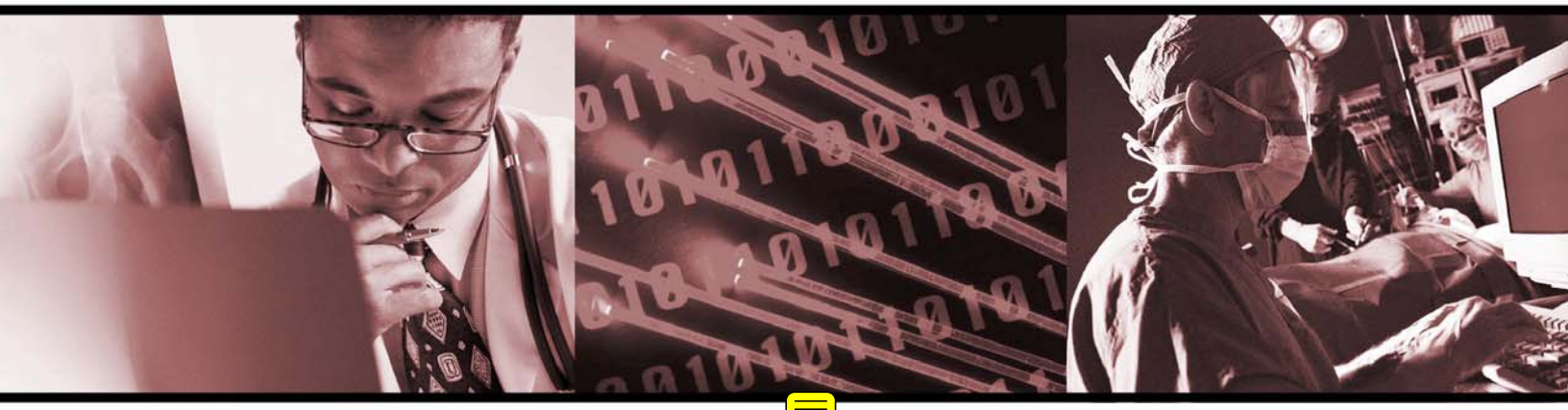
MARKLE FOUNDATION

CONNECTING FOR HEALTH

A Public-Private Collaborative



The Privacy and Security Working Group

Report and Findings

June 5, 2003

Table of Contents

Executive Summary

The electronic medical record offers the promise of improved care and increased efficiency. Introducing information technology into health care creates new risks to privacy as well as new means to protect privacy Patients are well aware of the potential risks associated with the automation and sharing of their medical information. These concerns can lead patients to withhold from their clinicians information that could be crucial for their care. Clinician concerns about privacy and security can lead to exclusion of sensitive information from medical records reducing the value of the record to other clinicians treating the patient and to researchers and public health officials. This report brings the good and reassuring news that with conscious forethought and continuous care and attention, the use of information technology in healthcare can and should strengthen, not impair the security and privacy of personal health information.

Connecting for Health Privacy and Security Working Group

Connecting for Health …A Public-Private Collaborative brings together participants from every stakeholder group in healthcare with interests in driving an interoperable healthcare system, including practicing clinicians, hospitals, employers and other third-party payers, federal and state government organizations, healthcare information technology suppliers, academic and research institutions, national standards groups, manufacturers, community organizations, and consumer groups.

The purpose of Connecting for Health is to catalyze specific actions on a national basis that will rapidly clear the way for an interconnected, electronic health information infrastructure. The Collaborative plans to accomplish this by focusing on three key areas:

- Accelerating the rate of adoption of clinical data standards throughout the nation's healthcare system in order to facilitate interoperability.

- Identifying practical strategies and solutions for developing an interconnected electronic infrastructure that will ensure the secure and private transmission of medical information and support the continuity of personal health information across plans and providers.

- Actively working to understand what consumers will need and expect from an interconnected health information system and identifying key steps for meeting their needs.

The Connecting for Health Privacy and Security Working Group took as its charge:

- Reaching consensus on a set of principles and criteria for assessing "noteworthy practices" for clinical and administrative data sharing and management

- Identifying and disseminating examples of privacy and security "noteworthy practices" that are reasonable and practical in a variety of operational environments, comply with Health Insurance Portability and Accountability Act (HIPAA), represent consumer concerns, and balance costs and benefits

- Promoting the adoption of recommended practices that data producers and data users can employ to address privacy and security issues inherent in improving the delivery of healthcare, including quality, cost, access, and outcomes

To fulfill this mission the Privacy and Security Working Group sought out noteworthy and promising privacy and security practices that are currently in use to show that creative solutions are both possible and affordable, and to describe them so they can serve as a model for others. By this strategy, we hope to promote the creation and deployment of noteworthy privacy and security practices.

Methodology

The goal of the Privacy and Security Working Group was to identify noteworthy practices that others can implement to further the development of an interconnected healthcare system the national health information infrastructure. The Working Group did not conduct a comprehensive survey of practices currently being utilized. Nor did the Working Group attempt to rank organizations on their privacy and security practices. Rather, the goal was to seek out and promote noteworthy privacy and security practices that are currently in use.

Each noteworthy practice exhibited a subset of these fourteen principles:

- Trustworthy – can be relied on by patients to protect their health information
- Improved care for the patient – supported the implementation of practices or programs that enhance quality of care
- Increased patient involvement – provide opportunities for the patient to understand and engage in their care and interact with the information about their health status and healthcare
- Enhanced the healthcare relationship – enable communication between patients, healthcare organizations and clinicians
- Transparent – provide clear and complete information to patients about their methods and scope
- Interoperable – increase the access to information from independent healthcare systems

- User friendly – are easily understood and learned by the users
- Ubiquitous – apply to all data within the scope of the practice
- Scalable – can be adopted by organizations of differing size and complexity
- Sustainable – can be funded as part of ongoing operational budgets
- Enable specific healthcare functions – allow patients, healthcare organizations and clinicians to participate in healthcare in ways that are not readily feasible without the use of private and secure information technology
- Enhance the ability to protect public health – support public health reporting and surveillance
- Improve ability to measure, study, research – facilitate the creation of and access to data for research purposes
- Balance cost and risk – are seen by the implementing organizations as having sufficient value to justify their investment in the practice

Within the context of an interconnected healthcare environment, the Working Group evaluated the following technical and organizational practices:

- Monitoring patients electronically
- Sharing patient care, public health monitoring, and research data across enterprises
- Patient Provider communication
- Securing e-mail for personal health information
- Making medical records accessible for patients who do not have a regular source of care
- Controlling access to Personal Health Information
- Tracking access to Personal Health Information
- Authenticating users of Personal Health Information
- Training users of Personal Health Information in privacy and security policies and practices
- Measuring privacy and security performance

The following sites were reviewed and are included in this report:

- **Visitantes Información Acceso (VIA)** – A project funded by HRSA Rural Communities Assistance to provide migrant farmers with email accounts and a web-based medical record. California Migrant Health
- **CareGroup Healthcare System**: CareGroup is an integrated delivery system serving Massachusetts. The system includes four hospitals with more than 1,000 beds, as well as specialty clinics and research facilities. CareGroup's not-for-profit Provider Service Network serves more than 400,000 managed-care patients.
- **IDEATel:** A four year demonstration project funded by CMS to provide home monitoring of 1500 diabetes patients in urban and rural New York State
- **Denver Health Hospital Authority**: A public integrated delivery system that includes a hospital, school and community clinics, a managed care program, and the 911 emergency response system.
- **Department of Veterans Affairs**: The Veterans Health Administration provides care to 4.3 million patients at 1300 care sites, including 170 hospitals and 800 outpatient clinics.

