



Privacy and Security Issues of a National Health Information Network

**Patrick Stokes
2005 WISE Intern
Department of Biomedical Engineering
University of Texas at Austin**

August 3, 2005

Sponsored by



Preface

About the Author

Patrick Stokes was born in Austin, Texas and will graduate from the University of Texas at Austin in May 2006 with degrees in Biomedical Engineering and Economics. He worked at the Institute for Advanced Technology from June 2002 to June 2004 and is currently working in the Biomedical Informatics Lab in the Department of Biomedical Engineering at the University of Texas at Austin. He plans to pursue graduate work in biomedical engineering. He is a member of IEEE.

About WISE

The Washington Internships for Students of Engineering (WISE) program was founded in 1980. This collaborative effort among several engineering societies has become one of the premier Washington internship programs. Its goal is to groom future leaders in the engineering profession who are aware of and contribute to the important intersections of technology and public policy. This multi-society program is supported by the American Association of Engineering Societies. Please see <http://www.wise-intern.org> for more information.

Acknowledgments

I would like to thank IEEE for allowing me to spend this summer learning about government policy, the influence it has on science and engineering, and the role engineers play in the political process; investigating an interesting engineering topic from a policy perspective; and enjoying Washington D.C. I would also like to thank Faculty Member in Residence Steve Watkins for setting up meetings all over D.C. and keeping us on schedule. Special thanks to Dr. Michael Rozen, Chair of the IEEE-USA Medical Technology Policy Committee, for providing me with much needed advice and direction in approaching my topic; to Erica Wissolik for just about everything; and to the other WISE interns who made this a great summer.

Paper Citation

Patrick Stokes, "Privacy and Security Issues of a National Health Information Network," *Journal of Engineering and Public Policy*, vol. 9, 2005, available at <http://www.wise-intern.org>.

Table of Contents

Executive Summary.....	1
I. Introduction.....	5
a. The Proposed National Health Information Network.....	5
b. Purpose.....	6
II. Background.....	6
a. US Health Care.....	6
b. Benefits of HIT Adoption.....	7
c. Challenges to HIT Adoption.....	7
d. Need for Public Support.....	8
III. Privacy.....	9
a. Importance.....	9
b. Current Legislation.....	9
c. The HIPAA Privacy Rule.....	10
d. Privacy Issues of a NHIN.....	11
e. Ownership and Control of Health Information.....	11
i. Patient Ownership of Health Information.....	12
ii. Opt-in vs. Opt-out System.....	12
iii. Individual Privacy Settings.....	13
f. Division of Information.....	13
i. Role-Based Access.....	14
ii. Disclosure Limitations.....	14
iii. Access Notification.....	15
g. Patient Identification.....	15
i. De-identification.....	15
IV. Security.....	16
a. Importance.....	16
b. The HIPAA Security Rule.....	16
c. Security Issues of a NHIN.....	17
d. Technical Standards.....	18
i. Consolidated Health Informatics Initiative.....	18
V. Role of the Federal Government.....	19
a. Importance.....	19
b. The Veterans Health Administration.....	19
VI. Recommendations.....	21
References.....	23

Executive Summary

On April 27, 2004, President Bush called for a system of interoperable electronic health records (EHRs) covering most Americans within ten years and called for the creation of the Office of the National Coordinator (ONC) for Health Information Technology (HIT) to lead in the establishment and implementation of a National Health Information Network (NHIN). The adoption of HIT towards the development of a NHIN of interoperable EHRs can lower health care costs, reduce the number of medical errors, and improve the quality of health care. A NHIN will also allow for public health benefits including improved disease control for acts of bioterrorism and disease outbreak; greater medical research capabilities with large scale studies and patient outcome tracking; and an improved health care system due to determination and implementation of medical best-practices.

Unfortunately, the adoption of information technology (IT) in the health care system lags behind other industries because of financial and technical obstacles. The adoption of HIT requires substantial investment. A single EHR can cost between \$16,000 and \$36,000. But while the benefits of HIT are great, they mostly affect the patient and the public. Furthermore, even if a health care provider is inclined to adopt HIT to provide better care, there are no standards for technology, making information exchange and interoperability difficult and preventing the widespread adoption of HIT for a NHIN.

To drive the adoption of HIT and establish a NHIN, the public must be aware of the benefits of HIT and support its adoption. To build public support of and encourage participation in a NHIN, the privacy and security of personal health information must be established and demonstrated. Many federal laws address the discriminatory uses of personal health information. Currently the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the broadest legislation addressing privacy and security of personal health information. However, the HIPAA Privacy and Security Rules do not address specific privacy and security issues of a NHIN.

