December 21, 2007

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

Dear Secretary Leavitt:

I am pleased to present you with a report of the National Committee on Vital and Health Statistics recommending actions for "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data."[1] This report and its recommendations were developed in response to a request from the Office of the National Coordinator on Health Information Technology to address the benefits, sensitivities, obligations, and protections of uses of health data for quality measurement, reporting, and improvement; research; and other purposes that benefit the health of all Americans and the health care delivery system of the Nation.

Over the course of the last seven months, NCVHS heard testimony and deliberated about practical ways to ensure that benefits from more clinically rich information, available electronically and shared through health information exchanges, are accompanied by appropriate data stewardship for individuals' health data. It received comments from representatives of provider organizations, professional associations, accrediting organizations, consumer representatives, health plans, quality improvement organizations, health information exchanges, data aggregators, research and public health communities, and individual citizens.

Today, the health industry relies upon the HIPAA construct of covered entities and business associates to protect health data. The recommendations in this report call for a transformation to enhanced protections for *all uses* of health data by *all users*, independent of HIPAA covered entity status. NCVHS proposes that all organizations and individuals with access to personal health data follow attributes of appropriate data stewardship. The American Medical Informatics Association defines health data stewardship as encompassing the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information. NCVHS recommendations describe the attributes of

[1] NCVHS observes that "secondary use" of health data is an ill-defined term and urges abandoning it in favor of precise description for each use of health data.

appropriate health data stewardship as including, but not limited to: accountability and chain of trust, transparency, individual participation, de-identification, security safeguards and controls, data quality and integrity, and oversight of data uses.

The recommendations that are made in this report were guided by the goal of enabling improvements in health and health care, while balancing other needs including the need to: maintain or strengthen individual's health information privacy while enabling improvements in health and health care, facilitate uses of electronic health information, increase the clarity and uniform understanding of laws and regulations pertaining to privacy and security of health information, build upon existing legislation and regulations whenever possible, and not result in undue administrative burden.

In our deliberations, we identified several areas that require further analysis. One area is the process of de-identifying health data. There are many interpretations of what de-identification means. We also heard concerns about the ability to re-identify data, even while applying the HIPAA definition of de-identification. A second area relates to uses, and particularly the sale, of health data that are de-identified and therefore outside of the protections of HIPAA. A third area relates to the potential overlaps between quality and research, and where enhanced oversight may be useful. NCVHS will be further investigating and making subsequent recommendations in these areas. Finally there are a number of approaches to enhancing protections for health data uses within a NHIN that may be most appropriately evaluated in the trial implementations and other federally-sponsored demonstrations. NCVHS would be pleased to assist in such evaluations.

We appreciate your consideration of this report. If you or your staff would like a briefing on the recommendations, please let me know. We are committed to seeing benefits from uses of health data that can be achieved through health information technology while ensuring the protection of individuals' privacy.

Sincerely,

/s/

Simon P. Cohn, M.D., M.P.H., Chairman
National Committee on Vital and Health Statistics

Attachment
cc: DHHS Data Council

**NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS**

Report to the Secretary
of the U.S. Department of Health and Human Services

on

# Enhanced Protections for Uses of Health Data:
A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data

December 19, 2007

# Table of Contents

# Executive Summary

A transformation in health and health care is being enabled by health information technology (HIT). Clinically rich information is now more readily available, in a more structured format, and able to be electronically exchanged throughout the health and healthcare continuum. As a result, the information can be better used for quality improvement, public health, and research, and can significantly contribute to improvements in health and health care for individuals and populations. As the transformation to health information exchange (HIE) and a nationwide health information network (NHIN) occurs, there is an obligation to assure appropriate data stewardship[1] over the uses of individuals' health data.

The National Committee on Vital and Health Statistics (NCVHS) was asked by the Office of the National Coordinator for Health Information Technology (ONC) to develop a conceptual and policy framework to balance the benefits, sensitivities, obligations, and protections of what has typically been referred to as "*secondary uses*" of health data, including for quality and research uses. (NCVHS observes that "secondary use" of health data is an ill-defined term and urges abandoning it in favor of precise description for each use of health data).

In this Report, NCVHS summarizes the testimony it heard between June through October 2007, drawing observations about the benefits and concerns surrounding uses of health data. The NCVHS proposes recommendations intended to provide a durable framework, for all uses of health data by all users, irrespective of whether the data is *protected health information* collected and used by a HIPAA covered entity or business associate, or *personal health information* collected and used by an organization that is not a HIPAA covered entity. This framework is intended to anticipate and address data stewardship needs in the transition to HIE, a NHIN, and beyond.

### *Major Themes from Testimony*

NCVHS heard a wide range of testimony on several major themes concerning uses of health data, including both benefits and potential for harms:

- There is optimism for the growing number of benefits that can be achieved through uses of health data enabled by HIT and HIE. At the point of care, HIT enhances access to information and affords patient safety alerts and health maintenance reminders. Across the continuum of care, HIE enables readily accessible information needed in an emergency, and more complete information for coordination of care among providers. For quality measurement, reporting, and improvement, automated and structured data collection affords the

[1] The American Medical Informatics Association defines data stewardship as encompassing "the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information."

opportunity for efficient access to more comprehensive data and potential identification of new opportunities for improvement in care delivery. Clinical and population research and disease prevention and control are aided by access to more complete and timely data.

- There is potential for harms that may arise from uses of health data enabled by HIT and HIE. Erosion of trust in the healthcare system may occur when there is a divergence between what the individual reasonably expects health data to be used for and uses made for other purposes without the knowledge and permission of the individual. Compromises to health care may result when individuals fail to seek treatment or choose to withhold information that could impact decisions about their care because either they do not understand or do not trust how their data might be used or their identity protected. Risk for discrimination, personal embarrassment, and group-based harm may be amplified as there is greater ability to compile longitudinal data, re-identify data that have been de-identified, and share data through HIE.

Additional themes address the nature of enhanced protections needed, including attention to HIPAA Privacy and Security Rules, importance of data stewardship, and the need to address issues in specific uses of health data – including for treatment, payment, and healthcare operations; for quality measurement, reporting, and improvement; in research; for public health; and involving monetary exchange:

- Some commenters indicated that HIPAA provides adequate protections and may need only targeted administrative changes to address gaps or lack of clarity. Others observed that the relationship of business associates and their agents to covered entities needs strengthening to ensure that the chain of trust created through business associate contracts is assured and enables covered entities to provide transparency about uses of protected health information. There were concerns expressed about uses of de-identified data in general, and in particular the increasing ability to potentially re-identify data in merged databases. There were also cautions expressed about adding potentially burdensome and costly processes to HIPAA that may yield counterproductive results.

- A number of commenters described the importance of data stewardship for all uses of health data. A wide range of comments were heard. Some observed that current regulations may not fully address the expanding interest of consumers in their health data. They also observed that regulations may not fully address the potential harms that may arise from expanded uses of HIT and HIE. There were also segments of the general public that believed individuals have the only role in data stewardship, calling for individual permission for all uses of health data.

- With respect to specific uses of health data, the following issues were raised:

- For treatment, payment, and healthcare operations as defined under the HIPAA Privacy Rule, commenters raised the issue that the area of "healthcare operations" was broad in scope and not well-understood. It was noted that trust may factor more heavily than laws and regulations with respect to individuals and their privacy concerns as uses of data moved further away from the nexus of care.

- For quality measurement, reporting, and improvement activities, the question was raised as to whether the HIPAA definition of healthcare operations applies. Reviewing this definition and considering testimony, NCVHS believes that current quality activities remain within the HIPAA definition of healthcare operations and that enhancing transparency and applying internal oversight may allay any concerns.

- For research, it was observed that there were variations among federal agency regulations that would benefit from harmonization. There was also concern expressed that as quality activities are becoming more sophisticated, some may be evolving into research, potentially without the protections afforded by research on human subject regulations. The need to distinguish between quality and research and to appropriately shepherd quality into research was described.

- Use of health data involving monetary exchange was identified as an increasing concern. While there are instances where monetary exchange for health data is appropriate, there are uses that may result in harm, such as when individuals may not anticipate a use and as a result reduce their trust in their providers, or when there is undue influence over healthcare decisions as a result of a use, or when protected health information is not properly de-identified and is used to target marketing to individuals.

### *Guiding Principles*

NCVHS develops guiding principles to ensure its recommendations are consistent with the testimony heard and its task. NCVHS developed the following guiding principles to evaluate each recommendation for enhanced protections for uses of health data in light of new technologies. NCVHS recommendations for protections will:

1. maintain or strengthen individual's health information privacy
2. enable improvements in the health of Americans and the healthcare delivery system of the Nation
3. facilitate uses of electronic health information
4. increase the clarity and uniform understanding of laws and regulations pertaining to privacy and security of health information

5. build upon existing legislation and regulations whenever possible
6. not result in undue administrative burden

***Recommendations***

***In making its recommendations, NCVHS observes that currently, the health industry relies upon the HIPAA construct of covered entities and business associates to protect health data. Its recommendations call for a transformation, in which the focus is on appropriate data stewardship for all uses of health data by all users, independent of whether an organization is covered under HIPAA. NCVHS considers the attributes of data stewardship as including, but are not limited to: accountability and chain of trust, transparency, individual participation, de-identification of health data, security safeguards and controls, data quality and integrity measures, and oversight of data uses. The recommendations also recognize the circumstances under which data stewardship may apply and where there may need to be further analysis and other actions:***

1. **Recommendations for Data Stewardship on Accountability and Chain of Trust within HIPAA**:
   a. Covered entities should be specific in their business associate contracts about (i) what identifiable health data may be used and for what purpose, by both the business associate and its agents, (ii) what HIPAA-de-identified data may be used and to whom they are supplied, (iii) requiring business associates to have contracts with their agents that are equivalent to business associate contracts, and (iv) using the HIPAA definition for any de-identification of protected health information.
   b. Covered entities should confirm compliance by business associates with the terms of the business associate contract.
   c. HHS should provide guidance that any organization providing data transmission of protected health information and that requires access on a routine basis to the protected health information, such as an HIE or e-prescribing gateway, is a business associate.

2. **Recommendations for Data Stewardship on Transparency**. HHS should:
   a. Issue guidance to ensure that individuals have the opportunity to be informed about all potential uses of their health data (i) through education and clarity in the notice of privacy practices and other HIPAA administrative forms and required documentation and (ii) making information available about the specific uses and users of protected health information, including disclosures to public health, when requested.
   b. Develop and maintain a multi-faceted national education initiative that would enhance transparency regarding uses and of health data in an understandable and culturally sensitive manner.

3. **Recommendations for Data Stewardship on Individual Participation and Control over Personal Health Information Held by Organizations Not Covered by HIPAA Privacy and Security Rules.** HHS should:
   a. Urge the Federal Trade Commission (FTC) to utilize its full authority with respect to organizations that are not covered entities or business associates under HIPAA but that collect personal health information to ensure that (i) privacy policies on web sites collecting personal health information fully inform users of the uses that will be made of their personal health information and (ii) the organizations do not engage in misleading advertising or other deceptive trade practices.
   b. Assure that an authorization from the individual is obtained for collection, use, and disclosure of personal health information held by any organization *not covered* by HIPAA.

4. **Recommendations for Data Stewardship on De-identification**:
   a. HHS should issue guidance to covered entities that the HIPAA definition of de-identification (by statistical method or complete safe harbor definition) is the only permitted means to de-identify protected health information.
   b. NCVHS believes there are significant concerns surrounding uses of de-identified data that warrant more thorough analysis. NCVHS will conduct hearings to make subsequent recommendations.

5. **Recommendations for Data Stewardship on Security Safeguards and Controls**: HHS should issue guidance to covered entities to promote uses of technical security measures to reduce unauthorized access, and to ensure that their business associates and agents are fully compliant with the HIPAA Security Rule authorization, access, authentication, and audit control requirements. This should also be directed to organizations that are not covered entities that maintain and/or transmit personal health information.

6. **Recommendations for Data Stewardship on Data Quality and Integrity**: HHS data stewardship guidance should address the precision, accuracy, reliability, completeness, and meaning of data used for quality measurement, reporting, and improvement as well as other uses of health data.

7. **Recommendations for Data Stewardship on Oversight for Specific Uses of Health Data**:
   a. Quality measurement, reporting, and improvement remain within the scope of healthcare operations when conducted by covered entities, their business associates and their agents; across covered entities within an organized health care arrangement; and when under the accountability and data stewardship principles inherent in HIPAA. These uses may benefit from a voluntary, proactive oversight process accountable to senior management and governance of the institution to ensure there is compliance with HIPAA.

b. HHS should promote harmonization of research regulations within HHS and with other Departments that oversee regulations on human research protections to ensure consistent privacy and human subject protection for all research efforts.
c. HHS should encourage the Office for Human Research Protections (OHRP) in compiling its clarifying work on the research definition to continue to work collaboratively with the Office for Civil Rights (OCR) and to leverage the tools starting to be used in the industry to aid in distinguishing how requirements apply to uses of health data for quality and research, especially as questions relating to distinctions between research and quality uses of health data under the HIPAA healthcare operations definition arise. HHS should also encourage OHRP to widely disseminate its clarifying work, including beyond the research community.
d. HHS should foster the collaborative efforts between OHRP and OCR to identify approaches to ensure that when a quality study becomes generalizable and evolves into research, that HIPAA Privacy and IRB requirements are respected.
e. Certain areas require further investigation, such as research based solely on data from electronic health records, decedent research, and potential value for common oversight for quality and research within an organization. NCVHS will take the lead in working with OHRP and other federal agencies to further study these areas and make recommendations as appropriate.

8. **Recommendations on Transitioning to a NHIN**: NCVHS observes that at this time, a definition of a NHIN and how it will be used has not reached sufficient maturity to dictate how individual choice over uses of health data within a NHIN should or could be exercised. As a result, NCVHS recommends that trial implementations and other federally-sponsored demonstrations should include evaluation of: (i) the impact of applying good data stewardship, (ii) ways to manage individuals' authorizations, (iii) new methods or techniques to de-identify health data, (iv) chain of trust mechanisms between covered entities and business associates and their agents, (v) educational modalities to reach their target audiences, and (vi) appropriate safeguards needed to ensure that there is no unintended harm to individuals as de-identified data may be sold to support the possible business models of a NHIN.

9. **Recommendations on Additional Privacy Protections** – NCVHS has previously made several sets of recommendations setting the broad context for privacy improvement, including that privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. States are already beginning to enact laws intended to broaden protections. HHS should:
   a. Work with other federal agencies and Congress for more inclusive federal privacy legislation; and in the absence of comprehensive privacy legislation, HHS should address the need for more limited legislation that expands the

definition of covered entity under HIPAA, at a minimum to organizations such as vendors of personal health records systems that are not covered entities or business associates.

b. Work with other federal agencies and Congress for legislative or regulatory measures designed to eliminate or reduce as much as possible the potential discriminatory effects of misuse of health data.
c. Support the work of the Health Information Security and Privacy Collaboration (HISPC) that would guide harmonization among state laws where applicable and pinpoint where states have made explicit differences. HHS should support a state law mapping repository that clarifies where states differ and which aspects of state laws are more stringent than HIPAA.

# Introduction

## Purpose and Scope

A transformation in health and health care is being enabled by health information technology (HIT). Clinically rich information is now more readily available, in a more structured format, and able to be electronically exchanged throughout the health and healthcare continuum. As a result, the information can be better used for quality improvement, public health, and research, and can significantly contribute to improvements in health and health care for individuals and populations. As the transformation to HIE and a NHIN occurs, there is an obligation to assure appropriate data stewardship over the uses of individuals' health data.

