Federal regulations to broadly address the privacy and security of health information. They establish a baseline of national privacy and security standards for individually identifiable health information held by "covered entities" and a foundation of protection regardless of health condition, type of health program, population, state where the activity occurs, or other situational characteristics.

Although the HIPAA Privacy and Security Rules apply to health information in electronic form, the current landscape of electronic health information exchange poses new issues and involves additional organizations that were not contemplated at the time the rules were drafted.

METHODOLOGY

In the development of the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, ONC reviewed various international, national, and public and private sector privacy and security principles that focused on individual information in an electronic environment (but not necessarily on health), including those that focused on individually identifiable health information. This review included:

- *HEW Advisory Committee's Code of Fair Information Practice*[i]
- Markle Foundation's *Connecting Consumers: Common Framework for Networked Personal Health Information*[ii]
- Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[iii]
- *Health Information Technology – Consumer Principles*[iv]
- Federal Trade Commission's *Privacy Online: A Report to Congress – Fair Information Practice Principles*[v]
- The International Security Trust and Privacy Alliance's (ISTPA): *Privacy Framework*[vi]

  It is worth noting that ISTPA conducted a privacy and security principles analysis and harmonization, while accommodating variation from the following instruments, which resulted in the ISTPA principles reviewed by HHS:
  - *The Privacy Act of 1974*
  - OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

- UN Guidelines Concerning Personalized Computer Files
- EU Data Protection Directive 95/46/EC
- Canadian Standards Association Model Code (incorporated in the Personal Information Protection and Electronic Documents Act [PIPEDA])
- *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* Privacy Rules
- US FTC Statement of Fair Information Practice Principles
- US-EU Safe Harbor Privacy Principles
- Australian Privacy Act – National Privacy Principles
- Japan Personal Information Protection Act
- APEC (Asia-Pacific Economic Cooperation) Privacy Framework

There was a great deal of commonality across these principles. After a careful review and analysis of these principles, we harmonized them while accommodating as much variation as possible and being careful to consider how they may apply to electronic health information exchange. We also reviewed the approaches taken by various Federal laws, specifically the HIPAA Privacy and Security Rules, the Privacy Act, and FISMA, as well as recommendations that the Secretary had approved from two advisory committees, the National Committee on Vital and Health Statistics (NCVHS) and the American Health Information Community (AHIC).

PRINCIPLES

The principles outlined in the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information serve as a guide for public and private-sector entities that hold or exchange electronic individually identifiable health information and the development of any compliance and enforcement approaches, including industry self-regulation. Additionally, these principles are designed to complement and work with existing Federal, state, territorial, local, and tribal laws and regulations and should not be construed or interpreted as supplanting or altering any applicable laws or regulations. Various Federal Government agencies are expected to look to these principles as the framework for their policy and technology activities in this area and to encourage states and private sector organizations to do the same.

The implementation of these principles should be dynamic and subject to modification as information practices and technologies advance; however, these principles are designed to be applicable as technology changes.

- **Scope**

These principles are expected to guide the actions of all health care-related persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information. These principles are not intended to apply to individuals with respect to their own individually identifiable health information.

By adopting these principles, persons and entities will follow a common approach to privacy and security and develop appropriate and comparable protections for information, thereby increasing trust in electronic exchange of individually identifiable health information. These principles do not apply to individuals with respect to their own individually identifiable health information. Individuals may use and/or disclose their individual health information as they choose. For example, an individual may share details of a chronic disease on the Internet or in a public meeting but may decide not to share that information with all his or her health care providers or employers. Likewise, an individual should not be expected to implement the administrative responsibilities of these principles such as developing policies and procedures.

- **Organization of the Principles**

The framework is comprised eight principles that are organized as follows:

  - Principles (Level I): Each principle is made up of a short title and a concise statement designed to clearly and simply reflect the concept embodied within each: Individual Access; Correction; Openness and Transparency; Individual Choice; Collection, Use, and Disclosure Limitation; Data Quality and Integrity; Safeguards; and Accountability.

  - Detail (Level II): Each principle is followed by a short explanation that further elaborates on the principle, what it is designed to do, and its parameters.

- **Terminology**

In order to best understand the scope and application of the principles, it is recommended that the reader refer to the glossary (Appendix 1), particularly with respect to the definitions of “individuals” and “persons and entities.”