The Federal Government has over 20 years experience in the development and maintenance of a health information network focused on privacy and security of personal health information through its work with the Veterans Health Administration and establishment of the Consolidated Health Informatics (CHI) Initiative. Due to the significant cost of implementation and maintenance and the need for nationwide technical standards, the Federal Government is in the unique position to fund and oversee the development of a NHIN.

Overall, this report concludes that due to the significant public interest in the implementation of a NHIN, the slow adoption of IT in the health care system, and the need for public confidence in the confidentiality of personal health information, the Federal Government should take the responsibility to direct the adoption of HIT towards the establishment of a NHIN with a structure and technical standards focused on privacy and security.

Issues/Recommendations

Issue 1: Current legislation does not address ownership and control of personal health information as it relates to the collection and disclosure of information by non-covered entities, whether participation in a NHIN is voluntary or compulsory, and whether there will be individual privacy limitations set by patients.

Recommendations

- To prevent collection and disclosure of personal health information by non-covered entities and to demonstrate patient control of personal health information, Congress should enact legislation to establish patient ownership of health information.
- To prevent public perception of unauthorized disclosure of personal health information, HHS should establish the NHIN as an opt-in system.
- To give patients additional control of personal health information, HHS should establish that participation in a NHIN will allow individual privacy settings for patients to choose to disallow certain groups or individuals from accessing their information.

Issue 2: It is not currently established who will have access to what information and what are the limits of that access.

Recommendations

- HHS should adopt an interoperable EHR standard that incorporates role-based user access with a minimum data set, such as the Health Level 7 (HL7) EHR standard that incorporates the Continuity of Care Record (CCR) standard for a minimum data set.
- HHS should establish additional access and disclosure limits for instances when consent cannot be obtained or is not required, such as how long the user will have access, how the necessity of the privacy invasion is authenticated, and other similar issues.
- HHS should require automatic patient notification of user access of PHI.

Issue 3: Interoperability requires reliable identification of patients for matching records, but identification poses additional confidentiality risks.

Recommendations

- HHS should adopt a voluntary healthcare identifier program.
- Data should be de-identified to allow use of information to support government public health surveillance, quality control efforts, and statistical research without violating confidentiality.

Issue 4: Nationwide standards for technical implementation of security are absent, making interoperability difficult. However, constantly evolving technology could leave technical standards out of date, and currently, evaluation of privacy and security compliance is left to the health care provider or plan.

Recommendations

- CHI should continue to investigate standards for all aspects of storage and transmission of EPHI.
- HHS adopted technical security requirements should be reviewed and updated periodically by CHI.

- Congressional should give authority to HHS to oversee and evaluate compliance with privacy and security standards.

Issue 5: Additional privacy and security measures may have unintended consequences.

Recommendations

- HHS should document the costs, benefits, and impacts of implementing a NHIN with the above recommendations.

I. Introduction

a. The Proposed National Health Information Network

On April 27, 2004, President Bush called for a system of interoperable electronic health records (EHRs) covering most Americans within ten years. He signed Executive Order 13335 requiring the Secretary of Health and Human Services (HHS) to establish the Office of the National Coordinator (ONC) for Health Information Technology (HIT) to lead in the development and implementation of a National Health Information Network (NHIN). It is the responsibility of the National Coordinator to create “a strategic plan to guide the nationwide implementation of interoperable health information technology in both the public and private health care sectors,”¹ which will improve the quality of health care, lower medical costs, and reduce medical errors.

The National Coordinator presented his report outlining the strategic plan to the Secretary on July 21, 2004. The *Framework for Strategic Action: The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care* lists four goals to achieve: inform clinical practice with use of EHRs, interconnect clinicians so that they can exchange health information, personalize care with consumer-based health records and better information for consumers, and improve population health through advanced bio-surveillance methods and streamlined collection of data for quality measurement and research.²

On November 15, 2004, the ONC released a Request for Information (RFI) on the development and adoption of a NHIN. More than five hundred responses were received. The majority of respondents envisioned a NHIN of decentralized architecture built on existing technologies, such as the internet, with uniform standards of software and hardware. Most respondents also cited the need for incentives to encourage adoption of HIT and the need to address privacy and security concerns.³

b. Purpose

The adoption of information technology in the health care system lags behind other industries because of financial and technical obstacles. While the benefits of HIT are great, they mostly affect the patient and the public. To drive the adoption of HIT towards the establishment of a NHIN, the public be aware of and support such a network. To win public support for and encourage participation in a NHIN, the privacy and security of personal health information available on such a network must be clearly established and demonstrated.

This report investigates current regulations of privacy and security for personally identifiable health information, particularly the HIPAA Privacy and Security Rules, identifies specific issues concerning the establishment of a NHIN that are not addressed by the current legislation, and discusses the role the Federal Government should take in addressing these issues to build public support and confidence in the establishment of a NHIN.