The Office of the National Coordinator for Health Information Technology (ONC) asked the National Committee on Vital and Health Statistics (NCVHS) to develop recommendations for a conceptual and policy framework to balance the benefits, sensitivities, obligations, and protections of uses of health data, including for uses of health data for quality measurement, reporting, and improvement.

In developing recommendations to the Secretary of Health and Human Services (HHS), NCVHS adopted guiding principles that: maintain or strengthen individual's health information privacy; enable improvements in health and health care; facilitate appropriate uses of electronic health information; increase the clarity and understanding of laws and regulations pertaining to information privacy and security; build upon existing legislation and regulation whenever appropriate; and not result in undue administrative burden.

The NCVHS recommendations, therefore, are intended to provide a durable data stewardship framework, for all uses of health data by all users, irrespective of HIPAA covered entity status. This framework and other measures allow for a transition to occur to health information exchange (HIE), a NHIN, and beyond.

## Terminology

*"Secondary Uses" of Health Data*

As an initial step in developing its recommendations, NCVHS elected to describe each use of health data instead of using the term *secondary uses,* as has typically been used to collectively describe a wide variety of uses of health data. Secondary use of health data has no standard reference. Some consider primary uses of health data as those relating to direct care only, and all other uses secondary. Others consider primary uses inclusive of payment and healthcare operations as defined under the HIPAA Privacy Rule. In addition, grouping various uses of health data under the rubric of secondary use may result in treating all uses within that class the same. Different approaches may

be needed to afford protections for different types of uses. Finally, the term secondary use carries the connotation that these uses of health data are less important than other uses. As a result, NCVHS urges that the term "secondary use" be abandoned in favor of explicit description of each use of health data, such as "report communicable disease to public health," "use health data for quality improvement" or "keep health information in my personal health record."

*Terms Describing Health Data*

There are four key terms describing health data/information[2] that are important in the context of this report and they are described below.

- *Individually identifiable health information* is defined in HIPAA as "a subset of health information, including demographic information collected from an individual and: (1) is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (2) relates to the . . . health of an individual, provision of health care to an individual, or . . . payment for the provision of health care to the individual; and (3) that identifies the individual; or (4) with respect to which there is a reasonable basis to believe the information can be used to identify the individual" (45 CFR §160.103).

- *Protected health information* (PHI) is defined in HIPAA as "individually identifiable health information … that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium" by an entity covered under HIPAA (i.e., health plans, clearinghouses, and providers that transmit any health information in electronic form in connection with a transaction covered by the Administrative Simplification provisions of HIPAA) (45 CFR §160.103).

- *Personal health information,* as used in this report, is any individually identifiable information relating to the health, provision of health care, payment for healthcare, or other health information created by any individual or organization, irrespective of HIPAA covered entity status.

- *HIPAA de-identified health information* as used in this report is any health information, at the individual person level, which has been de-identified in accordance with the HIPAA definition of de-identification (using either a statistical approach or the safe harbor method of deleting 17 data elements plus any other unique identifier (45 CFR §164.514 (b)).

Additional terms are found in the **Glossary of Terms** in **Appendix C** (and definitions of **Abbreviations** used in this report in **Appendix E**). The glossary defines terms used

[2] For purposes of this report, no distinction is made between the meaning of *information* and *data*. The terms are used interchangeably, reflecting most common usage.

throughout this report, in testimony and related documents, and underscores the broader need for standardization of terms. For example, the terms *de-identification*, *anonymization*, and *pseudonymization* are all associated with protecting identity, but may be applied variably in different contexts, some of which diverge from the HIPAA definition of de-identification or limited data set (§164.514(a), (b), (c), and (e)), herein referred to as *HIPAA de-identification*.

### Organization of Report

This report includes:

1. **Background** – describing the process NCVHS undertook to hear testimony and obtain input on the current state and issues related to uses of health data that form the basis for the recommendations.

2. **Testimony and Considerations** – summarizing the testimony concerning the current state of health data uses and identifying significant gaps in protections for these uses which may be amplified as health information technology (HIT) and HIE become more prevalent.

3. **Guiding Principles** – identifying the six guiding principles that helped direct the recommendations.

4. **Observations and recommendations** – providing observations and recommendations described within a framework of data stewardship.

    a. Initial focus is on practical solutions that can be implemented today to address overall gaps in accountability, transparency, individual participation, de-identification, security safeguards, and data quality and integrity.

    b. Specific attention is also paid to recommendations for uses of health data that are most immediately enhanced through HIT and HIE – quality measurement, reporting, and improvement and research.

    c. There are recommendations for evaluation of approaches suitable to protect other and potentially unanticipated uses as transition is made to a NHIN.

    d. Recommendations that may take longer to implement are made for additional privacy protections, anti-discrimination, and state law mapping.

# Report Background

### NCVHS Coverage of Topic

NCVHS has a long history of engaging public comment, analyzing issues, and making recommendations to the Secretary of HHS on uses of health data from multiple perspectives.

In 1996, Public Law 104-191, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, directed the NCVHS to be responsible generally for advising the Secretary of HHS and the Congress on the status of the implementation of the HIPAA Administrative Simplification provisions. Subsequently, NCVHS has issued annual reports on various HIPAA compliance issues. Public Law 104-191 also directed the NCVHS to "study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information," which generated several sets of recommendations.

NCVHS has been at the forefront of promoting HIT and HIE. In 2001, NCVHS generated a report on *Information for Health: A Strategy for Building the National Health Information Infrastructure*, specifically addressing the need for a private, secure, and effective NHIN. *Recommendations on the Initial Functional Requirements for a NHIN* was delivered to the Secretary on October 30, 2006. Privacy issues within a NHIN were addressed in the NCVHS June 22, 2006 letter report, *Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network*. An update to the Privacy Letter with respect to coverage of healthcare and other organizations was delivered to the Secretary on June 21, 2007. The NCVHS *Report and Recommendations on Personal Health Records and Personal Health Record Systems* from February 2006 and its *Letter Report to the Secretary on Personal Health Record (PHR) Systems* from September 9, 2005, describe the state of affairs with respect to such health data collection.

NCVHS has also delivered numerous reports describing uses of health data for population studies and for use in quality improvement. Its *Recommendations on Populations Based Data Collection*, delivered to the Secretary of HHS on August 23, 2004, and its *Report on Measuring Health Care Quality* in May 2004 are seminal works on key issues for using health data. The *Recommendation Letter on Data Linkages to Improve Health Outcomes* on June 21, 2007 also addressed the special issue of merging data from disparate sources.

The NCVHS Web site (http://ncvhs.hhs.gov) provides access to all NCVHS documents referenced, as well as others.

## NCVHS Process

To enable NCVHS to make practical recommendations to facilitate uses and exchange of health data, the Committee's ad hoc work group (**Appendix A**) received public comment, both in formal testimony and in open public sessions.

### *Testimony and Comment*

NCVHS convened the workgroup at its meeting on June 21, 2007; then held three sets of public meetings in the Washington, DC area on July 17-19, August 1-3, and August

23-24, 2007 to receive verbal and written testimony. It published a draft document on its web site on October 19, 2007, and held an open call for public comment on October 31, 2007. (Testifiers and commenters are listed in **Appendix B**.) NCVHS also received a significant number of e-mail communications from private citizens concerning individual's consent for uses of health data. In the development of this report, NCVHS presented interim findings to the American Health Information Community (AHIC) Consumer Empowerment Work Group, September 12; Quality Work Group, October 3 and December 14; and full AHIC public meeting in Chicago on November 13, 2007.

Comments were received from provider organizations, professional associations, accrediting organizations, consumer representatives, health plans, quality improvement organizations, health information exchanges, data aggregators, research and public health communities, and individual citizens. Members of the NCVHS also participated in the conference on *Toward a National Framework for the Secondary Use of Health Data* sponsored by the American Medical Informatics Association (AMIA), June 14-15, 2007.

Although time for input was very short, NCVHS is appreciative of the effort so many put into contributing comments.

# Major Themes from Testimony about Uses of Health Data

NCVHS observes that enhanced protections for uses of health data is a controversial topic, with diverse viewpoints. NCVHS heard a wide range of testimony on several themes concerning uses of health data. These include assuring benefits while reducing the potential for harm, and the nature of enhanced protections. Some commenters indicated that HIPAA provides adequate protections and may need only targeted administrative changes to address gaps or lack of clarity. Cautions were expressed about potentially burdensome and costly processes that may be counterproductive.

Other commenters described the importance of data stewardship for specific uses of health data – including for treatment, payment, and healthcare operations; for quality measurement, reporting, and improvement; in research; for public health; and involving monetary exchange. Commenters suggested that current laws and regulations may not fully address the expanding role of consumerism and potential harms that may arise from expanded uses of HIT and HIE. Some segments of the general public viewed individuals as having the only role in data stewardship, calling for individual permission for all uses of health data.

### Benefits from Uses of Health Data Enabled by Health Information Technology (HIT) and Health Information Exchange (HIE)

NCVHS heard that the common good for all Americans is served when health data can be used to advance the quality of health and health care for the Nation. There is optimism for the growing number of benefits that can be achieved through uses of health data enabled by HIT and HIE.

*At the point of care*, HIT enhances access to information, affords patient safety alerts and health maintenance reminders, and supports care management. In an emergency, HIT enables speedier access to critical information. For example, during the hurricane disasters of 2005, the availability of more electronic health records would have improved health outcomes and likely would have saved lives. Across the continuum of care, HIE enables more complete information and coordination of care among referring providers and for transfer of care, such as from a hospital to a long term care facility.

*For quality measurement, reporting, and improvement*, automated data collection processes for obtaining clinical data (beyond what is available in claims data) provide richer data in an accessible form that facilitates benchmarking and identification of quality improvement opportunities in care delivery. HIT enables virtual aggregation of data and data linkage, such as individual person matching algorithms. This supports longitudinal data collection to expand understanding of the benefits of various therapies or interventions. Testifiers also described improved and developing techniques available to secure data and to attach authorization for use of data to the data itself.

*Clinical and population research* can be strengthened. For example, studying a population of children with autism might allow understanding of the environmental or biological causes of increased incidence and potentially permit earlier detection. Also, identification and participation of candidates for clinical trials across a wider geographic area enables larger cohorts for testing hypotheses. Health services and other population-based research may be aided through greater availability to data.

*Disease surveillance, control, and prevention* can be more accurate, complete, and rapidly accessible when new sources of data, fully automated data collection processes, and improved data linkage capabilities exist. For example, public health data could potentially detect, on a timely basis, areas of the country where an infectious disease is suddenly spreading, thus alerting health officials to take speedier action to save lives.

*Personal health management* is aided by individuals having access to personal health information that may be compiled within a personal health record supported by HIE. Individuals who monitor their own health may lead healthier life styles, may be in a better position to pay attention to early warning signs of illness, and be better able to coordinate care among multiple providers.

**Potential for Harm from Uses of Health Data Enabled by HIT and HIE**

Commenters also pointed out potential for harms that may arise from uses of health data enabled by HIT and HIE.

*Erosion of trust* in the healthcare system may occur when there is divergence between what individuals reasonably expect health data to be used for and when uses are made for other purposes without their knowledge and permission. Individuals generally appear

to have a high degree of trust in their providers. There also appears to be a high degree of trust in public health from the perspective of protecting against disease outbreaks; and in health research when accompanied by informed consent. Trust may erode and privacy concerns may increase, however, when uses of health data are made for other less widely recognized purposes. In addition, when health data are sold – even when used to ensure the sustainability of the business model for expanded uses of HIT and HIE or when the data are de-identified – there are heightened concerns.

*Compromises to health care* may result when individuals fail to seek treatment or choose to withhold information that could impact decisions about their treatment because they do not understand how their data may be used or they may not trust that their identity will be protected, particularly if they consider their information to be especially sensitive. HIT can afford greater protections, but these must be diligently applied and made known to individuals.

*Risk of discrimination and personal embarrassment* may be amplified as electronic health data become more widely available through greater ability to automate health data collection, compile longitudinal data, re-identify data that have been de-identified, and share data through HIE. There have long been concerns that personal health information is being used to make decisions that adversely affect an individual, such as in employment, benefits coverage, or acceptance for loans or mortgages.

*Potential for group-based harm* may arise when data are aggregated and results potentially misused. For example, there is the potential that classifying disease as more prevalent in certain ethnic or racial groups of people or in certain communities might cause members of that group or community to be subject to discrimination or stigma, even as aiding high risk groups by supporting new health services and treatments.

## HIPAA Privacy and Security Rules

While several testifiers observed that the HIPAA Privacy and Security Rules provide a foundation for data stewardship, testimony also identified that there still is confusion among covered entities on how to carry out some of the requirements of HIPAA – in both current uses of protected health information and in light of new uses of health data enabled by HIT and HIE.

### *Variation in State Laws*

HIPAA regulations cannot supercede a contrary provision of State law if the State law imposes more stringent requirements. The resultant variation among state laws may impede interoperability, particularly when HIE crosses state lines.

The interim report by the Health Information Security and Privacy Collaboration (HISPC) identified lack of trust between covered entities in carrying out disclosures to other treating providers, variable access by individuals to their health information (especially

cited was access to physician notes), and confusion between HIPAA and state laws where there were inconsistent requirements across states relative to authorization requirements for use and disclosure of health data for treatment, payment, and healthcare operations.[3]

*HIPAA Covered Entities and Business Associates*

The HIPAA Privacy and Security Rules only cover protected health information maintained and/or transmitted by covered entities. HIPAA Privacy and Security Rules do not directly cover organizations and their agents who may perform functions involving protected health information on behalf of a covered entity. Rather, the HIPAA Privacy and Security Rules require these organizations to have business associate contracts or other arrangements with covered entities to apply the protections afforded by these Rules.

There are concerns that business associate contracts are often written without specifically describing the permitted uses of protected health information. Business associate contracts often include only vague statements such as, "the contract covers use and disclosure of protected health information only as permitted or required or as otherwise required by law." What is permitted or required is not identified in the contract.

The intent of the business associate contract is to establish satisfactory assurances that the Privacy and Security Rules will be followed from the covered entity to the business associate and beyond (i.e., establishing a chain of trust). A particular challenge is that the farther removed the use is from the covered entity, the weaker is the ability to monitor the intent of the contractual obligations of health data protection.

*De-Identification*

Another challenge is that the HIPAA Privacy Rule only addresses protected health information, which is identifiable. Once protected health information is de-identified according to the HIPAA definition of de-identification, it falls outside of the jurisdiction of the HIPAA Privacy and Security Rules. There is no accountability or transparency back to the covered entity or the individual concerning use of these HIPAA de-identified data.

*Organizations and Information Not Protected by HIPAA*

Finally, testimony also indicated that there are growing uses of identifiable *personal health information* that fall outside of the HIPAA chain of trust (or other regulations, such as those covering research on human subjects). For example, when an individual supplies personal health information to a personal health record (PHR) web site not

[3] Linda Dimitropoulos, PhD, RTI International; William J. O'Byrne, New Jersey e-HIT; and Steve Posnack, ONC, Testimony on the Health Information Security and Privacy Collaboration (HISPC) Report of June 30, 2007, July 17, 2007

sponsored by a covered entity or business associate, the personal health information is not protected under HIPAA.