II. The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information

SCOPE

These principles are expected to guide the actions of all health care-related persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information. These principles are not intended to apply to individuals with respect to their own individually identifiable health information.

INTRODUCTION

Adoption of privacy and security protections is essential to establishing the public trust necessary for effective electronic exchange of individually identifiable health information. A common set of principles that stakeholders accept and support is the first step towards realizing those privacy and security protections and establishing the necessary public trust. The approach of developing principles to guide information practices while advancing technology was marked by the 1973 release of the Code of Fair Information Practice and has been the basis for various activities in the public and private sectors, including the development of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and as the basis for this framework.

The implementation of these principles should evolve in concert with technological advances that allow for greater protections. Adherence should be the responsibility of each health care-related person or entity that holds and exchanges electronic individually identifiable health information through a network, as well as the responsibility of other persons and entities that receive or have access to such information, so that electronic individually identifiable health information is protected at all times.

These principles do not constitute legal advice and do not affect a person's or entity's duty to comply with applicable legal requirements. Where these principles set higher standards than legal requirements, adherence to these principles is encouraged.

INDIVIDUAL ACCESS

Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

Access to information enables individuals to manage their health care and well-being. Individuals should have a reasonable means of access to their individually identifiable health information. Individuals should be able to obtain this information easily, consistent with security needs for authentication of the individual; and such information should be provided promptly so as to be useful for managing their health. Additionally, the persons and entities, that participate in a network for the purpose of electronic

exchange of individually identifiable health information, should provide such information in a readable form and format, including an electronic format, when appropriate. In limited instances, medical or other circumstances may result in the appropriate denial of individual access to their health information.

CORRECTION

Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

Individuals have an important stake in the accuracy and integrity of their individually identifiable health information and an important role to play in ensuring its accuracy and integrity. Electronic exchange of individually identifiable health information may improve care and reduce adverse events. However, any errors or conclusions drawn from erroneous data may be easily communicated or replicated (e.g., as a result of an administrative error as simple as a transposed digit or more complex error arising from medical identity theft). For this reason it is essential for individuals to have practical, efficient, and timely means for disputing the accuracy or integrity of their individually identifiable health information, to have this information corrected, or a dispute documented when their requests are denied, and to have the correction or dispute communicated to others with whom the underlying information has been shared. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should make processes available to empower individuals to exercise a role in managing their individually identifiable health information and should correct information or document disputes in a timely fashion.

OPENNESS AND TRANSPARENCY

There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

Trust in electronic exchange of individually identifiable health information can best be established in an open and transparent environment. Individuals should be able to understand what individually identifiable health information exists about them, how that individually identifiable health information is collected, used, and disclosed and whether and how they can exercise choice over such collections, uses, and disclosures. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format. Notice of policies, procedures, and technology-- including what information will be provided under what circumstances -- should be timely and, wherever possible, made in advanced of the collection, use, and/or disclosure of individually identifiable health

information. Policies and procedures developed consistent with this Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information should be communicated in a manner that is appropriate and understandable to individuals.

INDIVIDUAL CHOICE

Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

The ability of individuals to make choices with respect to electronic exchange of individually identifiable health information concerning them is important to building trust. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities and capabilities for individuals to exercise choice with respect to their individually identifiable health information. The degree of choice made available may vary with the type of information being exchanged, the purpose of the exchange, and the recipient of the information. Applicable law, population health needs, medical necessity, ethical principles, and technology, among other factors, may affect options for expressing choice. Individuals should be able to designate someone else, such as a family member, care-giver, or legal guardian, to make decisions on their behalf. When an individual exercises choice, including the ability to designate someone else to make decisions on his or her behalf, the process should be fair and not unduly burdensome.

COLLECTION, USE, AND DISCLOSURE LIMITATION

Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

Establishing appropriate limits on the type and amount of information collected, used, and/or disclosed increases privacy protections and is essential to building trust in electronic exchange of individually identifiable health information because it minimizes potential misuse and abuse. Persons and entities, that participate in a network for the purpose of electronic exchange *of individually identifiable health information, should only collect, use, and/or disclose information necessary to accomplish a specified purpose(s). Persons and entities should take advantage of technological advances to limit data collection, use, and/or disclosure.*

DATA QUALITY AND INTEGRITY

Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

The completeness and accuracy of an individual's health information may affect, among other things, the quality of care that the individual receives, medical decisions, and health outcomes. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, have a responsibility to maintain individually identifiable health information that is useful for its intended purposes, which involves taking reasonable steps to ensure that information is accurate, complete, and up-to-date, and has not been altered or destroyed in an unauthorized manner. Persons and entities have a responsibility to update or correct individually identifiable health information and to provide timely notice of these changes to others with whom the underlying information has been shared. Moreover, persons and entities should develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.