- **Henry Ford Health System**: Non-profit healthcare enterprise with $2 billion in revenues annually. They are Michigan's sixth larges provider with 5 hospitals and 2.5 million patient contacts
- **Humana**: A publicly traded health benefits company, with approximately 6.4 million medical members. Humana has contracts with 296,000 physicians and 3,700 hospitals in 44 states.
- **Kaiser Permanente of Northern California**: Kaiser Permanente is a nonprofit prepaid, group practice health maintenance organization (HMO), The Kaiser Permanente Northern California Region has almost 3.2 million members. It includes 4,451 physicians in The Permanente Medical Group (TPMG) and approximately 46,000 employees
- **Mayo Foundation**: A not-for-profit healthcare system with 4 hospitals, 3 clinics and a health system network. Mayo serves over 500,000 patients each year and has over 45,000 employees in Minnesota, Arizona, and Florida.
- **North Carolina Emergency Department Database**: A statewide repository of emergency department visit data
- **Palo Alto Medical Foundation**: A not-for-profit multi-specialty group practice with 246 providers, 1,200 employees providing over 800,000 patient visits per year.
- **Partners Healthcare System**: A not-for-profit organization offering primary and specialist care, acute-care hospitals, and other services. Partners Community HealthCare, a physician network, encompasses 1,000 practitioners.
- **Indiana Network for Patient Care**: A community data sharing network under the auspices of the Regenstrief Institute
- **Montgomery County, Maryland Electronic Surveillance and Notification System**: A regional collaboration with Johns Hopkins University Applied Physics Laboratory. The project collects data from community hospitals, local pharmacies, public health agencies, schools, police, and fire departments.

Practices at these sites were identified as either noteworthy or promising. Noteworthy practices have been fully operational and can be considered to have a proven track record. Promising practices are those at the early stages of implementation but that may provide worthwhile new approaches to important privacy and security challenges.

Privacy and Security Practices by Site

Organization	Name of Project	Noteworthy	Promising
Visitantes Información Acceso (VIA)	VIA- Follow Me		Personal Health Page
CareGroup Healthcare System	Patient Site	Audit Trail Patient Provider Communication	
IDEATel	IDEATel	Patient Monitoring Communication PKI	

Organization	Name of Project	Noteworthy	Promising
Denver Health Hospital Authority	Single Sign-on		Single Sign-on
Henry Ford Health System	Patient Website	Secure Patient/Provider Communication	
Humana	PHI Net	Web-Based Training	Lexicon Email
North Carolina Emergency Department Database	North Carolina Emergency Dept Database	ER Data Sharing Data use agreement Limited Data Set	
Palo Alto Medical Foundation		Role Based Access Control Break the Glass	
Partners Health Care System	Patient Gateway	Patient Access to Medical Records Policies	Reason for Access
Indiana Network for Patient Care	Indiana Network for Patient Care	Governance of Inter-Enterprise Data Sharing	
Department of Veterans Affairs	Policy Privacy Training	Web-Based Training	
Kaiser Permanente of Northern California	Comprehensive Audit Trail	Audit Trail Training	
Mayo Foundation		Single Sign-on Break the Glass Web-Based Training	Privacy Dashboard
Montgomery County Electronic Surveillance and Notification System	National Capital Regional Surveillance Collaboration		Limited Data Set Data Use Agreement

Site Review Methods

The Privacy and Security Working Group identified organizations that have developed technical and managerial practices that demonstrate the protection of privacy and security, while making broad and creative uses of electronic health information. These organizations were identified through a review of literature and reports, as well as the extensive knowledge of the industry that exists across the members of the PSWG. The report is not intended to

present a comprehensive survey of all organizations or all practices that address privacy and security in an interconnected healthcare environment.

Within each of these organizations we focused our review on specific privacy and security practices. We did not undertake a comprehensive review of each organization's overall approach to privacy and security. Our review of each organization's practices is based on interviews, analysis of documentation, examination of web sites, and review of published articles and reports. We did not conduct site visits.

Conclusions from Noteworthy and Promising Practices

The set of practices presented in this report provide lessons specific to each practice and broader lessons about the potential for healthcare organizations to advance an interconnected healthcare system and maintain a high level of privacy and security.

- **Monitoring Patients Electronically –** Patient-provider messaging and remote monitoring of patient health status can be accomplished with full security and privacy protections. The secure patient monitoring program is an excellent example of using technology to monitor chronically ill patients. The use of this technology improves the communication between patient and clinician and allows for the regular exchange of clinical data.

- **Sharing Patient Care, Public Health Monitoring And Research Data Across Enterprises --** Despite the complex and competing interests of hospitals and the minimal resources available, there are successful models of data sharing among enterprises. By focusing on improving health outcomes, competitors have been willing to share information electronically. These organizations have voluntarily instituted data use agreements and ensured that direct identifiers are removed. Many of these projects are currently sustained by grant funding. They will need sustainable funding sources over the long term. Further research is needed to demonstrate the value of the projects for the participants. This may provide the basis for long-term funding by the participants themselves.

- **Patient-Clinician Communications --** Secure email solutions are working well at a number of different institutions. However, the success of all of these projects has been a bi-product of the existence of an online medical record. These projects further emphasize the added benefit and value that can be derived from moving to an Electronic Health Record (EHR).

- **Screening Email For Personal Health Information** – The use of a lexicon to screen emails to protect patient privacy is a promising technology that is in use at some sites today may be introduced by additional vendors. Products may emerge with pre-packaged lexicons. With additional competition, a broad range of users may find these applications affordable and easy to implement in a variety of environments. The screening lexicon may be useful for other healthcare applications, e.g., identifying records with specific chief complaint

text. Standardization of terminology will enhance the value of a lexicon by reducing the error rate in records identified as meeting the specified criteria.

- **Making Medical Records Accessible For Patients Who Do Not Have A Regular Source Of Care –** The use of a web-based personal medical record is an accessible practice for both organizations and consumers. Once the record is set up, the patient controls the updates. Early testing suggests that this can be done without a high level of IT capacity or expertise. Because the responsibility to update the clinical record lies with the patient, there is little activity required for maintenance of this practice. The practice does require that the patients and providers have access to the Internet and be willing to review the web based record and add information regarding their care for the patient. While the program is still evolving, the simple technology required for this practice could allow it to flourish in many different settings.

- **Controlling Access to Personal Health Information –** Controlling access to electronic medical information using extensive specifications of an individual's roles and functions is feasible. This type of system can offer a highly refined level of control over data access. When these controls are embedded into an Electronic Health Record they can limit access to information in sophisticated ways that would not be possible in a paper-based environment. Even in a highly automated environment, the adoption of these practices requires a commitment to careful implementation, ongoing maintenance, and routine audit activities. It is important to balance the need for appropriate access with protecting patient privacy and limiting access to those with a need-to-know.