II. Background

a. U.S. Health Care

The United States spent \$1.8 trillion on health care in 2004, approximately 15.8 percent of GDP and \$6,300 per capita, and costs continue to rise.⁴ Health care premiums have increased at double-digit rates each of the past three.⁵ The rising costs of health care have placed a significant burden on employers, due to the large number of employer-based health care plans. It is estimated that health care costs employers \$1.50 per employee per hour.⁴

Despite large expenditures on health care, thousands die each year as the result of medical errors and many patients don't receive proper care. The Institute of Medicine estimated that 44,000 to 98,000 people died in hospitals in 2003 as the result of medical errors.⁶ One in every five doses

of medication administered in typical hospitals and skilled nursing facilities is incorrect, and seven percent of those errors are potentially life-threatening.⁷ Other studies indicate that adults in the U.S. only receive 55 percent of recommended care.⁴ Also, because of the lack of access to necessary information such as medical history and results of earlier diagnostic tests, many tests are needlessly repeated.⁸ It is estimated that 30 percent of health care spending is for treatments that may not improve condition, may be redundant, or may be inappropriate, amounting to \$300 billion in 2004.⁴

b. Benefits of Health IT Adoption

The adoption of health IT, in particular portable and interoperable EHRs, is necessary to control the rising cost of health care in the U.S. It also offers the potential to improve the quality and efficiency of health care at lower costs. Studies estimate that the use of EHRs in ambulatory care would save \$112 billion per year, including \$34 billion for administrative costs and \$78 billion from interoperability.⁴ The Center for Information Technology Leadership estimates the implementation of nation-wide computerized order-entry systems with decision support would save \$44 billion annually.⁹ The Office of the National Coordinator for Health Information Technology estimates savings between 7.5 percent and 30 percent of annual health care spending.⁴ These estimated benefits exceed the estimated costs of \$275 billion over the next ten years and \$16.5 billion each year after.

The development of a NHIN would also offer numerous public health benefits including: improved disease control for acts of bioterrorism and disease outbreak; greater medical research capabilities with large scale studies and patient outcome tracking; improved health care system due to determination and implementation of medical best-practices; and the possibility of national health insurance through nationwide risk and cost assessment.

c. Challenges to HIT Adoption

The health care system is currently 5 to 10 years behind other industries in the adoption of IT, and most IT development is centered in densely populated urban areas.⁴ A major impediment to

widespread adoption of HIT is the absence of economic incentives for HIT adoption because the patients and not the physicians are the primary recipients of HIT benefits. It is estimated that \$21.6 billion to \$43.2 billion in government incentives over the next 7 to 10 years is necessary to drive widespread adoption of HIT.⁴ Another impediment to HIT adoption is the absence of interoperability standards, which are necessary to ensure that the information is accurate and useful. The last and perhaps the most significant hindrance to HIT adoption is the lack of public awareness of and demand for its benefits.

d. Need for Public Support

While the functionality and benefits of a NHIN depend on interoperability, the widespread adoption of HIT towards the establishment of such a system depends on public awareness, confidence, and support. A poll conducted by Harris Interactive found that 71 percent of Americans had not heard anything about a national EHR system to improve care, reduce errors, and reduce costs.¹⁰ Other studies indicate many patients are concerned about privacy and confidentiality of health records, particularly the possibility of personal health information appearing on the internet.⁴ A report by the HIT Leadership Panel concluded that the American public would not support a system of EHRs if “security and privacy were not readily apparent”⁴ and that successful implementation of a NHIN must not only comply with current federal privacy regulations but clearly demonstrate “that patient information is adequately safeguarded.”⁴

Public confidence is not only necessary to drive adoption of a NHIN but it is also necessary to encourage patient participation and enable the acquisition of reliable information. A Gallup poll found that 78 percent of Americans feel confidentiality of their medical records is very important, similar to 84 percent that feel confidentiality of their financial information is very important.¹¹ Another study found that one in six people withhold medical information because they are worried about who will have access.¹² Accessible and reliable health information is dependent on protecting privacy.

III. Privacy

a. Importance

The privacy of health information is extremely important because of the personal nature of the information and because access to such information can carry power over the individual. Personally identifiable health information affects employment and insurance opportunities.¹³ Further, advances in genetic testing capabilities allows for the possibility of additional discrimination, and the growing rate of identity theft significantly increases the importance of privacy.

b. Current Legislation

Federal legislation relating to privacy of health information addresses either confidentiality or discrimination. Most of the many federal laws applicable to a NHIN relate to discrimination. Federal law only prevents health plans from dropping a specific individual. Plans can choose to not cover an entire condition.¹² The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects individuals from losing their health insurance when they lose their jobs, and The Americans with Disabilities Act protects against employer discrimination, but the third party system of payment still allows employers to access employee health information.