Testifiers observed that there will be increasing challenges with respect to HIPAA and chain of trust with hybrid PHRs, in which both covered entity-supplied and individual-supplied health data are collected.

**Importance of Data Stewardship**

As concerns increase about the widening range of uses of health data, there is an increasing need for appropriate data stewardship by all organizations and individuals that have access to health data, independent of HIPAA covered entity status. When an individual provides personal health information, whether to a provider, payer, online web site, or anyone else, the information is provided in confidence and with the trust that the information will not be used in unintended ways. In other words, the recipient of the health data is expected to demonstrate appropriate data stewardship.

The American Medical Informatics Association (AMIA) states that data stewardship "encompasses the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information." Further, AMIA notes that "principles of data stewardship apply to all the personnel, systems, and processes engaging in health information storage and exchange within and across organizations."

Views concerning a "national health data stewardship entity" were sought by the AHRQ, in a request for information about creating a "public/private entity that will set uniform operating rules and standards for sharing and aggregating public and private sector data on quality and efficiency; offer guidance on implementation of such national operating rules and standards; and provide a framework for collecting, aggregating, and analyzing data, to afford means of more effective oversight of healthcare data analyses and reporting in the United States." Whatever final configuration develops, respondents agreed that appropriate data stewardship was very much needed.[4]

NCVHS heard that when *any* organization that is responsible for making use of personal health information is trustworthy, there is greater acceptance of the use of the health data. This is the case independent of HIPAA covered entity status. Trust was observed to be something that an organization earned over time through acting as a responsible data steward. Trust may be enhanced through transparency and affording appropriate rights to individuals on how their health data may be used.

NCVHS observes that the HIPAA Privacy Rule, despite being broad in definition and not anticipating every future use, inherently includes an initial set of data stewardship

[4] National Health Data Stewardship, Request for Information, Agency for Healthcare Research and Quality, *Federal Register*, Vol. 72, No. 106, Monday, June 4, 2007.

principles for uses of health data. As new uses of health data are made in a new world of HIT and HIE, the framework of data stewardship inherent in HIPAA needs realignment to adapt to this changing landscape. Appropriate data stewardship is important for building transparency and trust throughout all organizations that may use health data for any purpose; and in particular to ensure that individuals are informed about uses of their health data which they may not anticipate.

It is important for all stakeholders to thoroughly understand the need for appropriate data stewardship for uses of health data. An educational campaign may be necessary to engage the public about the benefits and protections surrounding uses of health data. In addition, HIPAA covered entities, business associates and their agents, and other organizations not covered by HIPAA need education about appropriate data stewardship to enhance transparency and protect privacy.

It was also observed that transparency and trust have limits to their effectiveness and should not be substitutes for other measures. For example, the HIPAA notice of privacy practices (NPP) is a means to provide transparency, but does not achieve its purpose if it is not read or understood by individuals. Clarifying the language of a NPP or taking time to explain its contents, while beneficial, will not fully address trust issues.

**Specific Uses of Health Data**

NCVHS sought and heard testimony describing issues associated with those uses of health data that are most relevant to the current focus of HIE and NHIN, including uses for treatment, payment, and healthcare operations; quality measurement, reporting, and improvement; research; public health; and in monetary or other value exchange.

*Uses of Health Data for Treatment, Payment, and Healthcare Operations*

The HIPAA Privacy Rule permits covered entities to use and disclose protected health information without authorization from the individual in the following circumstances: when requested by the individual; for treatment, payment, and healthcare operations (TPO); incident to an otherwise permitted or required use or disclosure, provided the covered entity has taken adequate safeguards; and when required by law, public health, and for certain other uses within prescribed limitations.[5, 6] (State laws which are more stringent may require authorization for some uses or disclosures.)

- *Treatment* means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a provider with a third party; consultation

[5] HIPAA Privacy Rule, §164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required
[6] HIPAA Privacy Rule, §164.514 Other requirements relating to uses and disclosures of protected health information (e) Limited data set, (f) Fundraising, and (g) Underwriting and related purposes

between providers relating to an individual; or the referral of an individual for health care from one provider to another.

- *Payment* refers to the activities undertaken by a health plan to determine coverage and provision of benefits under the plan and to obtain or provide reimbursement for the provision of health care.

- *Healthcare operations* encompass quality assessment, competency review, health benefits processes, compliance activities, business planning, and general administrative activities (45 CFR §164.501).

A common theme that NCVHS heard in testimony related to the broad scope of some aspects of the HIPAA Privacy and Security Rules. Testifiers observed that HIPAA may serve well enough in providing data stewardship guidance for the "treatment and payment" processes of care delivery, but the area of "healthcare operations" was observed to be broad in scope and often not well-understood. It was noted that trust may factor more heavily than laws and regulations with respect to individuals and their privacy concerns. The further a use of health data is from the point of care, the less transparency there may be and the less individuals may trust the ability of their health data to be protected.

*Uses of Health Data for Quality Measurement, Reporting, and Improvement*

The definition of quality assessment and improvement activities, included in the HIPAA Privacy Rule under healthcare operations, includes "outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment" (45 CFR §164.501).

*Benefits* of quality measurement and reporting include the capacity to assess progress toward achieving high performance in the six dimensions of care identified in the Institute of Medicine *Quality Chasm* report, including: "better safety, effectiveness, patient-centeredness, timeliness, efficiency, and equity"[7] These aims require more clinically rich information than what is available solely from claims data. Individuals can make more informed decisions about their care when quality is accurately reported. Providers can improve the quality of care delivered when they understand the current status of the care being provided and have access to evidence-based protocols. Payers can assure greater value through pay for performance, pay for quality, and other mechanisms. Purchasers of care can ensure they are receiving value when they have

[7] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century,* Washington, DC: National Academies Press, 2001, p. 43

access to accurate quality reporting. These benefits are well understood, by providers, purchasers, and payers, but poorly understood or appreciated by individuals. Greater education of the public is needed in this area.

*Challenges* in uses of health data for quality measurement, reporting, and improvement include balancing the need for accurate and complete data to ensure meaningful outcomes while protecting individuals' privacy. Uses of identifiable health data for quality improvement are permitted under HIPAA. However, organizations are increasingly challenged to protect such data and to increase awareness in individuals of the value of using health data for quality improvement. HIT and HIE enables more complete and accurate data through linking health data about individuals longitudinally, across multiple settings, and from multiple sources. For example, data linkage enables identification of factors such as hospital re-admission rates that may signify quality issues. There are, however, increasing concerns that such data linkage may have the potential for heightened privacy risk. Yet, health data becomes less useful for quality improvement as more identifying information (such as admission date) is removed. To address both data needs and privacy concerns, some organizations are using de-identification techniques, such as pseudonymization that assigns a pseudonym to the data, to improve privacy protection while enabling re-identification to ensure accuracy and completeness of data.

*Organizations that link health data have an important place in promoting quality health care but must not violate the trust of individuals and providers.* For example, pharmacy benefits managers (PBMs), that may be covered entities or business associates, compiled medication histories for individuals impacted by the hurricane disasters of 2005 and provided an important public service. Today, such medication histories are being used to support medication reconciliation activities in compliance with The Joint Commission standards across provider settings. However, there are organizations who acquire health data by direct access through the systems they sell to HIPAA covered entities or by purchasing HIPAA de-identified data. Some of these organizations use the data to support quality purposes; but others may link the data to provider databases to market to providers, or use the data to market to a circumscribed population likely to include a target group of individuals.

*Uses of Health Data in Research*

Testifiers identified two important issues with respect to uses of health data in research – variation in research regulations across different federal agencies and distinguishing between uses of health data for quality and research in certain instances.

How health data may be used in research varies among the HIPAA Privacy Rule (§164.512(i)), the Federal Policy for Protection of Human Subjects (45 CFR 46, a.k.a. The Common Rule), the Food and Drug Administration (FDA) Protection of Human Subjects Regulations (21 CFR 50 and 56), and the Protection of Human Subjects of Research in the Veterans Health Administration (VA) Regulations (38 CFR 16).

The result of multiple and overlapping regulations can be confusion on the part of both individuals and researchers**.** An example cited was where an individual may be asked to participate in a research project sponsored by the VA and another project under the FDA jurisdiction, each with somewhat different requirements that may result in confusion about the two projects' needs for privacy protections.

In addition to the issues related to multiple regulations, testifiers also expressed concern about the overlap of quality activities and research. For example, using health data collected for quality improvement that evolves into a research study may violate the HIPAA Privacy Rule and/or The Common Rule, and yet be of profound importance to the health of the Nation.

> *For example, a review of cases for quality assurance may reveal that administration of a new drug is causing a previously undescribed and/or unanticipated consequence that may pose a public safety risk – a fact that may cause a more thorough study of the drug's use to be conducted and findings widely disseminated. In this example, the quality study takes on the systematic investigation and generalizable knowledge characteristics of research.*

A quality assessment study is defined under the HIPAA Privacy Rule as healthcare operations and does not require an authorization from the individual. However, use of protected health information for research either requires an authorization or a waiver of authorization from a privacy board, or an Institutional Review Board (IRB) when research is supported by federal funds. As value-based purchasing increases in prevalence and providers want to understand their own data better, the likelihood of compiling more comprehensive databases for immediate quality measurement and improvement increases. Such work initiated as part of performance improvement likely will result in more frequent discovery of important, reportable findings that can improve quality of care for a larger population. How to distinguish a quality activity from a research study, and how to ensure protection of the data commensurate with that of a research study when the use of the data evolves from quality were issues cited by both provider and payer testifiers.

*Uses of Health Data for Public Health*

Public health databases are used for surveillance and to compile registries, such as in support of cancer treatment and to track immunization. Such uses are authorized by state and local law, and permitted under HIPAA. Yet surveillance is extending in scope, such as to collect Hemoglobin A1c results with the intent to contact individuals directly about potential improvements in diabetes management (e.g., New York). Testimony indicated that the transparency of such uses is variable. Many individuals are unaware of required reporting; others are aware to the extent that they may see a caregiver under a false name to avoid consequences of reporting.

Public health data collected directly by the Centers for Disease Control and Prevention (CDC) are obtained using a variety of mechanisms. Included are health statistical data obtained from surveys, which may be conducted under an IRB process or with the informed consent of the individual responding to the survey. These data may be released to others only through strict data release agreements or as statistically de-identified datasets. CDC is starting nationwide data collection efforts, such as the BioSense project, that involve contractual agreements similar to HIPAA business associate contracts. Such efforts utilize new data sources and are enabled by automated data collection processes and data linkage capabilities. However, and despite new and better techniques to protect data, such large databases may present unanticipated issues or concerns for public health activities.

*Uses of Health Data in Exchange for Money or Other Financial Benefit*

The issue of exchanging data for money or other financial benefit was raised as a use of health data that needed heightened attention. It is important to note that some uses of health data that result in financial benefit to an organization also benefit the individual recipient of health care, directly or indirectly. However, there are potential harms that may result as well.

The following are examples of benefits where money or other forms of financial benefit have been exchanged for health data: Hospitals submit supplemental health data on core measures to the Centers for Medicare and Medicaid Services (CMS) in exchange for the hospital receiving full reimbursement under the Medicare Conditions of Participation.[8] This equips individuals with quality-of-care information to make informed provider choices. Researchers may purchase HIPAA de-identified health data to determine the prevalence of a certain type of disease before conducting a thorough research study under the auspices of Institutional Review Board (IRB) approval. This enables research to improve the overall quality of health and health care. Pharmaceutical manufacturers may purchase HIPAA-de-identified data to conduct post-marketing drug surveillance at a macro level, which contributes to medication safety. HIEs may charge subscription fees for data consolidation and transmission services they provide. HIEs enable providers to gain access to more complete health data for the individuals they treat.

NCVHS, however, heard concerns relating to the sale of, or other value exchange for, health data. Such uses are not anticipated by the individual, may unduly influence healthcare decisions, and may result in target marketing to individuals:

*Unanticipated use of health data involving exchange of money.* Individuals are especially concerned about uses of their health data which they did not anticipate when they originally shared this information with their provider. For example, a supplier of an

[8] Reporting Hospital Quality Data for Annual Payment Update, www.cms.hhs.gov/HospitlQualityInits/20_HospitalRHQDAPU.asp (accessed 11/30/07)

EHR system may contract with a provider to sell de-identified health data from the provider's EHR to other companies in return for supplying the provider with a portion of the proceeds from the sale of the data. The EHR supplier may merge this data with other databases, potentially causing it to be re-identifiable. Individuals expressed concern about such unanticipated uses of their health information, the financial gain from such transactions, and the potential for re-identification of the data.

*Use of health data by third parties to influence healthcare decisions.* A supplier of HIT or HIT services may be provided access to health data in an EHR or PHR to target advertisements to the provider (via the EHR) or the individual consumer (via the PHR) in return for money or a discount on services provided (e.g., license fee for the EHR or PHR). These advertisements may unduly influence health decisions made by the provider or individual. A specific example arose during the NCVHS proceedings where a pharmacy benefits manager (PBM) sold data to data mining companies for subsequent use by pharmaceutical companies in marketing targeted to providers. A PBM may be a covered entity or a business associate with the right to aggregate data, but the concern expressed was that such marketing may increase the sale of trade drugs, which may increase the cost of health care.[9]

*Use of health data for targeted marketing to individuals*. HIPAA is very specific that an individual's signed authorization for any use or disclosure by covered entities of protected health information for marketing is required except if the communication is face-to-face by the covered entity to an individual or if it is in the form of a promotional gift of nominal value provided by the covered entity (45 CFR §164.508(a)(3)(i)). HIPAA also specifies that if marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved (45 CFR §164.508(a)(3)(ii)). While HIPAA does permit the de-identification of protected health information which then may be used for any purpose, there are two potential risks associated with using de-identified data in marketing to individuals. First, de-identified data purchased from a specific provider may be used to target individuals in the geographic vicinity of the provider. When they receive the marketing material that appears to be targeted directly to them they may feel betrayed that information was disclosed by their provider to a marketer. Second, protected health information may not have been de-identified in accordance with HIPAA requirements making it re-identifiable, especially when linked with public databases. In these cases, the result is protected health information being used for marketing which is not permissible under HIPAA – putting the covered entity in non-compliance and potentially harming the individual receiving such marketing materials.

NCVHS recognizes that this area is complex and deserving of additional attention. As such, additional hearings are being planned to further investigate the issues and make recommendations where applicable.

[9] Eyre, E. "Company Sold PEIA Prescription Information, *The Charleston Gazette*, November 25, 2007.

# Guiding Principles for Making Recommendations on Enhanced Protections for Uses of Health Data

As NCVHS considered the testimony and its task to develop recommendations for enhanced protections for uses of health data in light of new technologies and health information exchange, it recognizes there are diverse viewpoints – both in the public and within its membership. NCVHS adopted the following guiding principles[10] to help develop recommendations that strike a balance between assuring benefits from optimal uses of health data, but not at the cost of reasonable privacy. Protections should . . .