- **Tracking Access to Personal Health Information --** Large institutions with electronic health records can implement audit trails that track both accesses and changes to records without degrading system performance. Addressing the use of an audit trail early in the system's development life cycle can simplify the implementation of this practice. Audit trails can be an important tool for identifying and investigating possible security incidents. The existence of an audit trail ensures that charges of privacy incidents can be investigated based on documented records and not rely solely on the word of one employee against another. Audit systems can also deter employees from inappropriately accessing information, because employees are aware their data access is being monitored. Audit trails must be coupled with effective reporting, investigation and follow-up, including sanctions if appropriate.

- **Authenticating Users of Personal Health Information** -- Both single sign-on and Public Key Infrastructure (PKI) can be implemented to enhance user authentication. Adoption of single sign-on has a greater chance of success when it is coupled with enhanced system capabilities, such as, computerized physician order entry. It is important that the single sign-on process be compatible with user workflow.

- **Training Users of Personal Health Information in Privacy and Security Policies and Practices --** Large institutions will be able to afford and justify the investment in web-based training for their workforce. They can also design and

implement training programs that address their specific policies and practices. Web-based training eliminates the need for distribution and installation of software on each workstation. Users of web-based training can access the training at their own convenience rather than having to attend a classroom training program with fixed schedules. Smaller institutions may be able to use generic web-based training programs. In these cases they will need to supplement the web-based training with education about their specific policies and practices. Web-based training may not be feasible for populations, , who are not users of the Internet.

- **Measuring Privacy and Security Performance** – Implementation of an annual review and updating of an organization's privacy and security compliance plan has the potential to reinforce that privacy and security are an ongoing organizational priorities rather than a one-time HIPAA compliance event. The use of a "dashboard" report can enable managers to routinely monitor their privacy performance. There may be opportunities for segments of the healthcare industry to come together to develop models and benchmarks of annual compliance plans and "dashboard" reports.

Lessons Learned

The practices discussed in this report share some common characteristics that can provide useful guidance to those seeking to establish high levels of security and privacy in their own organizations. These include:

- Adoption of an Electronic Health Record (EHR) can enable greater security and privacy than is possible in a paper-based record if these elements are built in to the application and fully implemented.

- Making privacy and security an upfront and integral part of adopting new information technology has the potential to decrease costs and increase the likelihood of successful implementation.

- The practices described in this report demonstrate that organizations adopting new healthcare information technology can achieve high levels of security and privacy.

- Coordination and commitment among internal and external stakeholders will enable organizations to agree on common policies and practices and take the steps necessary to implement them.

- Not all the practices in this report are readily scalable at this time. As information technology evolves and becomes more pervasive in healthcare, practices such as these may be realistic options for a broader range of organizations.

- Rigorous privacy and security practices enable sharing of clinical care information, public health data and research. These same security practices need not interfere with a clinician's access to the information needed to deliver patient care.

Within the context of an interconnected healthcare environment, the Working Group evaluated the following technical and organizational practices:

- Individual authentication of users
- Access controls
- Tracking of access and changes to records
- Protection of remote communications links and access
- Limited data sets
- Data use agreements
- Procedures for access to sensitive information in emergency situations
- Providing patients access to and ability to amend information
- Communication of privacy practices
- Organizational approaches to fostering privacy and security awareness

Background

The electronic medical record offers the promise of improved care and increased efficiency. Introducing information technology into health care creates new risks to privacy as well as new means to protect privacy Patients are well aware of the potential risks associated with the automation and sharing of their medical information. These concerns can lead patients to withhold from their clinicians information that could be crucial for their care. Clinician concerns about privacy and security can lead to exclusion of sensitive information from medical records reducing the value of the record to other clinicians treating the patient and to researchers and public health officials. This report brings the good and reassuring news that with conscious forethought and continuous care and attention, the use of information technology in healthcare can and should strengthen, not impair the security and privacy of personal health information.

Connecting for Health

Connecting for Health brings together participants from every stakeholder group in healthcare with interests in driving an interoperable healthcare system, including practicing clinicians, hospitals, employers and other third-party payers, federal and state government organizations, healthcare information technology suppliers, academic and research institutions, national standards groups, manufacturers, community organizations, and consumer groups.

This initiative intends to address the challenge of mobilizing information to improve the quality of care that is delivered to patients, conduct timely research to improve health outcomes, empower patients to become full participants in their care, and to bolster the public health infrastructure.

The purpose of Connecting for Health is to catalyze specific actions on a national basis that will rapidly clear the way for an interconnected, electronic health information infrastructure. The Collaborative plans to accomplish this by focusing on three key areas:

- Accelerating the rate of adoption of clinical data standards throughout the nation's healthcare system in order to facilitate interoperability.
- Identifying practical strategies and solutions for developing an interconnected electronic infrastructure that will ensure the secure and private transmission of medical information and support the continuity of personal health information across plans and providers.
- Actively working to understand what consumers will need and expect from an interconnected health information system and identifying key steps for meeting their needs.

Mission of the Privacy and Security Working Group

The Connecting for Health Privacy and Security Working Group took as its charge:

- Reaching consensus on a set of principles and criteria for assessing "noteworthy practices" for clinical and administrative data sharing and management

- Identifying examples of privacy and security "noteworthy practices" that are reasonable and practical in a variety of operational environments, are compliant with HIPAA, represent consumer concerns, and balance costs and benefits

- Promoting adoption of practices that data producers and data users can adapt to address privacy and security issues inherent in improving the delivery of healthcare, including quality, cost, access, and outcomes

To fulfill this mission the Privacy and Security Working Group sought out noteworthy privacy and security practices that are currently in use to show that creative solutions are both possible and affordable, and to disseminate them so they can serve as a model for others.

This Report

This report details the findings of the Privacy and Security Working Group. In order to identify practices that would best reflect the anticipated structure of an interconnected healthcare system, the Working Group focused its review on organizations and projects that currently are interconnected, i.e., share health information electronically with a variety of persons and entities and for a range of purposes. We looked at both large and small organizations and reviewed practices that span a wide range of costs to implement and supported a variety of healthcare functions.

The Working Group identified a number of organizations that have developed both technical and managerial practices that are noteworthy for the level of privacy and security they afford to health information that is maintained, used, and shared in an interconnected environment. These are practices that can be replicated today within reasonable fiscal constraints. We believe that these noteworthy practices may be useful to the healthcare industry as it develops approaches to ensuring the privacy and security of health information as it is held and shared among various sectors in the healthcare system.

Methodology

The goal of the Privacy and Security Working Group was to identify noteworthy practices that others can implement to further the development of an interconnected healthcare system the national health information infrastructure. The Working Group did not conduct a comprehensive survey of practices currently being utilized. Nor did the Working Group attempt to rank organizations on their privacy and security practices. Rather, the goal was to seek out and promote noteworthy privacy and security practices that are currently in use.