HIPAA is also the first Federal Law to address issues of genetic discrimination. HIPAA dictates that genetic information not be treated as a pre-existing condition and prevents plans from using the information to establish eligibility or setting premiums, but does not protect groups as a whole, nor does it prevent plans from requiring or disclosing genetic information, and it permits exclusion and benefit limits for specific conditions.¹⁴

HIPAA is the broadest legislation addressing confidentiality of health information. Prior to

HIPAA there were no federal laws governing confidentiality of health information. States and localities had their own unique laws affecting patient access, disclosure, privilege, and other issues. Section 264 of HIPAA requires HHS to develop standards of privacy for personally identifiable health information.¹³

c. The HIPAA Privacy Rule

The Final HIPAA Privacy Rule, released by HHS on August 14, 2002 and effective in April 2003, established a set of basic consumer protections and a series of regulatory permissions to limit use and disclosure of personally identifiable information, so that health information can be protected while allowing necessary information flow for improved care and public health.¹⁵ The Privacy Rule covers applicability, individual rights, permitted uses and disclosures with and without consent, information practices, preemption, enforcement, and penalties.

The Privacy rule defines Protected Health Information (PHI) as any personally identifiable health information. The Privacy Rule also defines covered entities as any health plans, health care providers, and health care clearinghouses and defines covered information as any information electronically maintained and transferred and any form of PHI.¹³

The Privacy Rule states individuals have a right to access their medical records, to request amendments to their information, to a list of disclosures, to file complaints about disclosures, and to request restrictions be placed on disclosure. Providers also must make a “good faith” effort to obtain written acknowledgment of receipt of privacy practices notice from patients.¹³

Use and disclosure of PHI for treatment, payment, or health care operations (management and other supportive activities) does not require a patient’s prior written consent. Disclosures for other uses require prior written authorization.¹³

Disclosures for the legal oversight of the health care system, such as instances of fraud or civil rights abuses, disclosures for emergency treatment and public health activities in instances of serious threat to health and safety to any person, disclosures for authorized research, and

disclosure to law enforcement for investigations of abuse, neglect, or domestic violence do not require prior written consent or authorization.¹³

Disclosure of PHI for anything other than treatment must use “minimum necessary” information. Covered entities must enter contracts with “business associates” requiring them to protect PHI and must act if violations are discovered. The Privacy Rule also specifies procedures for using PHI for fundraising and marketing and requirements for federal and private funded research. Psychological notes cannot be used or disclosed without explicit authorization.¹³

The Privacy Rule preempts state laws, except when the state law is more stringent. The HHS Secretary is responsible for evaluating compliance and enforcement. HHS Office for Civil Rights handles complaints of non-compliance and violations are subject to civil penalties. Knowingly disclosing PHI is subject to criminal penalties enforced by the Department of Justice (DOJ). Patients are not allowed to sue.¹³

d. Privacy Issues of a NHIN

Nationwide adoption of EHRs and the establishment of a NHIN can actually “increase our ability to protect confidential information,”¹² as well as improve care, because access can be defined and enforced. While much legislation exists to protect patients against discrimination and The Privacy Rule establishes limits for uses and disclosures of PHI, these do not address specific privacy issues of establishing a NHIN including ownership and control of personal health information, the nature of patient participation, the division of information for role-based access, the need for additional disclosure limitations, and the means of patient identification. It is at this stage, prior to the nationwide implementation of a NHIN, that the privacy expectations from such a system should be outlined and should provide the basis for its structure.

e. Ownership and Control of Health Information

There is currently no consensus or regarding ownership of medical records or health information in general—whether they belong to the patients, the doctors, the insurance companies, or

business associates. This question may determine who maintains the records, who controls the information, and who has access to what information. Health care providers are in the position to update and maintain health records, and health care plans are in the position update and maintain treatment and payment information, but all PHI information concerns the patient, who is the only one affected by the ramifications of privacy breaches.

Privacy has been described as the ability to control information about yourself even after you have given it to someone else,¹⁴ and the 10 million instances of identity theft per year indicate that there is no market incentive for privacy.¹² Citigroup used unencrypted computer tapes to transport financial information of 4 million customers via UPS and the tapes are lost. Time Warner lost financial data on 600,000 employees. 1.4 million DSW Shoe Warehouse customer credit-card numbers were compromised by hackers. ChoicePoint sold information on 145,000 Americans to criminals. “Companies are all too cavalier when it comes to protecting financial info that can lead to identity theft” because it does not directly affect the companies.¹⁶