SAFEGUARDS

Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

Trust in electronic exchange of individually identifiable health information can only be achieved if reasonable administrative, technical, and physical safeguards are in place to protect individually identifiable health information and minimize the risks of unauthorized or inappropriate access, use, or disclosure. These safeguards should be developed after a thorough assessment to determine any risks or vulnerabilities to individually identifiable health information. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should implement administrative, technical, and physical safeguards to protect information, including assuring that only authorized persons and entities and employees of such persons or entities have access to individually identifiable health information. Administrative, technical, and physical safeguards should be reasonable in scope and balanced with the need for access to individually identifiable health information.

ACCOUNTABILITY

These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

These nationwide privacy and security principles will not be effective in building trust in electronic exchange of individually identifiable health information unless there is compliance with these Principles and enforcement mechanisms. Mechanisms for assuring accountability include policies and procedures and other tools. At a minimum, such mechanisms adopted by persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should address: (1) monitoring for internal compliance including authentication and

authorizations for access to or disclosure of individually identifiable health information; (2) the ability to receive and act on complaints, including taking corrective measures; and (3) the provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals.

---

[i] The U.S. Department of Health, Education and Welfare now the U.S. Department of Health and Human Services: http://www.hhs.gov/
Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973): http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

[ii] Markle Foundation: http://www.markle.org/
Common Framework for Networked Personal Health Information: Overview and Principles (Current as of 2008): http://www.connectingforhealth.org/phti/reports/overview.html

[iii] Organisation for Economic Co-operation and Development (OECD): *http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html*
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980): http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[iv] H*ealth Information Technology – Consumer Principles* (2006), Endorsed by: AARP AFL-CIO; American Federation of State, County and Municipal Employees; American Federation of Teachers; Center for Medical Consumers; Communications Workers of America; Consumers Union; Department for Professional Employees, AFL-CIO; Childbirth Connection Health Care for All; Health Privacy Project; International Association of Machinists and Aerospace Workers; International Union, United Auto Workers; National Coalition for Cancer Survivorship; National Consumers League; National Partnership for Women & Families; Service Employees International Union; Title II Community AIDS National Network; United Steelworkers International Union (USW): http://www.nclnet.org/health/final%202006%20principles%20PDF.pdf

[v] Federal Trade Commission (FTC): http://www.ftc.gov/
Privacy Online: A Report to Congress (1998) – Fair Information Practice Principles: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[vi] International Security Trust and Privacy Alliance (ISTPA): www.istpa.org
Analysis of Privacy Principles: An Operational Study (2007, Version 1.8): http://www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf

APPENDIX I: GLOSSARY

Administrative safeguards: Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic individually identifiable health information and to manage the conduct of the entity's workforce in relation to the protection of that information. Administrative safeguards include policies and procedures, workforce training, risk management plans, and contingency plans.

Collect/Collection: The acquisition or receipt of information, including individually identifiable health information.

Corrective measures: Actions taken to address a security breach or privacy violation, with the intent to counteract the breach or violation and reduce future risks.

Disclose/Disclosure: The release, transfer, exchange, provision of access to, or divulging in any other manner of information outside the person or entity holding the information.

Health Information: Any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individual: A person who is the recipient of health and/or wellness services.

Individually Identifiable Health Information: Health information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Open: Actively communicating information through notice or otherwise.

Persons and Entities: Health care professionals, partnerships, proprietorships, corporations and other types of organizations and their agents when acting on their behalf.

Physical safeguards: Physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. Physical safeguards include workstation security and use procedures, facility security plans, data backup and storage, and portable device and media controls.

Privacy: An individual's interest in protecting his or her individually identifiable health information and the corresponding obligation of those persons and entities, that participate in a network for the purposes of electronic exchange of such information, to respect those interests through fair information practices.

Security: The physical, technological, and administrative safeguards used to protect individually identifiable health information.

Technical safeguards: The technology and the policies and procedures for its use that protect electronic individually identifiable health information and control access to it.

Transparent: Making information readily and publicly available.

Use: Is the employment, application, utilization, examination, analysis or maintenance of individually identifiable health information.