The Working Group identified a number of different challenges facing healthcare organizations, including:

- How do providers securely monitor patients electronically?
- How do you share patient care, public health monitoring and research data across enterprises?
- How do you securely allow patients and providers to communicate electronically?
- How do you screen emails for personal health information?
- How do you make medical records accessible for patients who do not have a regular source of care?
- How do you control access to personal health information?
- How do you track access to personal health information?
- How do you authenticate users of personal health information?
- How do you train users of personal health information in privacy and security policies and practices?
- How do you measure privacy and security performance?

Each noteworthy practice exhibited a subset of these fourteen principles:

- Trustworthy – can be relied on by patients to protect their health information
- Improve care for the patient – support the implementation of practices or programs that enhance quality of care
- Increase patient involvement – provide opportunities for the patient to understand and engage in their care and interact with the information about their health status and healthcare
- Enhance the healthcare relationship – enable communication between patients, healthcare organizations and clinicians
- Transparent – provide clear and complete information to patients about their methods and scope
- Interoperable – increase the access to information from independent healthcare systems
- User friendly – are easily understood and learned by the users
- Ubiquitous – apply to all data within the scope of the practice
- Scalable – could be adopted by organizations of differing size and complexity
- Sustainable – can be funded as part of ongoing operational budgets

- Enabled specific healthcare functions – allow patients, healthcare organizations and clinicians to participate in healthcare in ways that are not readily feasible without the use of private and secure information technology
- Enhance the ability to protect public health – support public health reporting and surveillance
- Improve the ability to measure, study, research – facilitate the creation of and access to data for research purposes
- Balance cost and risk – are seen by the implementing organizations as having sufficient value to justify their investment in the practice

Within the context of an interconnected healthcare environment, the Working Group evaluated the following technical and organizational practices:

- Individual authentication of users
- Access controls
- Tracking of access and changes to records
- Protection of remote communications links and access
- Providing patients access to and ability to amend information
- Communication of privacy practices
- Organizational approaches to fostering privacy and security awareness

We looked at a wide cross-section of organizations that utilize health information in a broad section of settings, across a broad range of activities, and that interact with a broad range of other organizations and individuals. We examined security and privacy practices in the following contexts.

- Emergency room
- Primary care or office-based care
- Primary care
- Integrated healthcare system
- Health plan
- Inpatient
- Community health centers
- e-health
- Public health
- Home care

Connected Activities & Purpose

We looked at functions that support a wide range of healthcare activities:

- Monitoring patients electronically
- Sharing patient care, public health monitoring, and research data across enterprises
- Patient Provider communication
- Securing e-mail for personal health information
- Making medical records accessible for patients who do not have a regular source of care

- Controlling access to Personal Health Information
- Tracking access to Personal Health Information
- Authenticating users of Personal Health Information
- Training users of Personal Health Information in privacy and security policies and practices
- Measuring privacy and security performance

The following sites were reviewed and are included in this report:

- **Visitantes Información Acceso (VIA)** – A project funded by HRSA Rural Communities Assistance to provide migrant farmers with email accounts and a web-based medical record. California Migrant Health
- **CareGroup Healthcare System**: CareGroup is an integrated delivery system serving Massachusetts. The system includes four hospitals with more than 1,000 beds, as well as specialty clinics and research facilities. CareGroup's not-for-profit Provider Service Network serves more than 400,000 managed-care patients.
- **IDEATel:** A four year demonstration project funded by CMS to provide home monitoring of 1500 diabetes patients in urban and rural New York State
- **Denver Health Hospital Authority**: A public integrated delivery system that includes a hospital, school and community clinics, a managed care program, and the 911 emergency response system.
- **Department of Veterans Affairs**: The Veterans Health Administration provides care to 4.3 million patients at 1300 care sites, including 170 hospitals and 800 outpatient clinics.
- **Henry Ford Health System**: Non-profit healthcare enterprise with $2 billion in revenues annually. They are Michigan's sixth larges provider with 5 hospitals and 2.5 million patient contacts
- **Humana**: A publicly traded health benefits company, with approximately 6.4 million medical members. Humana has contracts with 296,000 physicians and 3,700 hospitals in 44 states.
- **Kaiser Permanente of Northern California**: Kaiser Permanente is a nonprofit prepaid, group practice health maintenance organization (HMO), The Kaiser Permanente Northern California Region has almost 3.2 million members. It includes 4,451 physicians in The Permanente Medical Group (TPMG) and approximately 46,000 employees
- **Mayo Foundation**: A not-for-profit healthcare system with 4 hospitals, 3 clinics and a health system network. Mayo serves over 500,000 patients each year and has over 45,000 employees in Minnesota, Arizona, and Florida.
- **North Carolina Emergency Department Database**: A statewide repository of emergency department visit data
- **Palo Alto Medical Foundation**: A not-for-profit multi-specialty group practice with 246 providers, 1,200 employees providing over 800,000 patient visits per year.
- **Partners Health Care System**: A not-for-profit organization offering primary and specialist care, acute-care hospitals, and other services. Partners Community HealthCare, a physician network, encompasses 1,000 practitioners.

- **Indiana Network for Patient Care**: A community data sharing network under the auspices of the Regenstrief Institute
- **Montgomery County, Maryland Electronic Surveillance and Notification System**: A regional collaboration with Johns Hopkins University Applied Physics Laboratory. The project collects data from community hospitals, local pharmacies, public health agencies, schools, police, and fire departments.

Practices at these sites were identified as either noteworthy or promising. Noteworthy practices have been fully operational and can be considered to have a proven track record. Promising practices are those at the early stages of implementation but that may provide worthwhile new approaches to important privacy and security challenges.

Privacy and Security Practices by Site

Organization	Name of Project	Noteworthy	Promising
Visitantes Información Acceso (VIA)	VIA- Follow Me		Personal Health Page
CareGroup Healthcare System	Patient Site	Audit Trail Patient Provider Communication	
IDEATel	IDEATel	Patient Monitoring Communication PKI	
Denver Health Hospital Authority	Single Sign-on		Single Sign-on
Henry Ford Health System	Patient Website	Secure Patient/Provider Communication	
Humana	PHI Net	Web-Based Training	Lexicon Email
North Carolina Emergency Department Database	North Carolina Emergency Dept Database	ER Data Sharing Data use agreement Limited Data Set	
Palo Alto Medical Foundation		Role Based Access Control Break the Glass	
Partners Health Care System	Patient Gateway	Patient Access to Medical Records Policies	Reason for Access
Indiana Network for Patient Care	Indiana Network for Patient Care	Governance of Inter-Enterprise Data Sharing	
Department of Veterans Affairs	Policy Privacy Training	Web-Based Training	

Organization	Name of Project	Noteworthy	Promising
Kaiser Permanente of Northern California	Comprehensive Audit Trail	Audit Trail Training	
Mayo Foundation		Single Sign-on Break the Glass Web-Based Training	Privacy Dashboard
Montgomery County Electronic Surveillance and Notification System	National Capital Regional Surveillance Collaboration		Data Use Agreement Limited Data Set

Site Review Methods

The Privacy and Security Working Group has identified organizations that had developed technical and managerial practices that demonstrate the protection of privacy and security while making broad and creative uses of electronic health information. These organizations were identified through a review of literature and reports, as well as the extensive knowledge of the industry that exists across the members of the PSWG. The report is not intended to present a comprehensive survey of all organizations or all practices that address privacy and security in an interconnected healthcare environment.