i. Patient Ownership of Health Information

One possibility to ensure confidentiality and control the improper dissemination of PHI is improved legislation granting patient ownership of their health information and making it illegal for anyone to purchase or sell PHI, making it illegal for anyone other than the patient, provider, and payer to collect or disclose PHI, and establishing more stringent limits on disclosure by providers or payers. This is similar to Executive Order 13145, signed by President Clinton on February 9, 2000, which prohibits the Federal Government from requesting, collecting, purchasing or disclosing protected genetic information.¹⁴

ii. Opt-in vs. Opt-out System

Proposed models for a NHIN focus either on opt-in adoption, in which a patient would actively grant permission for their information to be made available on the NHIN, or opt-out adoption, in which a patient’s information is automatically made available on the NHIN until they actively request their information be removed. An opt-out adoption would cost less but would lead to

public perception that their information is shared unwillingly. A Gallup poll found that 95 percent of Americans feel doctors should get permission before releasing information to a national computerized database.¹¹ An opt-in model, on the other hand, may lead to slower adoption. A Harris Interactive Poll found that 48 percent of Americans feel the benefits of an EMR system outweigh possible privacy risks.¹⁰ But a recent study found that between 250,000 and 500,000 people now have electronic “personal health records,” through employers or insurers.¹⁷

iii. Individual Privacy Settings

Additional patient control could be established by allowing patients to set individual information access settings to grant access to specific groups of users. A Harris Interactive poll asked Americans if they favored or opposed a list of groups being allowed to see their medical records without a priori permission: 59 percent opposed pharmacists; 92 percent opposed government agencies; 88 percent opposed police or lawyers; 84 percent opposed employers; 82 percent opposed insurance companies; 71 percent opposed local and state health agencies; 71 percent opposed doctors; 67 percent opposed medical researchers; 95 percent opposed banks.¹¹ This demonstrates the importance patient control of health information. Division of information through role-based access, which will be discussed in the next section, will allow at least partial patient choice in disclosure limitations.

f. Division of Information

The question of medical privacy for a NHIN is an issue of who has access to what information. On the one hand privacy is necessary for public support and participation, but protecting confidentiality may affect care given to patients if the necessary information is not available to health care providers.¹³ Currently, physicians don’t have all the information needed and “too much information is available to people who don’t need it. When someone requests the paper record, it is an all-or-nothing proposition.”¹² Many Americans are unaware of the numerous instances in which their health information can be disclosed without their permission as the

information is exchanged for treatment and payment. “Estimates indicate that 150 to 400 individuals may have access to the data collected in a person’s medical records.”¹⁵

i. Role-Based Access

Role-based user access with a minimum data set standard would ensure that users such as health care providers and payers only view necessary information. It would allow separation of personal, physical, mental, and financial information, such as shielding mental health information from only mental health professionals or separating personal information told to a physician that would only viewable by the specific physician.¹² A Gallup poll found only 4 percent of Americans believe personal information told to a doctor should be recorded in a national database.¹¹

Health Level Seven (HL7) a standard development organization (SDO) has developed an EHR standard using core functionalities identified by the Institute of Medicine (IOM). However, the standard does not currently establish specific data standards. It is currently undergoing a two-year trial.¹⁸

A Continuity of Care Record (CCR), which is a national standard for a minimum data set that ensures that a user only has access to necessary parts of an EHR, is being developed by ASTM International in conjunction with the American Academy of Family Physicians, the Massachusetts Medical Society, and the Health Information Management and Systems Society. Each new health care provider is able to access and update the CCR.¹⁸

ii. Disclosure Limitations

There are many instances when it is necessary to disclose PHI without the patient’s consent, such as when a patient is unable to grant access, in instances public health risk, or when a crime has possibly been committed, such as gunshot wounds and child and elder abuse.¹² Many of these instances are outlined by the Privacy Rule, however, a NHIN poses new issues that are not

addressed by the Privacy Rule, such as the duration of access, the role of the user, and the authentication of the need to violate the confidentiality.

iii. Access Notification

Oversight can be improved by automatically recording those agents that access a patient's records and informing the patient. A Harris Interactive Poll found that 45 percent of Americans feel it is very important that an EMR system incorporate tools that allow consumers to track their information and exercise privacy rights. Thirty-seven percent feel it is somewhat important.¹⁰ "Maintaining audit trails in computer-based patient records holds all [participants] to new levels of accountability."¹² The current Privacy Rule already has established procedures for investigating complaints against those that access and disclose information improperly.

g. Patient Identification

Correct identification and matching of patients with their health records is essential to achieving the benefits of interoperability. Both a national patient identifier and algorithmic patient identifier have been proposed as means of patient identification. The risks of privacy intrusions and improper information disclosures could be increased by the existence of a national patient identifier. A Gallup poll found that only 12 percent of American had heard about proposals for national patient identifiers, and only 8 percent would support a plan that required such a number.¹¹ However, the use of an algorithmic identifier would increase the occurrence of false-positives, in which the incorrect patient record is provided, and false-negatives, in which an existing patient record is not found.

i. De-identification

EHRs allow for the removal or encryption of identifiers to track individuals over time without knowing the identity.¹² This allows for improved bio-surveillance for acts of bioterrorism and disease outbreak, large-scale clinical and public health research studies; monitoring

establishment of medical best-practices nationwide, and the determination of fair insurance costs estimated from nationwide risk and cost assessment, all without infringing on patient confidentiality.