1. maintain or strengthen individual's health information privacy
2. enable improvements in the health of Americans and the healthcare delivery system of the Nation
3. facilitate appropriate uses of electronic health information
4. increase the clarity and understanding of laws and regulations pertaining to privacy and security of health information
5. build upon existing legislation and regulations whenever appropriate
6. not result in undue administrative burden

# Observations and Recommendations

***Today, the health industry relies upon the HIPAA construct of covered entities and business associates to protect health data. The following recommendations call for a transformation to enhanced protections for all uses of health data by all users, independent of HIPAA covered entity status. NCVHS believes that all organizations and individuals with access to personal health data should follow attributes of appropriate stewardship, including, but not limited to:***

1. ***Accountability and chain of trust***
2. ***Transparency***
3. ***Individual participation***
4. ***De-identification***
5. ***Security safeguards and controls***
6. ***Data quality and integrity***
7. ***Oversight of data uses***

***As there is much to be learned about a NHIN, recommendations also recognize circumstances where there may need to be further analysis and other next steps.***

[10] Adopted from "Criteria for Evaluating Solutions" described in the Minnesota Health Records Act Fact Sheet, June 7, 2007, developed in response to concerns about the lack of consensus around the best solutions for implementing Minnesota's patient consent requirements within health information exchange.

A framework of data stewardship for health data uses may aid potential users contemplating a specific use of health data to analyze the use and consider appropriate ways to address data stewardship. In general, a framework is a conceptual structure used to think about a complex issue and outline possible courses of action. Achieving the benefits of health data uses while reducing the potential for harms presents a complex issue among a myriad of uses and users of health data. No single report can identify all uses and users, let alone anticipate all potential new uses and users. The Data Stewardship Conceptual Framework for Health Data Uses, in **Appendix D**, serves as a tool for organizations in evaluating the need for enhanced data stewardship for any contemplated use of health data.

***HHS has a variety of means to promote appropriate data stewardship and achieve enhanced protections for uses of health data. These include issuance of guidance, such as the HIPAA Security Guidance distributed by CMS on December 28, 2006; generation of requirements for Federal agency adoption; inclusion of requirements in contractor rules; provision of incentives; inclusion in Conditions of Participation rules; and modification of other processes in addition to recommending new legislation and issuing new regulations. The recommendations that follow should be adopted by whatever means is most expeditious and will promote the broadest possible adoption, including those which will most influence organizations not covered by HIPAA.***

***NCVHS commits to monitoring the usefulness of this guidance and offering further recommendations as may be needed.***

## 1. Observations and Recommendations for Data Stewardship on Accountability and Chain of Trust within HIPAA

*HIPAA Covered Entities*

The HIPAA Privacy and Security Rules apply directly only to healthcare payers, clearinghouses, and providers who electronically transmit health information in connection with transactions for which HHS has adopted standards under HIPAA. The protections afforded by the Privacy and Security Rules apply only indirectly to other organizations that may have access to protected health information when received from or on behalf of a covered entity.

*Business Associates and Their Agents*

The HIPAA Privacy and Security Rules require covered entities to enter into a contract, or other agreement, with organizations that support the business of the covered entity. The business associate contract must establish the permitted and required uses and disclosures of protected health information by the business associate, and essentially

binds the business associate to the data stewardship principles inherent in the HIPAA Privacy and Security Rules. The covered entity may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate and to provide data aggregation services relating to the healthcare operations of the covered entity. The provisions in the HIPAA Privacy and Security Rules describe that the contract must be able to be terminated by the covered entity if there is a material breach that cannot be reasonably cured or end the violation, as applicable, and if such steps to cure were unsuccessful. (45 CFR §164.504(e) and §164.314(a))

In practice, NCVHS heard that an explicit enumeration of what data the business associate will use or how it intends to use the data is often not included in business associate contracts. Many business associate contracts are vague on what the business associate can do with protected health information.

Furthermore, since HIPAA de-identified data are not protected health information under HIPAA, business associates or their agents may use de-identified data for purposes not required to be described in the business associate contract. There are also no assurances that the de-identification process used by the business associate will be consistent with that required by HIPAA. NCVHS heard testimony concerning varying ways protected health information may be de-identified.

Without assurances of proper de-identification methods being employed and without an awareness of the uses made of de-identified data, covered entities are unable to describe what uses may be made of individuals' data and are not able to confirm whether proper and reliable methods of de-identification are being used. The risk of information being re-identified continues to increase as more public databases become available and techniques for re-identification become more sophisticated.

Re-identification of information that was previously believed to be de-identified constitutes a use of protected health information not described in, and in violation of, a business associate contract. If re-identification occurs further down the chain of trust, it is more difficult for the business associate to identify such a violation and report it to the covered entity. Consequently, these issues open up an individual's data to uses that the individual does not anticipate and for which the individual may not be in agreement.

Business associate contracts require business associates to report to the covered entity "any use or disclosure of the information not provided for by its contract of which it becomes aware" (§164.504(e)(2)(ii)(c)). However, business associate contracts do not require periodic review or renewal. Since the description of permitted uses and disclosures is broad, the covered entity may be unaware of uses and disclosures the business associate is making of health data as these change over time.

> *For example, a business associate may collect data for the purpose of aggregating data for provider accreditation activities. Once the data are de-identified, the*

*business associate may set up a web site for public reporting of provider-specific chronic disease benchmarks.*

Business associates are also permitted to utilize agents in support of their work with covered entities. Business associates must ensure that any agents, including a subcontractor, to whom it provides protected health information . . . agrees to the same restrictions and conditions that apply to the business associate" (§164.504(e)(2)(ii)(D)), or in the case of the Security Rule "ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it ((§164.314(a)(2)(i)(B)).

Business associates are not explicitly required to have a business associate contract with their agents that enumerate uses of data, and they are not required to identify the agents to the covered entity. As a result, there is no opportunity for the covered entity to monitor health data usage by agents of business associates. Consequently, the desired "chain of trust" is broken.

*For example, an EHR vendor that has a business associate contract with a covered entity may use a third party application service provider (ASP) to host the covered entity's EHR data at a remote location. The agent of the business associate, however, may de-identify the data and sell it to a health products supply vendor that links it to provider data and hence is able to market to individuals in specific geographic regions, without the covered entity being aware of the use, object to the use, or describe such use to individuals it serves.*

*Organizations Providing Data Transmission Services*

Organizations whose business is to transmit health data may or may not be business associates. If such transmissions are likened to an envelope, many of these organizations only transmit data via routing information on the outside of the envelope. The response to a Frequently Asked Question (FAQ) posted on the HHS Office for Civil Rights (OCR) web site, observes that "the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information." A conduit is described as "an organization that transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation services or as required by law." The response to the FAQ goes on to note that "since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity."

However, there are some organizations that provide transmission services which do need access to the contents of the envelope on a routine basis. Examples might include e-prescribing gateways that may need to convert a prescription transaction for an

individual from one version of the National Council for Prescription Drug Programs (NCPDP) standard to another, or from the electronic transaction to a fax where an individual's preferred pharmacy cannot accept a transaction. Banks are increasingly gaining access to explanations of benefits addressed to individuals as they process electronic funds transfers. Some of these organizations recognize themselves as business associates or are required by the covered entity with whom they do business to have business associate contracts. In other cases, however, the organization may originally not have been a business associate, but over time the level of access may increase.

> *For example, an e-prescribing gateway that only initially transmitted data between providers and pharmacies as a conduit may become a business associate when it is asked to follow a provider's specific routing instructions based on drug type for prescription refill requests.*

1.1 **Recommendation on business associate contract provisions**: HHS should update applicable guidance documents, including its business associate contract model form, and take other applicable means to ensure that covered entities **specify the limits of health data use in their business associate contracts**. Such guidance and models should continue to be available for use on a voluntary basis. In addition, HHS should apply these means to limit uses of health data in their own agreements. Covered entities should specify in their business associate contracts:

1.1.1 **terms that explicitly describe what identifiable health data may be used and for what purposes, by both the business associate and by any agents with whom the business associate may contract.** Specificity in the contract allows the covered entity to describe such uses to individuals and determine any potential changes over time. **The contract must not permit the business associate to use or disclose identifiable health data in ways that the covered entity is not permitted to use or disclose.**

1.1.2 **terms that explicitly describe what HIPAA-de-identified data may be used and to whom HIPAA de-identified data are supplied.** This allows the covered entity to describe such uses to individuals and determine any potential changes over time.

1.1.3 **that there must exist a contract, with protections equivalent to the business associate contract as described above, between the business associate and all of its agents**, including agents of agents. This assures a chain of trust from the covered entity through all organizations that may have access to identifiable or HIPAA de-identified health data. It also enables the covered entity to be able to describe uses

of health data made by agents to individuals and determine any potential changes over time.

1.1.4 **that any organization that supplies de-identified health data for a specified purpose will ensure that the de-identification process follows the HIPAA requirements for de-identification**. (See also Recommendation 4.1.)

1.2 **Recommendation on confirmation of business associate contract compliance**: HHS should take applicable means to ensure that covered entities can confirm compliance by business associates with the terms of the business associate contract on a regular basis. A regular confirmation of compliance with the business associate contract would ensure that:

(a) business associates' actions remain consistent with the permitted uses,
(b) all agents have been properly engaged by the business associates, and
(c) the business associate and its agents are in compliance with all other applicable provisions of the business associate contract.

In the event of any changes in uses or agents, the business associate contract must be amended. This recommendation may be accomplished by HHS:

1.2.1 issuing guidance about practical scenarios where a covered entity fails to appropriately address a contractual violation by a business associate that could result in violations of the HIPAA Privacy Rule for a covered entity

1.2.2 updating the business associate contract model form

1.2.3 incorporating such confirmation of compliance in HHS own business associate agreements.

1.3 **Recommendation on organizations providing data transmission functions**: HHS should provide guidance that clarifies that any organization providing data transmission of protected health information and that requires access on a routine basis to the protected health information in order to conduct the transmission is a business associate and must be bound by the requirements for business associates. This does not apply to routing instructions external to the protected health information content of the transmission nor to only incidental disclosures, such as when investigating a potential security incident or upgrading equipment.

## 2. Observations and Recommendations for Data Stewardship on Transparency

The primary means by which HIPAA covered entities provide transparency today is through distribution of a notice of privacy practices (NPP), which is intended to explain to individuals how their protected health information may be used and disclosed. Providers who have a direct treatment relationship with an individual must make a good

faith effort to have the individual acknowledge receipt of the NPP. As a result, the NPP is often referenced as a "HIPAA consent," when it is only an informational document advising individuals about the covered entity's information policies and procedures. In addition, the NPP is frequently long, difficult to read, and is only required to provide examples of uses and disclosures. A NPP is not required to describe potential uses of de-identified data.

Because of the limitations inherent in the NPP and its use, and the extensive network of business associates and their agents that many covered entities use, the NPP is not serving well in alerting individuals to all potential uses of their health data or clarity surrounding how they may exercise control over uses of their health data. NCVHS heard testimony about several projects focusing on the need for transparency in communication about personal information. Findings from these projects revealed a number of insights:

> *In a consumer research project for developing privacy notices performed for six federal agencies, it was found that the point of a disclosure form is not to lead people to a conclusion or particular action, but to give them information to make an informed decision – based on their own values*.[11]
>
> *A risk communication specialist discussed advice for medical institutions concerning concerns about misunderstanding or misuse of information released to persons or the public, indicating that the remedy for misunderstanding is always more information, not less*.[12]
>
> *A "lay person's" perspective observed that most individuals do not know about the use of their personal health information; that physicians are often worried about these uses; and that transparency would lead to investment in increasing involvement and engagement by individuals in their health care*.[13]

In addition to the NPP, the next most visible way covered entities have of explaining disclosures of protected health information is the *authorization* for uses and disclosures, commonly referred to as an authorization for release of information. There are two issues associated with uses of an authorization as intended by the HIPAA Privacy Rule.

The first issue associated with the use of an authorization as intended by the HIPAA Privacy Rule is that it does not *require* an authorization to use or disclose to another covered entity protected health information for treatment, payment, or healthcare operations, so long as the entities have a relationship with the individual who is the subject of the protected health information (§164.506(c)). An authorization, however, is required for other uses and disclosures that are enumerated in (§164.508). However,

---

[11] Susan Kleimann, PhD, Kleimann Communication Group, Inc., Testimony, August 23, 2007
[12] Peter M. Sandman, Written Testimony, August 8, 2007
[13] Sharon F. terry, Genetic Alliance, Testimony, August 2, 2007

the Privacy Rule *permits* a covered entity to obtain a *consent* for uses and disclosures for treatment, payment, and healthcare operations by covered entities (§164.506(a)). C*onsent* in health care more commonly refers to the permission given by an individual to a provider for providing healthcare services (which may include interviewing, examination, specimen collection, and treatment of the individual, as well as use of health information). In summary, the use of the terms *authorization* and *consent,* and when such are required or permitted, causes confusion.

The section on consent (45 CFR §164.506(a)) in the original HIPAA Privacy Rule was modified in 2002 from requiring to permitting consent for use or disclosure of an individual's protected health information for a covered entity's use in treatment, payment, or healthcare operations. This still allows covered entities to obtain consent as desired, and to follow more stringent state laws containing "consent requirements" for uses and disclosures of protected health information for treatment, payment, and healthcare operations. Some public comment urged a return to the requirement of consent for all uses and disclosures of protected health information.
NCVHS does not support changing this requirement at this time, but to build upon the HIPAA Privacy Rule to enhance privacy protections and to evaluate ways to manage individuals' authorizations in a NHIN (see Recommendation 8.1.2).

The second issue with respect to the authorization requirement in the HIPAA Privacy Rule relates to the core elements and required statements that must be included in the authorization (at §164.508(c)). These elements are intended to afford transparency, but if not written in plain language, may be confusing and even intimidating. NCVHS received comments that clarifying the use and content of authorization forms would be helpful. NCVHS also observed that there are a number of other requirements for administrative documentation that would likely benefit from careful review.

2.1 **Recommendation on Transparency**: HHS should issue guidance to ensure that individuals have the opportunity to be informed about all potential uses of their health data. Transparency should be achieved through:

2.1.1 **education and clarity in the NPP**: HHS should issue guidance to covered entities on the importance of the NPP to transparency. As an initial step, HHS should issue guidance on writing model notices in plain language, clarifying that the NPP is neither an authorization nor consent. HHS should also offer other tools to enhance understanding of the NPP and find ways to make the acknowledgement of receipt a more meaningful process.

2.1.2 **education and clarity in other HIPAA administrative forms and required documentation**: HHS should issue guidance to covered entities on the appropriate uses of an authorization for uses and disclosures of protected health information, clarifying definitions and uses of authorization and consent, and the importance of transparency intended by the authorization. HHS should issue guidance on writing model

authorizations in plain language. This guidance should extend to other administrative documentation required for evidence of compliance with the HIPAA Privacy and Security Rules.

2.1.3 **making information available about the specific uses and users of protected health information when requested**: HHS should issue guidance to covered entities to incorporate reference in the NPP that additional information about how protected health information is used by business associates and their agents shall be made available upon request. A regular confirmation of business associates and their agents such as described in Recommendation 1.2 would permit the covered entity to keep such information current and able to supply the information when individuals express concern about uses of their health data.

2.1.4 **making information available about the specific nature of protected health information disclosed to other organizations, such as public health**: HHS should issue guidance to covered entities to incorporate references in the NPP about what types of protected health information are disclosed to other organizations, such as when legally required or permitted for public health purposes, and make this information available to individuals upon request.

2.2 **Recommendation for education on uses of and protections for health data**: HHS should develop and maintain a multi-faceted national education initiative that would enhance transparency regarding uses of health data, including for quality measurement, reporting, and improvement and for research, in an understandable and culturally sensitive manner. The initiative should involve all relevant HHS agencies. Educational activities should be appropriately integrated into Federal agencies' respective programs, policies and practices, as well as directly targeted to public and professional audiences. Various educational modalities should be included in NHIN trial implementations and other federally-sponsored demonstrations.