Within each of these organizations we focused our review on specific privacy and security practices. We did not undertake a comprehensive review of each organization's overall approach to privacy and security. Our review of each organization's practices is based on interviews, analysis of documentation, examination of web sites, and review of published articles and reports. We did not conduct site visits.

The site review consisted of the following steps:

- Suggestions by work group members
- Initial screening by staff
- Compilation of profiles
- Work group consensus on sites to be reviewed
- Compilation of documentation
- Interviews
- On-line demonstrations
- In-person presentations
- Work group review of findings

Profiles of Noteworthy and Promising Practice Sites

Challenge: How Do Providers Securely Monitor Patients Electronically?

Monitoring the status of patients with chronic conditions, such as diabetes, often requires frequent office visits and at these visits the provider must rely on the patients to accurately report clinical readings such as glucose and blood pressure. Absent an office visit the provider may be unaware of important changes in the patient's health status.

Possible Solutions: Secure Patient Monitoring

Technology has developed to the point where patients are now able to transmit clinical information, such as blood pressure readings, from their homes to healthcare institutions. This allows clinicians to monitor the status of chronically ill patients quickly and efficiently. It also allows chronically ill patients to be monitored from their homes, rather then travel to the provider's office.

This project addresses HIPAA privacy requirements for access controls and HIPAA security requirements for information access management, access controls, transmission security, audit controls, and authentication.

In urban and rural New York State, the **Informatics for Diabetes Education and Telemedicine *IDEATel Project*** was developed to monitor the status of patients with diabetes from their homes. The project uses a PC-based Home Telemedicine Unit (HTU) that integrates a finger stick glucose and blood pressure monitors. The HTU can be connected to the Internet to upload results, view data, and send messages to the patient's case manager. Patients and diabetes case managers can communicate through a secure clinical email system as well as via video-conferencing.

IDEATel is a 4 year $28 million demonstration project funded by CMS involving 1666 Medicare beneficiaries with diabetes. It is a consortium including Columbia University, New York-Presbyterian Hospital, SUNY Upstate Medical University at Syracuse, and a number of other collaborating provider organizations. The project was intended to improve the health status of the enrolled patients. Currently, about 600 project specific patients are involved in the home monitoring. IDEATel has been up and running since January 2001. Patients enrolled in the program reside in either rural or urban federally designated medically underserved areas.

Securing the System

Results are automatically encrypted and transmitted over the Internet into the Columbia Web-based Clinical Information System (WebCIS) at New York Presbyterian Hospital and to the Siemens case management EMR. At the patient end the HTU provides Internet access,

video conferencing, and connects to the glucose and blood pressure reading devices. The following security controls are implemented:

- Authentication –Providers and researchers on-site must enter IDs and passwords. Providers outside of Columbia Presbyterian use a time-based token to authorize their access. Patients and case managers access the system using a PKI solution. A VPN supports remote access for researchers. The data is stored on a separate server that can only be accessed from specific IP addresses.
- Transport – 128 bit SSL encryption is used for transmissions from all sources. Video conferences utilize dedicated connections, but are not encrypted.
- Authorization/Access Control – Users are assigned to one of four levels of access that determine the patients and data that the user can access. Clinical data access is limited to specific patient lists.
- Auditing – Audit logs are maintained and routinely monitored. Designated patient data accesses require documentation of reason for each access.
- Physical Security – All servers are housed at a single site that is staffed 24 hours a day and has biometric access controls. Controls are in place to prevent the installation of unauthorized software.

The project employs the equivalent of one full time case manager for roughly 200 patients. In addition, the project has one-full time employee who serves as both network and security officer. Home Telemedicine Units (HTU) are installed and maintained by vendor staff (American Telecare). The cost of one HTU is approximately $3,000 - $4,000.

By embedding the PKI solution into the patient unit, the security is extremely user friendly. The mouse that is provided with the application is designed to provide the user with one-button access to each function that they use. Patient training focused on basic computer skills. Because they wanted the unit to be usable by patients with little or no previous computer experience and varying degrees of literacy and dexterity, function buttons are color-coded and all materials are at 6th grade reading level or less. They have also developed a Spanish language version of the software.

The Case Managers have full access to the system. Physicians use both paper and EMR access to the data. Physicians in outlying practices are using paper records. Internal Columbia users access the data through the Columbia EMR.

Security implementation spanned multiple vendors, requiring close collaboration among vendors to integrate their products with the system. In addition, multiple institutions and IRBs needed to sign off on the access and security model.

Because so many different groups were involved in the effort, meetings and conference calls involving the management team and key vendors were held weekly to track progress and address issues that developed during implementation.

Conclusions

Patient-provider messaging and remote monitoring of patient health status can be accomplished with full security and privacy protections. The secure patient monitoring program is an excellent example of using technology to monitor chronically ill patients. The use of this technology improves the communication between patient and clinician, and allows for the regular exchange of clinical data.

Challenge: How do you share patient care, public health monitoring and research data across enterprises?

Collaboration and sharing data across enterprises is critical for identifying and addressing public health issues. With a public health crisis, such as anthrax or SARS, it is critical that public health officials aggregate and evaluate clinical data on a community level. It is also important that the data be reported in a timely fashion, so that public health officials can address problems quickly. While most experts agree this practice is desirable, many healthcare communities struggle with the challenge of sharing data securely across enterprises. Enterprise policies and procedures can be a barrier. Implementation of the HIPAA privacy regulation has made many institutions cautious about participating in data sharing programs.

Possible Solutions:

In an effort to improve public health, several different communities across the country have created mechanisms for sharing data across different enterprises. In order to achieve this, some of these communities de-identify data to protect the privacy of patients. Other communities have created a governance structure to allow for this type of collaboration. In many instances where state laws or mandates do not apply, communities developed their own individual "data use agreements" to ensure the privacy of patients. In many states, public health reporting mechanisms can experience delays of up to a year. All of these organizations have focused on providing timely data, so that health officials can address problems quickly.

These projects address HIPAA privacy requirements for limited data sets, data use agreements, authorizations, and access controls. They address HIPAA security requirements for access management, access controls, transmission security, and authentication.

Institutions Addressing the Challenge

In central Indiana**, the Indiana Network for Patient Care (INPC)** is made up of competing independent institutions, which have set up a clear and specific governance structure that facilitates sharing data across enterprises. The providers count on each other to comply with agreements and privacy policies. Each provider in the network signs a

participant agreement. The agreement states, among other things, that if information from another institution is violated they are disciplined as though it were their own data. Every patient for whom data is shared also signs an authorization form for their data to be included in the system.

Currently, 3.5 million patients are included in the system. 25 different healthcare organizations are involved in the network at over 400 different locations. In many cases, these organizations can be considered competitors. One of the underlying concepts is that there is trust among the institutions. Each institution has a certain level of exposure by participating. Competing organizations agreed to work together under the premise that participants will receive better care in this environment.

The Process-- Records for each organization are stored in separate databases. The data that is input across the different entities differs, and is not all standardized. For example, ER presenting complaints are input differently at each institution. However, about 98% of the data is standardized; all radiology data, pharmaceutical and medication data and lab data are standardized.