IV. Security

a. Importance

Even though privacy expectations of health information are established by the conceptual structure of the NHIN, security rules are the only way to ensure that those expectations are met. For example, the confidentiality achieved by preventing a health care provider from disclosing PHI is negated if a workstation with access to PHI is not secured from unauthorized users or if an authorized transmission is intercepted. To ensure privacy expectations of PHI there must be administrative procedures and technical standards for storage and transmission of PHI and credentialing and authentication of users. For this reason, Section 262 of HIPAA required HHS to develop standards for electronic exchange and storage security of PHI.

b. The HIPAA Security Rule

HHS released The Final HIPAA Security Rule on February 20, 2003. The Security Rule presents management-based standards for securing privacy of Electronic Protected Health Information (EPHI). The Security Rule also presents required and addressable implementation specifications to meet the standards. The general provisions are to guarantee the confidentiality, integrity, and availability to EPHI that a covered entity creates, maintains, receives, or transmits; to protect against foreseeable threats or hazards to security; to protect against foreseeable uses or disclosures not permitted by the Privacy Rule; and to guarantee workforce compliance. The implementation specifications are divided into administrative safeguards, which are security management policies and procedures to prevent, detect, contain, and correct security violations; physical safeguards to protect EPHI from unauthorized disclosure, modification, or destruction; and technical safeguards of security services and mechanisms.¹⁹

The administrative safeguards require covered entities to hire a single individual in charge of security management to perform risk analysis and risk management, to sanction security policy, and to review information system activity. Other required safeguards include procedures for responding to and reporting instances of security breach; contingency plans for data backup, disaster recovery, and emergency mode operation; and periodic self-evaluation of security. Addressable safeguards include workforce security, such as clearance, authorization, supervision, and termination procedures; security awareness training, such as security reminders, log-in monitoring, and password management; and information access management, such as access authorization, establishment, and modification.¹⁹

The physical safeguards require proper use and physical security of workstations that access EPHI, as well as procedures for the re-use and disposal of hardware or media containing EPHI. Addressable safeguards include facility access controls, such as a security plan, access control and validation procedures for staff and visitors, as well as records of movement of hardware and electronic media and the staff responsible and data backup and storage.¹⁹

The technical safeguards require access controls, such as unique user identification and emergency access procedures; user authentication procedures; and audit controls to track user activity via hardware and software or procedural methods. Addressable safeguards include additional access controls, such as automatic logoff and encryption and decryption of EPHI; integrity mechanisms to authenticate EPHI to prevent improper alteration or destruction; and transmission security, such as encryption and integrity controls to ensure electronically transmitted EPHI is not improperly modified.¹⁹

c. Security Issues of a NHIN

The difficulties in establishing security for a NHIN are similar to the difficulties in the adoption of HIT in general: the absence of technical standards and the high costs of implementation and maintenance. As mentioned previously, the Security Rule was left intentionally left unspecified in terms of technical specifications for implementation to allow covered entities the opportunity to

achieve security by means individually determined best-fit. This, however, interoperability challenges and makes evaluation of compliance more difficult.

d. Technical Standards

The lack of technical standards in the Security Rule leads to difficulties achieving interoperability. For example, encryption of transmitted EPHI is not required because there is no standard for encryption and so the receiving entity may not be able to decrypt the information from the sending entity. The lack of implementation specifications also leads to variances in security across the nation, due to differences in administrative procedures and user credentialing and authentication. This is particularly important as the health care system shifts towards outpatient care, such as electronic prescription ordering and at home patient monitoring of elderly patients, due to the use of remote sensors and wireless transmission.

Because of the absence of technical standards, evaluation of security capabilities is left to the covered entities themselves. With technical standards in place, HHS could evaluate compliance with security standards and oversee maintenance. Further, if standards were imposed in a modular approach, it would allow for implementing, maintaining, and updating separate security standards in phases at cheaper costs and would allow workers to adapt to new rules and technology more easily.¹⁵

Unfortunately, the imposition of technical standards allows for the possibility of requiring the use of an obsolete technology. Security technology constantly evolves and mandating a specific technology could lead to an outdated system without legal means to make improvements.

i. Consolidated Health Informatics Initiative

The Consolidated Health Informatics (CHI) initiative is a collaboration between HHS and the Departments of Defense (DOD) and Veterans Affairs (VA) as part of an eGov initiative

supported by President Bush to establish health information interoperability standards. CHI has adopted 20 sets of standards developed by a private SDO. The standards are focused on narrow aspects of health information exchange such as pharmacy transactions and exchange of lab results and images. However, these standards do not yet apply to all storage and transmission of EPHI.¹⁸

V. Role of Federal Government

a. Importance

Due to the significant public interest in the widespread adoption of a NHIN and the necessity of public confidence in the confidentiality of PHI to drive the adoption of and encourage participation in a NHIN, the Federal Government has the responsibility to establish a NHIN structure focused on privacy and security of PHI.