## 3. Observations and Recommendations for Data Stewardship on Individual Participation and Control over Personal Health Data Held by Organizations Not Covered by HIPAA Privacy and Security Rules

Protections afforded by HIPAA only extend to covered entities and through contractual arrangements to their business associates and the agents of the business associates. This leaves many organizations outside of the protections afforded by HIPAA:

- *Providers who do not accept insurance or who do not file claims electronically* are not covered entities. NCVHS observes that several types of providers are not covered by HIPAA. These providers may be very small and exempt from filing electronic claims with Medicare, do not file claims with Medicare and are

otherwise not required to file claims electronically, or their patients self-pay. They may also be providers that create records covered by the Family Educational Rights and Privacy Act (FERPA) which are explicitly excluded from the definition of protected health information.[14]

- *Personal health record services* that are not offered by covered entities are increasing in number. While a number of personal health records are supported by providers or health plans, others are independent commercial products, frequently offered via web sites. The Congress has not enacted any law requiring privacy policies on web sites; however, the Federal Trade Commission (FTC) has broad authority under the Federal Trade Commission Act to bring enforcement actions against organizations engaging in "unfair or deceptive acts or practices in or affecting commerce."[15] The FTC can use this authority to prosecute organizations that mishandle consumers' personal information. An increasing number of states are following the lead of the California Online Privacy Protection Act (COPPA) that requires the operator of any web site that collects "personally identifiable information" from California residents to post a privacy policy. In California, violators are subject to an injunction and/or a civil penalty of $2,500 for each infraction. Private causes of actions can also be brought under this statute.

- *Other organizations with no relationship to covered entities*, such as life insurers, employers, schools, and others, may also collect individually identifiable health data and are not regulated by HIPAA. While individuals may voluntarily choose to participate in such data collection, there are concerns as to whether individuals are aware of how the data may be used. As personal devices that collect health data and automatically transmit the data electronically to web sites become more prevalent, concerns about how the data are used are increasing.

  *For example, an employee posting health information to an employer wellness program web site may be unaware that the data are used by the employer to design insurance benefit packages.*

3.1 **Recommendation on FTC privacy policy support**: HHS should urge the Federal Trade Commission (FTC) to utilize its full authority with respect to organizations that are not covered entities or business associates under HIPAA but that collect personal health information to ensure that (1.) privacy policies on web sites collecting personal health information fully inform users of the uses that will be made of their personal health information and (2.) the organizations do not engage in misleading advertising or other deceptive trade practices. Further, if more inclusive Federal privacy legislation is enacted, these web sites must be

[14] NCVHS Letter to the Secretary of HHS on Update to Privacy Laws and Regulations Required to Accommodate NHIN Data Sharing Practices, June 21, 2007
[15] Privacy Policies Increasing in Importance, Willcox & Savage P.C., April 2006

included. HHS should then collaborate with the FTC to promote harmonization of regulations covering these organizations to ensure consistent privacy protection.

3.2 **Recommendation on obtaining authorization for use of personal health information not covered by HIPAA protections**: HHS should take applicable means to ensure that an authorization from the individual is obtained for collection, use, and disclosure of personal health information held by any organization *not covered* by HIPAA. See also Recommendation 9.1

## 4. Observations and Recommendations for Data Stewardship on De-Identification

The HIPAA Privacy Rule applies only to protected health information. Therefore, the Privacy Rule permits use of de-identified data without individual authorization. The Privacy Rule requires either a safe harbor or statistical approach to de-identification. De-identification removes the data from the protection of HIPAA requirements.

In addition, applications of HIPAA's safe harbor definition of de-identification often remove only the 17 data elements in the definition and ignore the requirement to remove "any other unique identifying number, characteristic, or code, except as permitted" (§164.514(b)(2)(i)(R)). Furthermore, one testifier indicated that removal of the 17 data elements specified in HIPAA may result in a small ability to re-identify an individual.[16]

Other forms of identity protection, such as anonymization, masking, etc. (see **Appendix C**: Glossary of Terms), have also been adopted – whether to remove the data from the protection of HIPAA or to enhance the protection beyond what is required. For example, covered entities are permitted to disclose protected health information for public health purposes. Because public health departments are very sensitive to the data they hold, they may use an approach called pseudonymization to protect the identity of the data yet enable re-identification when authorized. Other organizations, however, may be using de-identification techniques that are not consistent with the HIPAA requirements and pose a risk to personal privacy.

Finally, testifiers identified concerns about de-identification and offered the following examples:

> *Example 1: While not all uses of de-identified data pose a risk to individuals, the lack of transparency about such uses and the inability to opt into or out of such uses are concerns. When individuals receive marketing that appears to be targeted to them individually, they may well question the source of the data and be frustrated by the inability to exercise control over such use.*

[16] In testimony on August 23, 2007, Latanya Sweeney, PhD, Carnegie-Mellon University, described a 0.04% chance of re-identifying data when de-identified by removal of the 17 data elements in the HIPAA safe harbor definition of de-identification when compared to voter registration records for a confined population.

*Example 2: There is potential for risk to accrue not only to individuals but providers as well. The Prescription Project raised concerns about potential conflicts of interest in the medical profession created by pharmaceutical marketing conducted through linking physician prescribing records with physician demographic data.*[17]

*Example 3: Data mining is another technology increasingly being applied to health data. Electronic health records may be mined to generate on-screen ads. While meant to afford the opportunity for physicians to acquire electronic health record systems at no cost, there are also concerns that such a business model may violate individual-physician trust.*[18]

4.1 **Recommendation on de-identification**: HHS should issue guidance to covered entities (1.) explaining the practical situations and problematic issues surrounding uses and disclosures of HIPAA de-identified data and (2.) clarifying that the HIPAA definition of de-identification (by the statistical method or complete safe harbor definition) is the only permitted means to de-identify protected health information.

4.2 **Recommendation on uses of de-identified data**: NCVHS heard that there are significant concerns surrounding uses of de-identified data and that these warrant more thorough analysis. NCVHS will conduct hearings to determine how to structure guidance for best data stewardship practices. Topics which should be addressed may include, but not be limited to, use of the statistical de-identification process to meet a certain threshold for probability of re-identification, uses involving sale of de-identified data, exposure from re-identification, potential for group-based harms, and allowable uses of de-identified data.

## 5. Observations and Recommendations for Data Stewardship on Security Safeguards and Controls

The HIPAA Privacy Rule describes implementation specifications for minimum necessary uses of protected health information, including the identification of persons or classes of persons in its workforce who need access to protected health information to carry out their duties, and for each person or class of persons the category or categories of protected health information to which access is needed, and any conditions appropriate to such access (§164.514(d)(s)(A) and (B)). It also includes a "mini-security rule" at §164.530(c) where the covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

[17] Sean Flynn, Prescription Project, August 23, 2007.
[18] Dolan, P.L., "Free Electronic Medical Record System Comes with Strings Attached," *AMNews*, May 7, 2007.

The HIPAA Security Rule affords the administrative and technical safeguards to support minimum necessary uses and disclosures. Administrative safeguards include access authorization in which policies and procedures must describe how access to electronic protected health information may be granted, for example, to a workstation, transaction, program, process, or other mechanism (§164.308(a)(4)(ii)(B)). Technical safeguards require implementation of technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). This requirement for access controls includes a requirement for emergency access procedures, commonly referred to in the industry as "break-the-glass" that enables necessary access in an emergency. In practice, these mechanisms are often accompanied by the means to quickly annotate a rationale for the access and generation of a special audit trail.

Testifiers to NCVHS reported that such technology and others that are not necessarily required by HIPAA but afford stronger security, such as digital signature using X.509 certificate and non-repudiation for person or entity authentication, are technologies available and being used successfully in some implementations.[19] For example, several hospitals recently adopted a "zero-tolerance policy" on confidentiality, including use of computer programs to identify potential cases of inappropriate access, and found significant reduction in employees disciplined for privacy violations.[20] It was also observed, however, that not all covered entities need to deploy stronger technology, and that technology continues to change. The HIPAA Security Rule is risk-based and must remain flexible and scalable to accommodate the needs of a wide variety of covered entities.

5.1 **Recommendation on technical data security management approaches**: HHS should issue guidance to covered entities to promote uses of technical security measures to reduce unauthorized access, and to ensure that their business associates and agents are fully compliant with the HIPAA Security Rule requirements, including authorization, access, authentication, and audit control. This guidance for security management should also be directed to organizations that are not covered entities that maintain and/or transmit personal health information, as well as to vendors of health information technology.

## 6. Observations and Recommendations for Data Stewardship on Data Quality and Integrity

HIT and HIE can aid in comprehensive data collection and sharing, but data integrity, uniformity of definition, and validity must be assured. Just because data are available electronically, does not mean that the data are accurate or are reliably captured or processed. As enhanced uses of health data are enabled by the creation of larger, more

[19] Assaf Halevy, dbMotion, August 23, 2007
[20] Minnesota Facilities Target Unauthorized Employee EHR Access, *Minneapolis Star Tribune*, July 19, 2007.

comprehensive databases, with the potential for linkage of personal health information to acquire longitudinal views, data integrity and quality become essential for meaningful uses of the health data.

> *For example, during hearings on NHIN functional requirements, NCVHS heard testimony describing the multiple ways Hemoglobin A1c may be referenced (e.g., Hb A1c, Hg A1c, A1C,* GHb*) and the issues this causes in managing laboratory processes and reporting results.*

Furthermore, erroneous assumptions about accurate data may be made during aggregation resulting in misinformation.

> *For example, while it is important to know that everyone who is diabetic has had a Hemoglobin A1c measured; it is not accurate to assume that everyone having had a Hemoglobin A1c test is a diabetic.*

There currently are efforts being conducted by the AQA alliance, HQA, and the National Quality Forum (NQF), the Secretary's Quality Alliance Steering Committee (QASC), as well as the American Health Information Community Quality Workgroup to advance the precision and reliability of quality measures. The CMS Better Quality Information Pilots (PQI Project) being conducted in six states and with five health plans are serving as demonstration sites to pioneer the pooling of private data with Medicare claims data to produce more accurate, comprehensive measures of quality of services at the provider level. The Minnesota Community Measurement project and the Blue Health Intelligence (BHI) program are examples underway that have successfully addressed issues of data integrity and quality. The Agency for Healthcare Research and Quality (AHRQ) is also promoting the concept of "value exchange," a multi-stakeholder collaborative of community purchasers, health plans, providers, and consumers to advance the four cornerstones of value-driven health care (interoperable HIT, measure and publish quality information, measure and publish price information, and promote quality and efficiency of care). There are many opportunities to learn lessons from existing, successful initiatives to ensure precise data collection.

6.1 **Recommendation on data quality and data integrity:** HHS data stewardship guidance should address the precision, accuracy, reliability, completeness, and meaning of data used for quality measurement, reporting, and improvement as well as other uses of health data.

## 7. Observations and Recommendations for Data Stewardship on Oversight for Specific Uses of Health Data

NCVHS was asked to consider uses of health data for quality measurement, reporting, and improvement. This effort also identified the need for attention to the distinction between when a use of health data relates to quality measurement, reporting, and improvement and when it relates to research, and which agency's research regulations

apply. Quality assessment activities are defined within HIPAA and cited as permissible uses of protected health information under healthcare operations. Research is also defined within HIPAA, using the definition from The Common Rule. HIPAA permits protected health information to be used in research consistent with The Common Rule, or where those regulations may not apply, in a manner that utilizes oversight provided by a privacy board convened by the healthcare organization. Use of health data for research often requires an informed consent process, where use of health data for quality measurement, reporting, and improvement is permitted under HIPAA without an individual's authorization.

For many uses of health data for quality activities and research activities, there is a clear distinction. However, several testifiers indicated that there are times when the distinction between quality and research activities is not clear. Such lack of clarity in distinguishing between quality and research activities is described further below. It is important to make a distinction between these two activities in order for an organization to comply with the applicable regulations, while still advancing quality and research. NCVHS offers an initial set of recommendations, and will be holding additional hearings to further study this issue.

*Uses of Health Data for Quality Measurement, Reporting, and Improvement within Healthcare Operations:*

NCVHS considered whether there were or should be boundaries around what quality activities are included in HIPAA's definition of healthcare operations and which may be outside of that definition and may call for greater choice by individuals whose data are included.

As identified in the HIPAA definition of quality assessment and improvement activities within healthcare operations, uses of health data for quality activities may be many and varied. The HIPAA Privacy Rule accounts for the fact that many such uses might not have been able to be anticipated at the time of the writing of the Rule. It allows for "related functions that do not include treatment" to be covered under the definition.

In addition, HIPAA defines an organized health care arrangement (OHCA) that supports the sharing of health data for quality assessment purposes. An OHCA is defined in HIPAA as a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; an organized system of health care in which more than one covered entity participates in utilization review, quality assessment, or payment activities; and various configurations of group health plans that share the same sponsor or participants (§160.103).

Several testifiers observed that they had instituted oversight processes to ensure that quality assessment activities were, indeed, those described by HIPAA.

Several recent articles also describe the state of affairs in quality improvement. O'Kane[21] observes that "most management structures do not support integrated quality management" that would enhance accountability for quality, and describes the need for a quality oversight process by a responsible structure accountable to senior management and the governance of the institution for all quality improvement activities.

Testimony was also heard that suggested the desire for a wider role for individuals in deciding whether to permit their health data to be used for quality assessment activities. In a study on authorization bias for a data based research study reported by Harris, 3.2 percent of individuals actively declined participation, while another 17.5 percent did not respond.[22] Dubler and others argue that "if the data are adequately protected to address issues of individual privacy, individual informed consent should, in general, not be required." They also observe that a process of "informed participation," which they define as a process in "which institutions design quality improvement interventions and educate and engage patients about their obligations to help improve quality" will "allow the vast majority of quality improvement projects to go forward without triggering [a research-like informed consent process]."[23]

Having heard the testimony concerning the benefits, protections employed, and potential risks to individuals that may arise from uses of health data for quality measurement, reporting, and improvement, NCVHS believes that enhanced protections for such uses of health data should build upon the protections afforded by the HIPAA Privacy Rule while remaining as part of healthcare operations.

7.1 **Recommendation on protecting data for quality measurement, reporting, and improvement**: HHS should issue guidance to covered entities that health data uses for quality measurement, reporting, and improvement:

7.1.1 **remain within the scope of healthcare operations** when conducted by covered entities or their business associates and their agents, and under the accountability and data stewardship principles inherent in HIPAA. This guidance should clarify and reassure covered entities that there is no need to redefine the HIPAA definition of healthcare operations relative to quality measurement, reporting, and improvement.

7.1.2 **when conducted across covered entities within an organized health care arrangement** as defined by HIPAA, are within the scope of the HIPAA definition of healthcare operations, although the covered entities should assess any heightened risk of potential harm to individuals through such use of HIT and take measures to further protect the data, such as through pseudonymization, as applicable.

[21] O'Kane, Margaret, "Do Patients Need to be Protected from Quality Improvement?" 2007.
[22] Marcelline Harris, PhD, RN, Mayo Clinic, Rochester, MN, Testimony August 2, 2007.
[23] Dubler, Nancy, Jeffrey Blustein, Rohit Bhalla, David Bernard, "Informed Participation: An Alternative Ethical Process for Including Patients in Quality-Improvement Projects," 2007.