The system relies on electronic messages from registration and appointment systems to convey authorization and to notify providers that the patient is under care. During registration, a staff person enters a verification that the patient has agreed to have their information included in the system. Some institutions cannot do this electronically. In these instances, they use a paper fax notice which is scanned and access is terminated for that specific encounter.

As an additional layer of protection, Indiana has laws that allow providers to seek medical information from other institutions and that allow institutions that are participating in an approved research project to treat their medical record as one.

Access to patient data is limited by device. ER devices in a specific hospital can access data only for patients in that ER. Each facility has a personal computers or device that has to be registered. When logging into the network, each device has to be individually authenticated. Psychiatric data is flagged. Only if the provider is from the source institution, then the provider can see it. Pharmaceuticals are deemed to be appropriate to share.

Implementing the Program -- Getting agreement among the different participants took nearly 2 years. During this time, Regenstrief acted as a neutral party and helped coordinate the efforts of the different groups. Building the technical infrastructure took 3 years. Implementation required project management, technical, and legal support.

Initially, funding was provided under an NLM grant. Currently, the network is sustained through a variety of sources. There is additional grant funding and money from ongoing research studies. The network is also supported by local foundations and industries. They are also experimenting and creating new economic models that will sustain it through user fees.

The Regenstrief Medical Record System was also employed. All of the major health systems in the project have now begun to move to automated patient records. It is difficult to know

whether this is a direct result of their participation or if the network indirectly "caused" this to happen.

Details among the different participants were hard to work out and differed by participant. Multi-institutional user identification software and coordination across IT departments is a constant challenge. Another challenge was making sure that the patient knows what they are agreeing to on the authorization. For the first 5 years the network excluded some sensitive data, such as, STD. They allowed people to gain experience with less sensitive data.

Although the data is encrypted during transmission, it is fully identifiable within the database. This allows treatment for patients to occur in a number of different facilities and settings. The wealth of data the network creates is an excellent source for hundreds of different research projects and public health monitoring. The system proved itself last year, when a public health crisis was averted. An outbreak of shigella was identified and dealt with in the early stages.

All clinical research goes through a rigorous IRB process. If proper approval is granted, any facility within the network can use the data for research purposes. The majority of patients authorize the network to use their data for research purposes. Less then 4% of the patient population refuses.

The **North Carolina Emergency Department Database (NCEDD)** has designed and is building a statewide database that extracts and collects emergency department (ED) data from participating hospitals' disparate and heterogeneous information systems. Because collection of the ED data is not mandated by state public health laws, a Data Use Agreement is created with each of the participating hospitals.

The hospitals report a number of data elements, including: chief complaint, ICD-9 codes, and vital signs. When monitoring for infectious diseases, such as SARS, NCEDD consults with clinicians to see how the patients might present. Based on clinical advice they identify the data and values to track. At the present time, such a report developed to monitor SARS produces 9 - 15 cases per day from one hospital's data. These cases are flagged for review by Division of Public Health personnel as potential SARS cases. The data also allow each participating hospital an immediate look at what is happening in their own emergency department.

At the current time, four hospitals representing three healthcare organizations are participating. Annual ED visits for the 4 currently participating hospitals total approximately 170,000 per year. They are working to expand to up to 20 hospitals by the end of 2003. CDC has been involved from the beginning. Users are within the state Division of Public Health and the participating hospitals. Plans are being made to add local and regional public health officials as users also. Generally, each hospital has public health, clinical and administrative users. No training is required for local hospital staff. Once the software is installed on the hospital's system, no work is necessary from participating hospitals other than maintaining open lines of communication with NCEDD.

Data are sent to NCEDD daily. Users can look at data, as recent as yesterday, when looking at reports. Clinical staff is actively involved in the process, because they want to use the data.

NCEDD has an Advisory Committee with representatives from each participating hospital as well as Division of Public Health and other potential user groups. An infectious disease workgroup composed of physicians and epidemiologists, has been established to help develop standard reports for public health surveillance. For example, SARS and gastroenteritis syndromic reports were recently created for public health surveillance.

There has been no immediate effect on clinical operations. By design, NCEDD has attempted NOT to change ED operations. However, use of NCEDD data may result in improvements to ED practice and administration.

The practice addresses HIPAA compliance by using a limited data set, and information on patients is de-identified. NCEDD also complies by offering a data use agreement.

Implementing the Program

NCEDD was conceived and developed by ED clinicians (MDs and RNs), public health researchers, medical informatics experts, and hospital IT experts brought together under the auspices of the North Carolina Healthcare Information and Communication Alliance (NCHICA). The front end technical piece took about 9 months. This included investigating technical requirements and options and development. NCEDD had a pilot that began fall of 1999, resulting in a prototype database in spring 2001. Database refinement and expansion has continued and the current working database with daily data uploads has been functional since November 2002. Initial demonstration costs were under $400,000 for three years (most funding was for personnel costs). They are currently undertaking rapid expansion throughout the state.

By design, NCEDD is trying to minimize the effect on operations at the participating hospitals. Each participating hospital must provide minimal space on a server within its network. Centrally, NCEDD's hardware consists of a database server, a FTP server, and a web server. These servers are located at a data hosting center in Research Triangle Park, NC. In addition, NCEDD provides each participating hospital with an inexpensive (under $100) software license for WS-FTP, a transmission tool used to securely encrypt, schedule and transmit the data using SSL and 128-bit encryption. NCEDD provides VB scripts for one-way hashing to de-identify records. The database is in SQL server. Web reports are currently provided via ASP scripting. Any browser with SSL can work with the web portal. The legal issues surrounding protected health information (PHI) called for a system that would de-identify the patient record prior to leaving the hospital's network but maintain update functionality and re-identification by public health officials during a crisis.

Participating hospitals are not required to commit anyone to NCEDD but are invited to provide a representative to the NCEDD Advisory Committee which meets quarterly. During implementation at the local hospital level, a small amount of time is needed from an IT representative to work with NCEDD staff. They also provide hospitals with a $5,000 incentive to help with start-up costs. Within NCEDD, the pilot project involved 1.5 FTEs. Currently, the rapid expansion phase of NCEDD is involving between 6 and 7 FTEs.

Initially NCEDD investigated and began a pilot using an integration model for real-time connectivity at the application level. Application level interfaces are complex and expensive to implement and not practical for disparate, heterogeneous system owned by various private entities. NCEDD discovered major issues using the application level model including:

- The vendors approach was not an open architecture and required investment in a risky proprietary system.
- Getting a hospital CIO s approval for connecting to a production system was highly unlikely.
- Maintenance of such a system was expensive and time consuming and most hospitals have limited resources to dedicate

Many of the data elements collected are entered into the hospital system days, and perhaps weeks later, than the actual patient's visit. As a result data are not available in real time. Near-real time collection provides most of the necessary functionality at a fraction of the cost.

A data level integration model that accomplishes near-real time data transmission is less expensive, complex, and invasive to hospital systems and is more practical to implement. The probability of a successful integration is much higher. Also, the one-way, hospital-initiated data transfer functionality using FTP in the data-level model was appealing since real-time synchronized transmission raises politically sensitive security issues as well as adding to complexity.