Additionally, due to the high importance of interoperability standards and the extensive funding required to facilitate the implementation of security technologies to ensure confidentiality of PHI, the Federal Government is in the unique position to establish specifications for and fund implementation and maintenance of the necessary technologies to secure a NHIN.

Lastly, the Federal Government has over twenty years of experience establishing and maintaining an interoperable health information network focused on privacy and security needs through its operations in the Department of Veterans Affairs (VA) and its creation of the CHI initiative discussed earlier.

b. The Veterans Health Administration

The Veterans Health Administration, within the VA, first started developing its health information system in 1985 with the creation of the Decentralized Hospital Computing Program (DHCP).¹⁸ The system was updated during the 1990s to the Veterans Health Information Systems and Technology Architecture (VistA)—an automated inpatient and outpatient

information system. VistA is composed of three components: the Computerized Patient Record System (CPRS), which allows providers to review and update patient information with a real-time order checking system and offers a clinical reminder system and a notification system to alert physicians; VistA Imaging which immediately places x-rays, pathology slides, cardiology exam results, etc. into patients' records; and the Bar Code Medication Administration (BCMA) which is point-of-care software to match patient, medication, dose, and time.²⁰

The system is again being updated to the HealtheVet-VistA, which provides the same capabilities as the Vista system but focuses more on patient information by developing a national data repository, better standards to improve data portability, and One VA Architecture to increase security and data quality. HealtheVet-Vista strengthens privacy and security through role-based access – limit access by user identity, location, job function, and legal authority – and increases the ability to track who accesses what information and when.²¹ HealtheVet-Vista also has a modular design to allow incorporation of new technologies and flexible adaptation to changing health care needs at lower maintenance cost.²⁰ Eventually, HealtheVet-Vista will interconnect its five systems – VA Health Benefits System, Health Data System, Provider System, Health Management and Finance System, Health Information and Education System.²⁰

Also under development is the My HealtheVet Personal Health Record (PHR) System. My HealtheVet is a secure online environment for patients, which offers copies of medical records and other personal health information a patient deems important. The information is owned and controlled by the patient, allowing consolidation from multiple providers and encouraging patient involvement in health care decisions.²¹ My HealtheVet also provides health education tools, an online calendar for updating and monitoring information, such as cholesterol, blood pressure, blood glucose, weight, pain, and medications. The system encourages patients to communicate with clinicians and be more active in their treatment for improved health outcomes, treatment adherence, and satisfaction.²¹ The system is undergoing two new stages of development that will allow patients to refill prescriptions and make payments and allow patients to request portions of their health records electronically and grant authority to family members to view the information.²¹ My HealtheVet opened Veterans Day 2003 and now has fifty thousand registered users and 300 registrations a day.²¹

The VA is also developing a public version of VistA, called HealthePeople-VistA, through which the VA collaborates with outside providers to improve outpatient care by developing standards for data and communication and increase the adoption of EHRs and PHRs. The VA also works with the DOD and the ONC to develop longitudinal health records in collaboration with Non-VA providers that protect privacy in accordance with the HIPAA Privacy Rule.²¹

VI. Recommendations

It being that the adoption of HIT towards the establishment of a NHIN of interoperable EHRs would offer significant benefits to the public, including reducing health care costs, reducing the number of medical errors, and improving the quality of care; it being that the adoption of HIT lags behind other industries due to lack of standards and to the fact that the adoption benefits the public instead of the health care providers; it being that public support and demand is necessary to drive the adoption of HIT towards the implementation of a NHIN; it being that public confidence in the privacy and security of personal health information available on a NHIN is necessary to build public support for and encourage participation in a NHIN; and it being that the government is committed to the development of a NHIN utilizing existing infrastructure, such as the internet and mobile communications, to securely and reliably share health information and is willing to provide financial incentive to help providers cover costs in the widespread adoption of EHRs, this report presents the following recommendations to ensure privacy and security of PHI and build much needed public support for adoption of a NHIN:

To cover PHI against intrusion by uncovered entities and to demonstrate patient control of PHI, Congress should enact legislation to establish patient ownership of health information, making it illegal for anyone to purchase or sell PHI, making it illegal for anyone other than the patient, provider, and payer to collect or disclose personally identifiable health information, and establishing more stringent limits on disclosure by providers or payers. To further demonstrate patient control of PHI and to prevent the public perception of unauthorized disclosure of PHI, HHS should establish the NHIN as an opt-in system, whereby a patient's EHR is not released to a NHIN without prior written consent.