7.1.3 **would benefit from a voluntary, proactive oversight process** accountable to senior management and the governance of the institution to ensure there is compliance with HIPAA in uses of health data for quality measurement, reporting, and improvement. Such guidance may draw from the practices that are currently in place today that utilize model governance structures, processes, checklists, and agreements. Where it is determined through a risk/benefit analysis that there is heightened risk to individuals from the quality reporting process, the oversight process should recommend extra precautionary measures to protect the individuals.

*Uses of Health Data for Research*

The Common Rule (codified for HHS at 45 CFR 46, subpart A) defines research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." This is also the definition of research under the Privacy Rule (§164.501). There are several important issues, however, in uses of health data for research:

- *Variations in Interpretation of Research Regulations*: Federally-regulated research studies involving human subjects generally require approval by an institutional review board (IRB) and an informed consent to "opt in" to participating in the research project. NCVHS heard testimony that there is variation in interpretations of regulations addressing human research protections across the HIPAA Privacy Rule, the Common Rule, the FDA regulations (21 CFR 50 and 56), and the VA regulations (38 CFR 16). In addition, the Common Rule does not apply to human subjects' research when not supported by federal funds, or not conducted by an institution that has a Federalwide Assurance (FWA) with the Office for Human Research Protections (OHRP). The FWA is a process in which the institution has voluntarily elected to apply the FWA to all human subjects' research conducted at the institution regardless of the source of support for the research.

  Other gaps and clarification in research definition were also identified, such as surrounding decedent research and research solely using data from electronic health records. Representatives from the OHRP indicated to NCVHS that OHRP was working on clarifying the elements contained in the definition of research and that there is a Trans-HHS Taskforce on Harmonization of Ethical and Legal Policies Related to the Use of Human Specimens and Data in Research (HELPS) composed of representatives from NIH, FDA, OCR, OHRP, CDC, and others focused on harmonizing regulations under the jurisdiction of HHS.

- *Distinguishing Quality Activities from Research*: NCVHS heard from several testifiers in reviewing various reports[24] that quality activities are sometimes difficult to distinguish from research, and that some quality activities may evolve into research studies. It was observed that the "line between quality improvement and clinical research is relatively permeable, and it is sometimes difficult to determine with precision whether a project should be considered quality improvement or research, especially when a quality study may utilize techniques of randomization and prospective intervention with the support of electronic databases."[25] Testimony to NCVHS described a full spectrum of how organizations addressed quality/research overlaps, from requesting annual IRB review of quality studies (e.g., the Northern New England Cardiovascular Disease Study Group), using a decision tree framework to guide internal activities in determining when an activity is not research (e.g., the Center for Health Studies at Group Health Cooperative), to considering any study with intent to publish research (e.g., Mayo Clinic).

Good quality improvement activities share important characteristics with research, especially with respect to their ethical underpinnings. Lumpkin observes that basic principles of biomedical ethics, including respect for autonomy, beneficence, non-maleficence, and justice relate to all aspects of HIPAA TPO, and equally in quality, public health, and research uses of health data.[26]

As the Nation seeks value-driven health care, clarifying research regulations and distinctions between quality activities and research is critical.

7.2 **Recommendation on harmonizing research regulations**: HHS should promote harmonization of research regulations within HHS and with other Departments that oversee regulations on human research protections to ensure consistent privacy and human subject protection for all research efforts.

7.3 **Recommendation for quality/research overlap guidance:** HHS should encourage the Office for Human Research Protections (OHRP) in compiling its clarifying work on the research definition to continue to work collaboratively with the Office of Civil Rights (OCR) and to leverage the tools starting to be used in the industry to aid in distinguishing how requirements apply to uses of health data for quality and research, especially as questions relating to distinctions between research and quality uses of health data under the HIPAA healthcare operations definition arise.

---

[24] Jennings, B, et al. eds. *Health Care Quality Improvement: Ethical and Regulatory Issues*, reference works compiled by The Hastings Center under a grant from the Agency for Healthcare Research and Quality, 2007.
[25] E. Bellin and N.N. Dubler, "The Quality Improvement-Research Divide and the Need for External Oversight," *American Journal of Public Health*, 91(9)(2001): 1512-17.
[26] Lumpkin, John R., MD, MPH, Robert Wood Johnson Foundation, Testimony on August 1, 2007.

7.4 **Recommendation for wide dissemination of quality/research overlap guidance:** HHS should encourage the Office of Human Research Protections (OHRP) in compiling its clarifying work on the definition of research to widely disseminate the results. Limiting such dissemination only to the research community can limit its usefulness for providers, payers, and others who may not consider themselves researchers, but who may become engaged in quality work that ultimately falls within the scope of research on human subjects.

7.5 **Recommendation for means to transition quality activities into research when appropriate**: HHS should foster the collaborative efforts between OHRP and OCR to identify approaches to ensure that when a quality study becomes generalizable and evolves into research, that HIPAA Privacy and IRB requirements are respected.

7.6 **Recommendation on further investigation into uses of health data for research:** NCVHS identified certain areas that require further investigation, such as research based solely on data from electronic health records, and decedent research. It also heard the potential value for a common oversight of quality and research within an organization. NCVHS will take the lead in working with OHRP and other federal agencies to further study these areas and make recommendations as appropriate.

## 8. Observations and Recommendations on Transitioning to a NHIN

NCVHS observes that many uses of health data contemplated to be supported by a NHIN are being made today in the context of point-to-point communications, often between covered entities, their business associates and agents, and with individual recipients of care delivery services. At this time, a definition of a NHIN and how it will be used has not reached sufficient maturity to dictate how individual choice over uses of health data within a NHIN should or could be exercised.

The NCVHS Privacy Letter of June 22, 2006 observes that providers should have the right to maintain health data they compile about individuals in any medium. It notes, however, that it may be appropriate to permit individuals to opt into or out of certain uses of health data. For example, it may be suitable for individuals to opt out of direct disease management interventions by health plans. Testimony was heard from a health information exchange in which individuals were asked to opt into contributing data to a provider-oriented outcomes analysis and benchmarking data warehouse. They found that a high percentage (94 percent) of individuals opted in, with variation by specialty of providers.[27]

Testimony identified a number of new and innovative approaches to manage the way an individual could provide authorization for uses and disclosures of personal health

[27] Micky Tripathi, PhD, MPP, Massachusetts eHealth Collaborative, Testimony, August 23, 2007.

information. These include health record banking models, consent metadata, and federated consent registries. While these technologies are new and require testing, they may provide a suitable way for an authorization to follow data.

8.1 **Recommendation on adoption of data stewardship within a NHIN**: HHS should continue to pursue further definition of a NHIN and its uses, and concurrently study how to balance the benefits of health data uses as development of a NHIN progresses with the concerns expressed about potential for harms. Trial implementations and other federally-sponsored demonstrations should include:

8.1.1 **evaluation of the impact of applying enhanced data stewardship,** including how the glossary of terms may have helped inform the application of appropriate data stewardship for various uses of health data, especially as more comprehensive databases may be compiled by organizations that are not HIPAA covered entities that are spawned by a NHIN.

8.1.2 **evaluation of ways to manage individuals' authorizations**: HHS should include in its NHIN trial implementations and other federally-sponsored demonstrations the evaluation of how new technologies that have a track record of success in other settings may afford the ability for individuals to provide authorization for uses of their protected health information. The evaluation of such techniques should include determining to what data sharing scenarios an authorization would provide optimal protection while assuring the benefits of health data uses.

8.1.3 **evaluation of new methods or techniques to de-identify health data** to determine their effectiveness to protect identity and not enable re-identification when not intended.

8.1.4 **evaluation of and continued maturity of chain of trust mechanisms** to determine the impact on business associate relationships and ensure transparency between covered entities and business associates and their agents.

8.1.5 **evaluation of educational modalities** to determine the most effective messages and media for various target audiences.

8.1.6 **evaluation of appropriate safeguards needed to ensure that there is no unintended harm to individuals as de-identified data may be sold to support** the possible business models of a NHIN.

## 9. Observations and Recommendations on Additional Privacy Protections

Testimony indicates that there is a continuum of users of health data – from those with a close nexus with the delivery of care for the individual (i.e., individual care recipients, providers, and payers) to those that are very far removed from the individual-provider-payer relationship (e.g., data mining organizations that track health-related web sites). Testimony also identified that, while the HIPAA Privacy and Security regulations address protections as health data are used close to the nexus of care delivery, the farther removed from care delivery, the less protection, if any, is afforded. The lack of adequate protections across all uses of health data can result in serious harms to individuals and ultimately the quality of health and health care in the Nation.

NCVHS has previously made several sets of recommendations setting the broad context for privacy improvement, including that privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. States are already beginning to enact laws intended to broaden protections.

> *For example, California AB 1298, which goes into effect January 1, 2008, adds to the class of covered entities under California's Confidentiality of Medical Information Act "any business organized for the purpose of maintaining medical information in order to make the information available to an individual or a provider for purposes of allowing the individual to manage his or her health information, or for the diagnosis or treatment of the individual." This would include businesses that maintain PHRs. It also amends the State's consumer notification law requiring the owner or licensee of computerized personal information to provide notice of a breach of security of the data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.*

Finally, there is the need to address variations in state laws with respect to privacy. While it is important to identify best practices and states may be in the best position to test various practices, disparate laws across states make it costly and difficult for covered entities to comply with all nuances of the laws when data are exchanged across state boundaries. Just as technical interoperability is necessary in a NHIN, privacy law interoperability is needed as well.

9.1 **Recommendation on additional federal privacy legislation**: HHS should work with other federal agencies and the Congress:

9.1.1 **for more inclusive, federal privacy legislation** so that all individuals and organizations that use and disclose individually identifiable health information are covered by the data stewardship principles inherent in such legislation, including a range of organizations not currently covered by HIPAA. Reference NCVHS *Recommendations Regarding Privacy and*

*Confidentiality in the Nationwide Health Information Network* sent to the Secretary of HHS on June 22, 2006.

9.1.2 **on expanding the definition of covered entity under HIPAA**: *In the absence of comprehensive privacy legislation,* HHS should address the need for more limited legislation that expands the definition of covered entity under HIPAA from its focus on financial and administrative transactions to cover other organizations that manage, collect, view, store, share, disclose, or otherwise make use of personal health information. At a minimum, such organizations should include suppliers of personal health record systems that are not covered entities. Other examples may include health risk assessment suppliers and personal health trainers. Such legislation should not inadvertently weaken existing privacy protections. For example, some commenters expressed concern that organizations today that primarily obtain aggregated data, such as employer sponsors of health plans, not be included in the definition of covered entity, thus potentially enabling them to have access to more personal health information than they currently have.

9.2 **Recommendation on anti-discrimination legislation/regulation**: HHS should work with other federal agencies and the Congress for legislative or regulatory measures designed to eliminate or reduce as much as possible the potential discriminatory effects of misuse of health data (for additional information, see also NCVHS Privacy Letter, June 22, 2006).

9.3 **Recommendation on state data restriction laws**: HHS should support the work of the Health Information Security and Privacy Collaboration (HISPC) that would guide harmonization among state laws where applicable and pinpoint where states have made explicit differences. HHS should support a state law mapping repository that clarifies where states differ and which aspects of state laws are more stringent than HIPAA.

# Appendix A: NCVHS Members

**CHAIR**
Simon P. Cohn, M.D., M.P.H.
Associate Executive Director
The Permanente Federation
Kaiser Permanente
Oakland, California

**HHS EXECUTIVE STAFF DIRECTOR**
James Scanlon
Deputy Assistant Secretary
Office of Science and Data Policy
Office of the Assistant Secretary
for Planning and Evaluation, DHHS
Washington, DC

**EXECUTIVE SECRETARY**
Marjorie S. Greenberg
Chief, Classifications and Public Health Data
Standards Staff
Office of the Director
National Center for Health Statistics, CDC
Hyattsville, MD

**MEMBERSHIP**

Jeffrey S. Blair, M.B.A.
Director of Health Informatics
Lovelace Clinic Foundation
Albuquerque, NM

Justine M. Carr, M.D.
Senior Director
Clinical Resource Management
Beth Israel Deaconess Medical Center
Boston, MA

Leslie Pickering Francis, J.D., Ph.D.
Chairman, Department of Philosophy
Alfred C. Emery Professor of Law
University of Utah
Salt Lake City, UT

Larry Green, M.D.
University of Colorado
Health Science Center
Aurora, CO

John P. Houston, J.D.
Vice President, Privacy & Information Security
Assistant Counsel & Adjunct Professor
Professor of Biomedical Informatics
University of Pittsburgh School of Medicine
Pittsburgh, PA

Garland Land, M.P.H.
Executive Director
National Association for Public Health
Statistics
and Information Systems
Silver Spring, MD

Carol J. McCall, F.S.A., M.A.A.A.
Vice President
Humana
Center for Health Metrics
Louisville , KY

J. Marc Overhage, M.D., Ph.D.
President and CEO,
Indiana Health Information Exchange
Associate Professor, Indiana University
School of Medicine
Senior Research Scientist,

Regenstrief Institute, Inc.
Indianapolis, IN

Harry Reynolds
Vice President
Blue Cross Blue Shield of North Carolina
Durham, NC

Mark A. Rothstein, J.D.
Herbert F. Boehl Chair of Law and Medicine
Director, Institute for Bioethics, Health Policy and Law
University of Louisville School of Medicine
Louisville, KY

William J. Scanlon, Ph.D.
Health Policy R&D
Washington , DC

Donald M. Steinwachs, Ph.D.
Professor and Director
The Johns Hopkins University
Bloomberg School of Public Health
Department of Health Policy and Management
Health Services Research and Development Center
Baltimore, MD

C. Eugene Steuerle, Ph.D.
Senior Fellow
The Urban Institute
Washington, D.C.

Paul Tang, M.D.
Chief Medical Information Officer
Palo Alto Medical Foundation
Palo Alto, CA

Kevin C. Vigilante, M.D., M.P.H.
Principal
Booz Allen Hamilton
Rockville, MD

Judith Warren, Ph.D., RN
Associate Professor
School of Nursing
University of Kansas
Kansas City, KS

**LIAISON REPRESENTATIVES**

J. Michael Fitzmaurice, Ph.D.
Senior Science Advisor for Information Technology
Agency for Healthcare Research and Quality
Rockville, MD

Edward J. Sondik, Ph.D.
Director
National Center for Health Statistics
Hyattsville, Maryland

Steven J. Steindel , Ph.D.
Senior Advisor
Standards and Vocabulary Resource
Information Resources Management Office
Centers for Disease Control and Prevention
Atlanta, GA

Karen Trudel
Director, HIPAA Project Staff
Office of Operations Management
Centers for Medicare and Medicaid Services
Baltimore, MD

**Staff of the Centers for Disease Control and Prevention, National Center for Health Statistics**

Debbie Jackson
Katherine Jones
Marietta Squire
Cynthia Sydney

**NCVHS Ad Hoc Work Group on Secondary Uses of Health Data**

Simon P. Cohn, M.D., M.P.H., Chair
Justine M. Carr, M.D., Co-Vice Chair
Harry Reynolds, Co-Vice Chair
J. Marc Overhage, M.D., Ph.D.
Mark A. Rothstein, J.D.
William J. Scanlon, Ph.D.
Paul Tang, M.D.
Kevin C. Vigilante, M.D., M.P.H.