For these reasons, NCEDD chose a data-level integration model and distributed 3-tier architecture to meet the requirements for near-real time data collection at low costs to hospitals. The NCEDD model also implements a one-way hashing technique that de-identifies the record for patient privacy and implements security mechanisms that surpass HIPAA requirements.

Making the Program a Success -- While the project is covered by the public health authority of the State, participation is not mandated. HIPAA does not require organizations to participate. Due to misinformation about HIPAA regulations and state law, some organizations shy away from participating in important data sharing programs like NCEDD. Voluntary participation under public health authority is still troublesome to many. The development of a data use agreement under these circumstances has proven to be problematic. Hospitals have legitimate concerns from privacy and security officers about letting the data outside of the institution. However, the potential for cost savings through the good use of NCEDD data is an attractive benefit to many hospitals.

To ensure success, NCEDD has found it helpful to have a champion at each hospital, and provide ready access to do benchmarking comparisons to other participating hospitals. This access to their own local standardized data and aggregate data is a very important benefit to participating hospitals. The most important element of their success is perseverance and ongoing communications with all participants.

In Maryland, the Montgomery County Electronic Surveillance and Notification System is a regional collaborative effort among several public and private agencies: Community hospitals, local pharmacies, the Department of Health and Human Services (DHHS), Montgomery County Public Schools, private and parochial schools, the police, fire/rescue, sheriff departments and the Johns Hopkins University Applied Physics Laboratory. The coalition of organizations teamed up to create a secure electronic health alert and bio-terrorism surveillance system.

The state started requiring hospitals to manually report surveillance data in October 2001 with the Anthrax scare. Montgomery County is the first county in the state to automate the surveillance process with all of its county hospitals participating. The system currently collects and analyzes data from all hospital emergency rooms in the county, over the counter medication sales and physician visits. A web based application to track daily absentees of county public and private school students and county fire/rescue personnel is also being piloted.

Presenting complaints in all five hospital emergency rooms are collected using simple demographics. The system electronically queries the files at each institution, summarizes the data and generates a daily report of chief complaints. The data is then sent to a large database where there is automated analysis for special and temporal clustering patterns. The hospital de-identifies the data before submitting it and includes a coded unique identifier, for use by the county and state epidemiologist and hospital ICP. The identifying data is held internally at each hospital.

The information is collected in real time and reviewed at the beginning of each day by the Department of Health and Human Services public health epidemiologist and hospitals, so that an immediate response is possible when unusual cases/trends are observed.
If the public health epidemiologist spots a case that needs further investigation, the epidemiologist must present the coded unique identifier to the specific hospital to get more information. The DHHS public health epidemiologist also has access to other data sources, such as medication sales and physician visits in the county. All data is presented through a web-based GIS system interface to allow visualization of spatial distribution of health events. In addition to the GIS interface, patient data can be extracted for manipulation and other kinds of analysis.

Johns Hopkins University Applied Physics Laboratory (JHUAPL) is under contract with the state to automate the process in the county and elsewhere in a demonstration project. Therefore, hospitals have signed data use agreements with JHUAPL as the state contractor.

Implementing the Solution

The system has been in development since 9-11, and is still being improved upon.
The system consists of a web enabled GIS, central data system, data server, and a developed web based application. The county used in house, existing IT resources to create it. The county's application development is funded by the CDC and U.S. Department of Justice grants; participants also receive some technical assistance from the Johns Hopkins University Applied Physics Laboratory. Training for the system was minimal. The county received a grant to develop a web-based system for $125,000. Hardware for the private schools was approximately $75,000.

The system includes the participation of five competing community hospitals (Suburban, Holy Cross, Shady Grove Adventist, Washington Adventist and Montgomery General Hospitals). Participation was garnered through an established relationship among the hospitals and the health department, based on an emergency management planning committee. The Hospital/Public Health Committee has met for over ten years as part of the County's Emergency Management Group, being the only committee comprised primarily of

private sector entities, rather than government agencies. The trust relationships built on the committee provided the opportunity for the presentation and subsequent problem solving, cost sharing and willingness to set aside institutional barriers to participate as a group.

Preparing for Emergencies

Since 9-11, Montgomery County started designing and initiating implementation of an automated surveillance system to track indicators of disease trends and bio-terrorism in the county.

Because schools provide access to the largest population which can be tracked on a daily basis, and school absences may be sentinel for trends in the larger population, the county is implementing an enhancement which will provide daily reports of presenting problems of students visiting county school's health rooms. A web-based application is being tested which collects and reports student absentee data from the health room visits in public and private schools. Aggregate data will be transmitted electronically to the central data system and monitored and analyzed daily by the Montgomery County DHHS public health epidemiologist.

The system will also serve as a communication link between the agencies to convey and share public health alerts as well as health promotion and prevention information. It will alert public and private schools if there is a public health threat-- an outbreak in the community due to an emerging pathogen such as SARS or a bio terrorism event--and will provide information and guidance for school staff, students and parents. The application will also provide disease prevention and health promotion information to improve community outcomes, e.g., asthma management, diabetes, obesity, healthy food choices, and provide links to public health websites and other resources. The system provides complete capture of all hospital ER data.

Demonstrating Success

Montgomery County in collaboration with the Maryland Department of Health and Mental Hygiene conducted an exercise to test the capacity of the county surveillance system to provide data to assist in timely and effective response to a bio- terrorism event where a plague was released in the DC Metro System. Mock data collected from emergency rooms in five hospitals in the county was updated every four hours to simulate real time collection. The evaluation of the exercise showed that the reports generated by JHUAPL based on the mock data contributed to a greater understanding of the scope of the problem in terms of spatial distribution, new presentations in the population and the impact of the event on hospital systems and communication among the health department and emergency management agencies.

The county continues to track the system's performance by tracking timeliness, completeness, and the accuracy in coding algorithms. The County emphasizes that the system is helping them prepare for large scale public health events. The savings and benefits of the system will be demonstrated by their timely response----when they detect the next large scale public health events.

Conclusions

Despite the complex and competing interests of hospitals and the minimal resources available, there are successful models of data sharing among enterprises. By focusing on improving health outcomes, competitors have been willing to share information electronically. These organizations have voluntarily instituted data use agreements and ensured that direct identifiers are removed. Many of these projects are currently sustained by grant funding. They will need sustainable funding sources over the long term. Further research is needed to demonstrate the value of the projects for the participants. This may provide the basis for long-term funding by the participants themselves.

Challenge: How Do You Securely Allow Patients And Providers To Communicate Electronically?

Communicating timely, clinical information to patients about their personal health status is critical. Similarly, obtaining clinical information about a patient is critical to appropriate diagnosis and treatment. Healthcare institutions want to take advantage of the current technology to improve communications between patients and providers. However, many institutions are struggling to develop mechanisms to securely communicate clinical information through the Internet and protect patient privacy at the same time.

Possible Solutions: Patient-Provider Messaging

Several different healthcare systems are now offering electronic solutions that provide patients with a secure and private means to communicate with their providers. These organizations apply tight security and maintain strict access control in order to provide this service. In some institutions this service has helped to create an environment where improved communication has led to higher patient satisfaction.