To achieve interoperability and needed information exchange while preventing entities from obtaining more information than is necessary through the establishment of role-based access to EHRs with a minimum data set, HHS should adopt the HL7 EHR standard with the CCR model for minimum data set, maintained by health care providers and plans. In conjunction with an EHR model focused on role-based access with a minimum data set, HHS should adopt a model that incorporates individual privacy settings and automatic user access notification of the patient, to further demonstrate patient control of PHI. HHS should also establish additional disclosure limitations pertaining to instances where consent of the patient cannot be obtained, such as how long the user will have access, how the necessity of the privacy invasion is authenticated, and other similar issues.

To achieve interoperability of EHRs and obtain the full benefits of a NHIN, HHS should create a Voluntary Healthcare Identifier Program.²² De-identification of data should be adopted as a means to support government public health surveillance, quality control efforts, and statistical research without violating confidentiality.

To achieve nationwide security standards, such as standard encryption and decryption techniques, CHI should continue to investigate standards for all aspects of storage and transmission of EPHI. Adopted standards should be reviewed and updated periodically. Congress should give authority to HHS to oversee and evaluate compliance with adopted privacy and security standards. To monitor the unintended consequences of implementing a NHIN with the above recommendations, HHS should documenting the costs, benefits, and impacts of implementation.

References

1. Executive Order 13335 of President George W. Bush, April 27, 2004.
2. "Framework for Strategic Action – The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care", Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, July 21, 2004.
3. "Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses," Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, June 2005.
4. The Lewin Group, Inc., "Health Information Technology Leadership Panel – Final Report," March 2005.
5. The Kaiser Family Foundation and Health Research and Educational Trust, "Employer Health Benefits 2003 Annual Survey," <http://www.kff.org/insurance/ehbs2003-1-set.cfm>.
6. The Institute of Medicine, "To Err is Human: Building a Safer Health System," National Academies Press, 2000, <http://www.nap.edu/openbook/0309068371/html/>.
7. Barker, K.N., Flynn, E.A., Pepper, G.A., et al., "Medication Errors Observed in 36 Healthcare Facilities," *Archives of Internal Medicine*, vol. 162, no. 16, September 2002.
8. Health Information Management Systems Society, "EHR and the Return on Investment," <http://www.himss.org/content/files/EHR-ROI.pdf>.
9. Center for Information Technology Leadership, <http://www.citl.org/research/ACPOE.htm>.
10. Harris Interactive, "How the Public Sees Health Records and an EMR Program," February 16, 2005.
11. The Gallup Organization, "Public Attitudes Towards Medical Privacy," September 20, 2000.
12. Janlori Goldman, Paul Schwartz, and Paul Tang, "Roundtable: Medical Privacy," *Issues in Science and Technology*, Summer 2004.

13. Gina Marie Stevens, Legislative Attorney, American Law Division, "A Brief Summary of the HIPAA Medical Privacy Rule," RS20934, April 30, 2003.
14. Nancy Lee Jones and Alison M. Smith, Legislative Attorneys, American Law Division, "Genetic Information: Legal Issues Relating to Discrimination and Privacy," RL30006, March 11, 2005.
15. Rebecca T. Mercuri, "The HIPAA-potamus in Health Care Data Security," *Communications of the ACM*, vol. 47, no.7, July 2004.
16. Steven Levy, "Lost My Secrets? Pay Up, Buddy!" *Newsweek*, June 20, 2005.
17. Sarah Rubenstein, "Putting Your Health History Online," *The Wall Street Journal*, Tuesday, June 21, 2005.
18. C. Stephen Redhead, Specialist in Life Sciences, Domestic Social Policy Division, "Health Information Technology: Promoting Electronic Connectivity in Health Care," RL328858, April 13, 2005.
19. Tom Grove, Vice President, Phoenix Health Systems, "Summary Analysis: The Final HIPAA Security Rule," February 2003.
20. Department of Veterans Affairs, Veterans Health Administration, "Veterans Health Information System and Technology Architecture."
21. Testimony of Dr. Robert M. Kolodner, Acting Chief Informatics Officer of the Veterans Health Administration, before the Committee on Science, Commerce, and Transportation, Subcommittee of Technology, Innovation, and Competitiveness, United States Senate, June 30, 2005.
22. IEEE-USA Position Statement on Voluntary Healthcare Identifier, June 2004.