**Work Group Staff**

Kelly Cronin, HHS, Office of the National Coordinator for Health Information Technology
Mary Jo Deering, Ph.D., HHS National Institutes of Health, National Cancer Institute
J. Michael Fitzmaurice, Ph.D., Agency for Healthcare Research and Quality
Morris A. Landau, J.D., M.H.A., L.L.M., HHS, Office of the National Coordinator for Health Information Technology
John Loonsk, M.D., Office of the National Coordinator for Health Information Technology
Steven J. Steindel, Ph.D., HHS Centers for Disease Control and Prevention

**Consultants Under Contract to ONC**

Erin Grant, Booz Allen Hamilton
Kristine Martin-Anderson, Booz Allen Hamilton

**Consultant Writer**

Margret Amatayakul, MBA, RHIA, CHPS, CPEHR, FHIMSS, Margret\A Consulting, LLC

# Appendix B: Testifiers and Commenters on Uses of Health Data

Karen Adams, Ph.D., National Quality Forum

Elisabeth Belmont, Esq., MaineHealth

Sue A. Blevins, Institute for Health Freedom

Meryl Bloomrosen, M.B.A., RHIA, American Medical Informatics Association

Carmella Bocchino, America's Health Insurance Plans

Cindy Brach, Agency for Healthcare Research and Quality, HHS

William Braithwaite, M.D., Ph.D., Health Information Policy Consulting

David Carlisle, M.D., California Office of Statewide Health Planning and Development

Jean Chenoweth, Thomson Healthcare

Denise Childress, National Business Group on Health

Deborah Collyar, Group Health Cooperative

Jodi G. Daniel, J.D., M.P.H., Office of the National Coordinator for Health Information Technology, HHS

Carol Diamond, M.D., M.P.H., Markle Foundation

Richard S. Dick, Ph.D., You Take Control

Howard Dickler, M.D., Association of American Medical Colleges

Linda L. Dimitropoulos, Ph.D., RTI International

Marchelle Djordjevic, American College of Surgeons

Floyd Eisenberg, M.D., M.P.H., Siemens Medical Solutions Health Services

Lynn Etheredge, George Washington University

Kristin Fitzgerald, Confidentiality Coalition

Sean Flynn, Legal Consultant to the Prescription Project

John P. Glaser, Ph.D., AHIC Personalized Health Care Work Group

Jonathan Gold, M.D., MHA, MSC, McKesson Provider Technologies

Leon Goldman, M.D., Beth Israel Deaconess Medical Center

Joel W. Goldwein, M.D., Elekta, Inc.

Tina Olson Grande, Healthcare Leadership Council

Margaret Gunter, Ph.D., RN, HMO Research Network and Lovelace Clinic Foundation/NM RHIO

John Halamka, M.D., CareGroup Health System and Harvard Medical School; Health Information Technology Standards Panel

Assaf Halevy, dbMotion, Inc.

Doug Henley, AHIC Personalized Health Care Workgroup

Marcelline R. Harris, Ph.D., RN, Mayo Clinic

Vicki Hohner, M.B.A., Fox Systems, Inc.

Gail Horlick, M.S.W., J.D., Office of Scientific Regulatory Services, Centers for Disease Control and Prevention

Monica Jones, The Information Centre for Health and Social Care, UK

Julie Kaneshiro, Office for Human Research Protection, HHS

Susan Kleimann, Ph.D., Kleimann Consulting Group

Steven E. Labkoff, M.D., FACP, Pfizer Healthcare Informatics

Shirley S. Lady, Blue Cross Blue Shield Association

Leslie Lenert, M.D., Centers for Disease Control and Prevention

Marilyn Zigmund Luke, America's Health Insurance Plans

John R. Lumpkin, M.D., MPH, Robert Wood Johnson Foundation

Jennifer P. Lundblad, Ph.D., M.B.A., Stratis Health

Janet Marchibroda, eHealth Initiative

Glen Marshall, Siemens Medical Solutions

Sue McAndrew, Office for Civil Rights, HHS

Clement McDonald, M.D., NLM, National Institutes of Health

Sandra L. Meicher, PhD, Mental Health Association of MN

Julie Murchinson, Manatt Health Solutions

Sharyl J. Nass, Ph.D., Institute of Medicine Privacy Committee

William C. Nugent, M.D., Dartmouth-Hitchcock Medical Center, Northern New England Cardiovascular Disease Study Project

William J. O'Byrne, New Jersey e-HIT

Margaret O'Kane, National Committee on Quality Assurance

Jason D. Ormsby, PhD, MBA, MHSA, The Joint Commission

Wendy E. Patterson, Esq., National Cancer Institute

Deborah Peel, M.D., Patient Privacy Rights Foundation

Kevin Peterson, M.D., M.P.H., University of Minnesota School of Medicine

Steven Posnack, M.H.S., M.S., Office of the National Coordinator for Health IT

James C. Pyles, American Psychoanalytic Association

Mike Rapp, Centers for Medicare & Medicaid Services

Lori Reed-Fourquet, *e-HealthSign,* LLC

Peter M. Sandman, Ph.D., Risk Communication Consultant

John Santa, MD, The Prescription Project

Barbara Siegel, M.S., RHIT, American Health Information Management Association

Jenifer Simpson, American Association of People with Disabilities

Joel Slackman, Blue Cross Blue Shield Association

Sharon L. Sprenger, RHIA, CPHQ, MPA, The Joint Commission

Latanya Sweeney, Ph.D., Carnegie-Mellon University

Sharon F. Terry, M.A., Genetic Alliance

Jeanette Thornton, America's Health Insurance Plans

Micky Tripathi, Ph.D., MPP, Massachusetts eHealth Collaborative

Emily Welebob, R.N., M.S., Indiana Health Information Exchange, Inc.

P. Jon White, M.D., Agency for Healthcare Research and Quality

Steven Wojcik, National Business Group on Health

William A. Yasnoff, M.D., Ph.D., Health Record Banking Alliance

Scott Young, M.D., Kaiser Permanente

# Appendix C: Glossary of Terms

This glossary of terms identifies and defines terms used by testifiers (and in collateral documents) in discussion of uses of health data. Its purpose is to provide guidance to the reader of this report as well as to inform the development of its recommendations. The structure of the Glossary of Terms is generally consistent with the "Secondary Uses and Re-uses of Healthcare Data: Taxonomy for Policy Formulation and Planning" (a.k.a., AMIA Taxonomy) developed by the American Medical Informatics Association (AMIA). However, there are both similarities and differences between the two documents that are important to note:

- The NCVHS Glossary of Terms is intended to inform the recommendations included herein and to help provide guidance in determining suitable data stewardship approaches for various uses of health data by the organization having jurisdiction over the use.

- AMIA states that its Taxonomy is intended to be used as a "resource in developing plans and policies related to secondary uses of healthcare data." The AMIA Taxonomy provides a categorization of health data uses that could be described by various attributes and therefore relate policy statements to the particular use.

- The NCVHS Glossary of Terms includes annotated definitions to guide the reader of the report as well as to promote adoption of standard terminology associated with uses of health data.

**Terms**

Terms Used to Describe Status of Information

**Health information**, as defined by HIPAA Privacy/Security/Enforcement regulations: "any information, whether oral or recorded in any form or medium, that: (1) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (2) 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." (45 CFR §160.103)

**Individually identifiable health information** (IIHI), as defined by HIPAA Privacy/Security/Enforcement regulations: "a subset of health information, including demographic information collected from an individual and: (1) is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (2) relates to the . . . health of an individual, provision of health care to an individual, or . . . payment for the provision of health care to the individual; and (3) that identifies the

individual; or (4) with respect to which there is a reasonable basis to believe the information can be used to identify the individual." (45 CFR §160.103)

**Protected health information** (PHI), as defined by HIPAA Privacy/Security/Enforcement regulations: "individually identifiable health information … that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium" by an entity covered under HIPAA (i.e., health plans, clearinghouses, and providers that transmit any health information in electronic form in connection with a transaction covered by the Administrative Simplification provisions of HIPAA). Education records covered by the Family Educational Rights and Privacy Act (FERPA) and employment records held by a covered entity in its role as employer are not included in the definition of protected health information. (45 CFR §160.103)

**Personal health information**, as used in this report, is any individually identifiable information relating to the health, provision of health care, payment for healthcare, or other related health information created by any individual or organization, irrespective of HIPAA covered entity status.

*This report makes no distinction between* information *and* data *with respect to the use of these terms.*

Terms Used to Describe Oversight of Health Data

**Covered entity**, as defined by HIPAA Privacy/Security/Enforcement regulations: "a health plan; healthcare clearinghouse; a healthcare provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA." (45 CFR §160.103)

**Healthcare clearinghouse**, as defined by HIPAA Privacy/Security/Enforcement regulations: "a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and 'value-added' networks and switches, that does either of the following functions: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity." (45 CFR §160.103)

**Organized health care arrangement** (OHCA), as defined by HIPAA Privacy/Security/Enforcement regulations: "(1) a clinically integrated care setting in which individuals typically receive health care from more than one healthcare provider; (2) an organized system of health care in which more than one covered entity participates and in which the participating covered entities: (i) hold themselves out to the

public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (A) utilization review . . . , (B) quality assessment and improvement activities . . . , or (C) payment activities, if the financial risk for delivering health care is shared . . . ; (3) a group health plan and a health insurance issuer or HMO . . . ; (4) a group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or (5) the group health plans in (4) and health insurance issuers or HMOs . . .with respect to protected health information . . . that relates to individuals who are or have been participants or beneficiaries in any of such group health plans." (45 CFR §160.103)

**Business associate**, as defined by HIPAA Privacy/Security/Enforcement regulations: "a person who on behalf of a covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) a function . . . involving the use or disclosure of individually identifiable health information . . . ; or (B) any other function or activity regulated by [HIPAA Administrative Simplification]; or provides . . . legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services . . . where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." (45 CFR §160.103)

**Business associate contract**, as defined by HIPAA's Privacy and Security Rules: a written contract or other written agreement or arrangement between the covered entity and the business associate documenting satisfactory assurances for compliance with the implementation specifications of business associate contracts, including ensuring that any agents, including a subcontractor, to whom the business associate provides protected health information agrees to the same restrictions and conditions that apply to the business associate. (54 CFR §164.308(b), §164.314, §164.502(e), §164.504(e))

**Chain of trust** is a concept that ensures that a uniform level of security is applied at every "link" in the chain where information passes from one party to another. Steve Fox, Esq., of Pepper Hamilton LLP, observes that verification of uniformity at each link is necessary for optimal protection of transmitted data, and that a "chain of trust" agreement is a proxy for actual physical confirmation before and after each and every transmittal.

**Institutional Review Board** (IRB), as defined in the Protection of Human Subjects regulation (a.k.a. the Common Rule): is an administrative body, subject to membership requirements specified in the Common Rule, that provides oversight for "all research involving human subjects conducted, supported, or otherwise subject to regulation by any federal department or agency which takes appropriate administrative action to make the policy applicable to such research." (45 CFR §46.101)

**Privacy board**, as defined by HIPAA Privacy Rule: a group whose members have "varying backgrounds and appropriate professional competency as necessary to review the effect of [a] research protocol on [an] individual's privacy rights and related interests; includ[ing] at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and does not have any member participating in a review of any project in which the member has a conflict of interest. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research provided that . . . the covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization . . . has been approved by either an Institutional Review Board . . .; or a privacy board. . ." (45 CFR §164.512(i))

**Data use agreement**, as defined by HIPAA Privacy Rule: an agreement between a covered entity and the recipient of a limited data set that establishes the permitted uses and disclosures of the limited data set. (45 CFR §164.512(e))

**Data stewardship**, as defined by the American Medical Informatics Association: "encompasses the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information." Further, AMIA notes that "principles of data stewardship apply to all the personnel, systems, and processes engaging in health information storage and exchange within and across organizations."

**Organization**, as used in this report and as distinguished from HIPAA covered entity, refers to any person or body that may maintain or transmit personal health information.

Terms Used to Describe Identity Protection (of Individual Patient/Clinician; Entity)

**De-Identification of protected health information**, as defined by HIPAA Privacy Rule: "health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information." Requirements for de-identification include (1) **statistical method**: use of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable by a person with appropriate knowledge and experience; determining that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documents the methods and results of the analysis that justify such determination; or (2) **safe harbor method**: where specific identifiers of the individual or of relatives, employers, or household members of the individual, are removed, including 17 specific elements plus any other unique identifying number, characteristic, or code except as permitted for re-identification by the covered entity. **Re-identification** of de-identified data is permitted by the covered entity so long as the means of identification is not derived from or related to the information and the covered entity does not use or

disclose the code or any other purpose and does not disclose the mechanism for re-identification. (45 CFR §164.514(a),(b), and (c))

**Limited Data Set**, as defined by HIPAA Privacy Rule: protected health information that excludes all direct identifiers of the individual or of relatives, employers, or household members of the individual as defined in HIPAA's Privacy Rule's definition of de-identification, *except* city, State, and zip code; all elements of dates related to the individual; and any other unique identifying number, characteristic, or code not included in the HIPAA definition of de-identification. (45 CFR §164.514(e))

**Anonymization**, as submitted to the Health Information Technology Standards Panel (HITSP) by the Population Health Technical Committee upon the recommendation of the American Health Information Community (AHIC) Biosurveillance Data Steering Committee (May 11, 2007): a process of "removal and aggregation requirements for data variables [i.e., protected health information] submitted to a biosurveillance information system (BIS) [in accordance with the HIPAA Privacy Rule 45 CFR §164.519(b) that permits a covered entity to use or disclose protected health information when required by law] where some demographic data elements of interest [ordinarily removed under the HIPAA definition of de-identification] need to be retained in order to accurately evaluate the data to detect potential threats to public health."

**Pseudonymization**, as submitted to the Health Information Technology Standards Panel (HITSP) by the Population Health Technical Committee upon the recommendation of the American Health Information Community (AHIC) Biosurveillance Data Steering Committee (May 11, 2007): "a particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms." Also, "the process of supplying an alternative identifier that permits a patient to be referred to by a key that suppresses his/her actual identification information." A public health agency may use "pseudonymization through [a] trusted third party [to] support re-identification, . . . such as for verification and validation of data integrity, checking for suspected duplicate records, enabling requests for additional data, linking to supplement research information variable, compliance audit, informing data subject of significant findings, facilitate follow-up research, and law enforcement."

**Data aggregation**, as defined by HIPAA Privacy rule: "with respect to protected health information created or received by a business associate . . . [is] the combining of such protected health information . . . with the protected health information . . . of another covered entity, to permit data analyses that relate to the healthcare operations of the respective covered entities." (45 CFR §164.501) A common statistical definition of data aggregation is "any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis." (Data Warehouse Institute, May 2005, www.tdwi.org/Publications/WhatWorks accessed 11/4/07)

Terms Used to Describe Permission to Access/Use/Disclose

**Authorization**, as used in HIPAA Privacy Rule at 45 CFR §164.508: "Except as otherwise permitted or required . . . a covered entity may not use or disclose protected health information without an authorization that is valid under the [specifications within the Rule, including signature of individual or personal representative];" and the use or disclosure must be consistent with the limitations of the authorization. The HIPAA Privacy Rule also describes uses and disclosures requiring an opportunity for the individual to agree or to object relative to use and disclosure for facility directories and for involvement in the individual's care and notification purposes (45 CFR §164.510); and uses and disclosures for which an authorization or opportunity to agree or object is not required (45 CFR §164.512), such as when required by law, for public health purposes, for health oversight activities, etc.

**Authorization**, as used in HIPAA Security Rule at 45 CFR §164.308(4): "policies and procedures for [granting] access to electronic protected health information that are consistent with the applicable requirements of [the Privacy Rule]."

**Consent**, as used in HIPAA Privacy Rule at 45 CFR §164.506(b): "A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or healthcare operations. Consent . . . shall not be effective to permit a use or disclosure of protected health information when an authorization . . .is required or when another condition must be met for such use or disclosure to be permissible." This section further describes that a covered entity may disclose protected health information (1) for its own treatment, payment, or healthcare operations; (2) for treatment activities of a healthcare provider; (3) to another covered entity or a healthcare provider for the payment activities of the entity that receives the information; (4) to another covered entity for healthcare operations activities of the entity if each entity has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is for [treatment, payment, or healthcare operations] or for the purpose of healthcare fraud and abuse detection or compliance; (5) to other covered entities within an organized healthcare arrangement (OHCA) for any healthcare operations of the OHCA.

**Informed consent for research**, as used in the Common Rule at 45 CFR §46.116: "Except as provided elsewhere in this policy, no investigator may involve a human being as a subject in research covered by this policy unless the investigator has obtained the legally effective informed consent of the subject or the subject's legally authorized representative." Basic elements of informed consent are described as including a statement that the study involves research; statement of its purpose; expected duration; description of procedures to be followed, including those that are experimental; description of risks and benefits; appropriate alternative procedures or courses of treatment; confidentiality of records identifying the subject; explanation as to any compensation; whether any medical treatments are available if injury occurs; and whom to contact for answers to questions about the research.

**Informed consent for medical interventions**, as described by the American Medical Association (May 2007), Office of the General Counsel: "a process of communication between a patient and physician that results in the patient's authorization or agreement to undergo a specific medical intervention." The AMA observes that in the communications process, the physician providing or performing the treatment and/or procedure (not a delegated representative), should disclose and discuss with the patient: the patient's diagnosis, if known; the nature and purpose of a proposed treatment or procedure; the risks and benefits of a proposed treatment or procedure, alternatives (regardless of their cost or the extent to which the treatment options are covered by health insurance); the risks and benefits of the alternative treatment or procedure; and the risks and benefits of not receiving or undergoing a treatment or procedure. In turn, the patient should have an opportunity to ask questions to elicit a better understanding of the treatment or procedure, so that he or she can make an informed decision to proceed or to refuse a particular course of medical intervention.

**Opt in** and **Opt out**: These terms derive largely from email marketing, and have been codified in the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 that applies to all organizations that send out marketing by telephone, fax, automated calling system, email, SMS, MMS, or any other form of electronic communication. There appears to be no similar legislation or regulation in the U.S. The closest legislation appears to be related to wireless location privacy. The HIPAA Privacy Rule Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object (45 CFR §164.510) relates only to facility directories and involvement in the individual's care and notification purposes. The HIPAA Privacy Rule also includes Rights to Request Privacy Protection for Protected Health Information (45 CFR §164.522) in which the individual has the right to request restriction of uses and disclosures and for confidential communications. Neither of these requirements address opt in nor opt out as described more fully in the context of email marketing:

> **Opt in**: requires an action or affirmation by an individual for inclusion; the default is exclusion
>
> **Opt out**: requires an action or affirmation for exclusion; the default is inclusion.

**Consent management**, as submitted to the Health Information Technology Standards Panel (HITSP) by the Security and Privacy Technical Committee (October 15, 2007) on Manage Consent Directive Transaction Package: "describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent." It is noted that the "registry that manages the consents may very well be different from the registry which manages the clinical documents [i.e., federated consent management]." It is described that "a consent directive is a record of a healthcare consumer's privacy policy, which is in accordance with governing

jurisdictional and organization privacy policies that grant or withhold consent: to one or more identified entities in a defined role; to perform one or more operations (e.g., collect, access, use, disclose, amend, or delete); on an instance or type of IIHI; for a purpose such as treatment, payment, operations, research, public health, quality measures, health status evaluation by third parties, or marketing; under certain conditions, e.g., when unconscious; for specified time period, e.g., effective and expiration dates; in certain context, e.g., in an emergency."

Terms Used to Describe Uses of Data

**Permitted uses and disclosures**, as defined by HIPAA Privacy Rule: "a covered entity is permitted to use or disclose protected health information . . . to the individual; for treatment, payment, or healthcare operations . . . ; incident to a use or disclosure otherwise permitted or required . . ., provided that the covered entity has complied with the applicable requirements of [minimum necessary] and [administrative, physical, and technical safeguards to protect privacy]; pursuant to and in compliance with an authorization . . .; pursuant to an agreement under, or as otherwise permitted by [the requirement for the individual to be given an opportunity to agree or object to a use or disclosure]; as permitted by and in compliance with [uses and disclosures for which an authorization or opportunity to agree or object is not required]." (45 CFR §164.502)

**Required uses and disclosures**, as defined by HIPAA Privacy Rule: "a covered entity is required to disclose protected health information (i) to an individual when requested and as required by [right of access and accounting of disclosures]; and (ii) when required by the Secretary . . . to investigate or determine the covered entity's compliance . . . "(45 CFR §164.502)

**Healthcare operations**, as defined by HIPAA Privacy Rule: "any of the following activities of the covered entity to the extent that the activities are related to covered functions: (1) conducting quality assessment and improvement activities . . . ; (2) reviewing the competence or qualifications of healthcare professionals . . .; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits . . .; (4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development . . .; and (6) business management and general administrative activities of the entity . . ." (45 CFR §164.501)

**Quality assessment and improvement activities**, as defined by HIPAA Privacy Rule: "outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment." (45 CFR §164.501)

**Research**, as defined by HIPAA Privacy Rule: "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." (45 CFR §164.501) This definition is the same as that at 45 CFR 46, Protection of Human Subjects (a.k.a. the Common Rule).

**Public health authority**, as defined by HIPAA Privacy Rule: "an agency or authority of the United States, a State, a territory, . . . that is responsible for public health matters as part of its official mandate." (45 CFR §164.501)

**Primary uses** (of Patient Records), as used in the Institute of Medicine, *The Computer-based Patient Record: An Essential Technology for Health Care* (Washington, DC: National Academy Press, 1991) p. 33, "are associated with the provision of patient care, that is, with providing, consuming, managing, reviewing, supporting, and charging and reimbursing patient care services. *NCVHS recommends against distinguishing between primary and secondary uses of health data.*

**Secondary uses** (of Patient Records), as used in the Institute of Medicine, *The Computer-based Patient Record: An Essential Technology for Health Care* (Washington, DC: National Academy Press, 1991), p. 33-34, "are not considered necessary for a particular encounter between a patient and a health care professional, but such uses influence the environment in which patient care is provided. Education, research and development, regulation, and policymaking are all considered secondary uses of the patient record." *NCVHS recommends against distinguishing between primary and secondary uses of health data.*

Terms Used to Describe Transparency

**Transparency**, as used in the humanities: implies openness, communication, and accountability. On August 22, 2006, President Bush issued an Executive Order "Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs," directing Federal agencies to increase transparency in pricing, increase transparency in quality, encourage adoption of health information technology standards to facilitate the rapid exchange of health information, and provide options that promote quality and efficiency in health care. (Fact Sheet: Health Care Transparency: Empowering Consumers to save on Quality Care, August 22, 2006)

**HIPAA Notice of Privacy Practices** (NPP), as required by the HIPAA Privacy Rule (45 CFR §164.520): a notice, required to be written in plain language, containing specific information about uses and disclosures of protected health information that may be made by the covered entity and of the individual's rights and the covered entity's legal duties with respect to protected health information. Except in an emergency treatment situation, the covered entity is to make a good faith effort to obtain a written acknowledgment of receipt of the notice, and if not obtained, document its good faith efforts and the reason why the acknowledgment was not obtained. It is noted that the

NPP is often mistakenly referred to as "HIPAA consent," where it is *not* intended to be either a consent or authorization form to obtain an individual's permission for uses and disclosures of protected health information.

**Privacy Policy**, with respect to websites, is a notice regarding privacy issues and choice on how personal information is used. Under the Federal Trade Commission Act, the Commission "guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information." Under the Gramm-Leach-Bliley Act, the Commission has implemented rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information, and it aggressively enforces against pretexting [use of false pretenses]. The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act. (www.ftc.gov/privacy/ accessed 11/20/07)

Terms Used to Describe Exchange of Health Information

**Health information exchange** (HIE), as defined by the Office of the National Coordinator for Health Information Technology (June 21, 2007), is "an entity that enables the movement of health related data among entities within a state, a region, or a non-jurisdictional participant group."

**Nationwide health information network** (NHIN), as defined by the Office of the National Coordinator for Health Information Technology (June 21, 2007), is "a 'network of networks' [that] securely connects consumers, providers, and others who have or use health-related data." Working assumptions also include that a NHIN will have "no national data store or centralized systems at the national level, no national patient identifier, [but will have] shared architecture (standards, services, and requirements), processes, and procedures."

**NHIN health information exchange** (NHIE), as defined by the Office of the National Coordinator for Health Information Technology (June 21, 2007), is "an HIE that implements the NHIN architecture, processes, and procedures and participates in the NHIN Cooperative."

**Health information service provider** (HSP), as defined by the Office of the National Coordinator for Health Information Technology (June 21, 2007), is "a company or other organization that supports one or more HIEs by providing them with operational and technical health exchange services."

**National health information infrastructure** (NHII), as envisioned by the National Committee on Vital and Health Statistics in *Information for Health: A Strategy for Building the National Health Information Infrastructure*, November, 15, 2001 would be a "health support system – a comprehensive, knowledge-based system capable of providing information to all who need it to make sound decisions about health. . . The

NHII includes not just technologies but, more importantly, values, practices, relationships, laws, standards, systems, and applications that support all facets of individual health, health care, and public health."

Terms Associated with Collections of Data

**Data set**, in common usage there are two definitions: (1) a list of recommended data elements with uniform definitions that are relevant for a particular use (American Health Information Management Association, *Pocket Glossary*). (2) a collection of data.

**Data registry**, a collection of health data related to a specific disease, condition, or procedure that makes the data available for analysis and comparison (American Health Information Management Association, *Pocket Glossary*). Data registries typically collect data in accordance with the data set requirements of a particular project.

**Data repository**: a clinical data repository (CDR) is a "real-time database that consolidates data from a variety of clinical sources to present a unified view of a single patient. It is optimized to allow clinicians to retrieve data for a single patient rather than to identify a population of patients with common characteristics or to facilitate the management of a specific clinical department" (Sittig DF, *et al*, Building and Using a Clinical Data Repository, *The Informatics Review,* 1999). A data repository may also be referred to as a transactional, or operational, database (see also Data warehouse).

**Data warehouse**: is "a subject-oriented, integrated, time-variant, nonvolatile collection of data on which a data analyst can perform complex queries and analysis, such as data mining, without slowing down the operational systems" (McFadden FR, et al, Clinical Data Warehouse, *The Informatics Review,* 2006; and Naeymi-Rad, F, Clinical Data Warehouse, Intelligent Medical Objects, Inc.). A data warehouse may also be referred to as a translational, or informational, database (see also Data repository).

# Appendix D: Data Stewardship Conceptual Framework for Health Data Uses

The following Data Stewardship Conceptual Framework for Health Data Uses builds upon the *Secondary Uses and Re-Uses of Healthcare Data: Taxonomy for Policy Formulation and Planning* of the American Medical Informatics Association (AMIA); the *Connecting for Health Common Framework Privacy Principles* from the Markle Foundation; and the *cancer Biomedical Informatics Grid (caBIG™) Framework for Data Sharing Terms and Conditions*.

The Data Stewardship Conceptual Framework for Health Data Uses is a tool intended to outline how an organization may approach evaluation of its intended uses of health data and recognize where it may need to enhance its data stewardship processes.

> *For example, a business associate of a payer, that is covered by HIPAA, and wishes to use identifiable data for quality measurement under HIPAA's permitted uses for healthcare operations, should describe the benefits of this use and consider the potential risk for harms, then consider how it addresses each of the data stewardship attributes. In some areas, the user may believe it provides appropriate data stewardship, but in other cases may believe there are opportunities for improved transparency, or stronger security controls, etc.*

**Data Stewardship Conceptual Framework for Uses of Health Data**

| **Health Data User and Use Profile** | | | | | | |
|---|---|---|---|---|---|---|
| **User:** *Provider, Payer, Clearinghouse, Business Associate or Agent, Federally-sponsored Researcher, Commercial Researcher, Public Health, PHR Vendor, Other* | | | | | | |
| **Regulatory Status:** *HIPAA Privacy and Security Rules, State Data Statutes, Common Rule, FDA Research Regulations, VA Research Regulations, HIPAA Privacy Board, Other State Laws, FTC, Other* | | | | | | |
| **Identity Status:** *Identifiable, HIPAA De-identified (Safe Harbor), HIPAA De-identified (Statistical), Limited Data Set, Anonymization, Pseudonymization, Other* | | | | | | |
| **Analysis of Benefits and Potential Risks** | | | | | | |
| **Intended use of data:** *Treatment, Payment, Healthcare Operations, Research, Public Health, Other* | | | | | | |
| **Impact:** *Benefits to Individual and Society, Potential Risk for Harms* | | | | | | |
| **Data Stewardship Attributes** | | | | | | |
| *Accountability/ Chain of Trust* | *Transparency* | *Individual Participation* | *HIPAA De-identification* | *Security Safeguards & Controls* | *Data Quality & Integrity* | *Oversight of Data Uses* |

# Appendix E: Abbreviations Used in this Report

AHIC – American Health Information Community

AHIMA – American Health Information Management Association

AHRQ – Agency for Healthcare Research and Quality

AMIA – American Medical Informatics Association

ASP – Application Service Provider

BHI – Blue Health Intelligence

CCHIT – Certification Commission for Healthcare Information Technology

CDC – Centers for Disease Control and Prevention

CFR – Code of Federal Regulations

CMS – Centers for Medicare and Medicaid Services

COPPA – California Online Privacy Protection Act

EHR – Electronic Health Record

FAQ – Frequently Asked Questions

FDA – Food and Drug Administration

FTC – Federal Trade Commission

FWA – Federalwide Assurance (FWA)

HHS – U.S. Department of Health and Human Services

HELPS – Trans-HHS Taskforce on Harmonization of Ethical and Legal Policies Related to the Use of Human Specimens and Data in Research

HIPAA – Health Insurance Portability and Accountability Act

HIE – Health Information Exchange

HISPC – Health Information Security and Privacy Collaboration

HIT – Health Information Technology

HITSP – Health Information Technology Standards Panel

HSP – Health Information Service Provider

IIHI – Individually Identifiable Health Information

IOM – Institute of Medicine

IRB – Institutional Review Board

NCHS – National Center for Health Statistics

NCPDP – National Council for Prescription Drug Programs

NCVHS – National Committee on Vital and Health Statistics

NHIE – NHIN Health Information Exchange

NHII – National Health Information Infrastructure

NHIN – Nationwide Health Information Network

NIH – National Institutes of Health

NPP – Notice of Privacy Practices

NQF – National Quality Forum

OCR – Office for Civil Rights

OHCA – Organized Health Care Arrangement

OHRP – Office for Human Research Protections

ONC – Office of the National Coordinator for Health Information Technology

PBM – Pharmacy Benefits Manager

PHI – Protected Health Information

PHR – Personal Health Record

PQI – CMS Better Quality Information Project

QASC – Quality Alliance Steering Committee

RFI – Request for Information

TPO – Treatment, Payment, and Healthcare Operations

VA – U.S. Department of Veterans Affairs