These solutions address HIPAA privacy requirements for restricting access to PHI. HIPAA security requirements are also addressed for access controls, transmission security, and authentication

Institutions Addressing the Challenge

Henry Ford Health System in Michigan connects patients with their providers via their own personal web pages. Patients can create his/her own "*My Health*" page that allows patients to receive customized health information and a secure and private means to communicate with their physicians. Patients can schedule appointments, submit refill requests, and view lab results. The "My Health" pages are fully integrated into their online medical record, with both the inquiries from the patient and the outbound messages from the clinician are recorded in the online medical record.

Henry Ford has established a process to control access and protect information used in *My Health*. When a patient requests information, a message comes into an inbox in the

physician's offices. The message is in XML format with 128-bit encryption. The messages are then forwarded to providers with the patient's EHR attached so that the record can be reviewed as the provider responds to the patient's message. Responses from providers have a service level of 1-2 day response time. The web page records when the patient looks at their results.

At Henry Ford, there is good support from physician leadership, and medical directors are very supportive. The system tracks each message to confirm that there has been a response. The person who opens the message is responsible for the response. Nurses like the fact that the system allows them time to respond to messages when it is convenient, rather than answering calls as they are received.

In Massachusetts**, CareGroup Health System** is providing patients full electronic access to their medical records through the Internet on their *PatientSite* system. *PatientSite* has been up and running for 3 years. PatientSite provides secure messaging among patients, providers and office staff. Patients are able to securely view parts of their own clinical record and augment them. They can make requests to their providers via the web. With *Patient Site*, Patients get full electronic access to their medical records and can view security audits of their own medical record. Patient access to the system is via user name and password. Clinicians also use passwords, but while they are inside the virtual network they are required to additionally authenticate themselves using a Secure ID device. No clinical information is sent outside of PatientSite. When users have a new message waiting for them at Patient Site, a generic email is sent to their regular email account telling them they have a message waiting on PatientSite. Using PatientSite, patients can view medication lists, drug allergies, appointments, lab results (excluding HIV test results) and radiology results. By default, patient viewing of laboratory and radiology test results is turned off, but each physician can optionally turn this on for his or her panel of patients. CareGroup requires that providers respond to patient emails within 72 hours

Also in Massachusetts**, Partners HealthCare System** has created the *Patient Gateway,* which gives patients access to limited elements within their medical record and secure messaging with their doctor's office. Using *Patient Gateway,* patients can request a prescription renewal, request authorization of a referral, schedule or cancel appointments, and send messages to their doctor's office. Patients create their own personal profile by entering information about insurance, contact, pharmacy and other information. This allows *Patient Gateway* to automatically pre-fill forms for referrals and prescriptions. When a patient submits a request, it is automatically sent to their healthcare practice, with a copy stored in the patient's Gateway "sent messages" folder. If the practice responds, the message appears in the patient's inbox folder within *Patient Gateway*.

Patient Gateway includes information about healthcare provider's practices, including: directions to the office, contact numbers, a description of the types of services offered, and brief professional profiles of the healthcare providers in the practice. The *Patient Gateway* also provides reference information via access to the HealthWise® library. Illnesses and conditions, tests, drugs, and self-help organizations are all covered in this database.

Reported Benefits

These online methods of communication are reducing workload, decreasing the number of phone calls, and streamlining processes. These electronic messaging systems are more efficient in many cases, than the manual processes. For lab results, Henry Ford provides a 2 day turnaround time for a response and for Pharmacy requests they provide a 1 day turnaround. Their average response time is 16 hours. The system has the potential to automate processing for 802,000 Pharmacy calls and 300,000 lab calls per year. CareGroup reports that shared decision making and self review of drug/drug interactions has helped improve the quality of care. CareGroup has also seen a reduction in medical record pulls and copying. They have also reported an increase in patient satisfaction. At Partners, patients now access the web for information. Patients avoid making calls to the office, being placed on hold, or leaving phone messages and potentially missing returned calls. Patients can send information and requests via the computer at any time, and messages are promptly returned by office staff and/or their provider.

Securing These Systems

Henry Ford has designed their privacy and security practices to be compliant with both HIPAA privacy and security regulations. Each hospital has its own HIPAA privacy officer. Authentication is key to securing information for the Henry Ford program. When patients register to join the site, they must provide their demographic information and their medical record number. The system looks for various fields to verify authenticity, such as DOB, SSN, Medical Record Number, and other demographic information. If there is any question about the identity of the registrant, then a nurse follows up with the patient by phone and/or by mail. The system creates a user name and password and sends it to the patient through the U.S. Postal Service. Henry Ford also sends the patient a copy of their privacy policy and terms of use when the patient enrolls in the program. In addition, Henry Ford has daily backups of the online records and off-site disaster recovery sites. They have also been utilizing Business Associate agreements with their web partners to ensure confidentiality.

With the existence of the online medical record, the cost of implementing *My Health* at Henry Ford was around $300K. During implementation, Henry Ford brought key leaders from their medical centers to participate in a "train the trainer" session. They did about 5 or 10 sessions per medical office building to train staff and employees. To maintain the system, 1.5 FTEs are needed to verify the identity of individuals and to activate their accounts.

CareGroup developed their *PatientSite* system in only 6 Months. During implementation, they needed a team of 3 FTEs to rollout the program and support it. It took approximately one year to complete training and implementation for the program.

At Partners, they implemented a system based on the use of role-based access controls. The system rigorously tracks who accesses each account. For access to Patient Gateway, Patients are assigned a username and password. Patients can change their password at any time. All elements of the patient's medical record are secured at the site. Partners has account management within their de-centralized systems, audit trails, and "reason for access" processes whereby providers must verify the role and reason for access when accessing patient information. This does not prevent people from getting in, but does create

awareness that staff should access information only on a "need to know" basis. Employees can also perform a self-audit to see who has been accessing their information. Patients are notified of their privacy rights through Partners' "Notice of privacy practices".

Key Component: Online Medical Record

The common element in these three messaging programs is the existence of an online medical record. If another organization wanted to replicate this type of messaging system, they would need an electronic medical record.

At Henry Ford, they have a homegrown electronic medical record, with data feeds from 100 sources, all images, EKGs, labs, etc. Implementation was possible because Henry Ford had a good electronic medical record, in-house developers, and the basic email system was already developed, and in use.

The Partners program also benefited from existing online medical records. Implementation for this program did vary from hospital to hospital. Partners found that clinicians, who were already comfortable with the technology of CPOE, adapted more easily than those who were not.

Improved Patient Satisfaction

These programs resulted in improved satisfaction among patients. At Henry Ford, they provide surveys to receive feedback on the program and generate quarterly newsletters as a means of obtaining patient satisfaction. Patient satisfaction surveys at Henry Ford showed that 91% liked the system and 61% said it made a difference in their choice of provider. CareGroup has also seen a rise in patient satisfaction, reduced phones calls, and increased efficiency.

Conclusions

Secure email solutions are working well at a number of different institutions. However, the success of all of these projects has been a bi-product of the existence of an online medical record. These projects further emphasize the added benefit and value that can be derived from moving to an Electronic Health Record (EHR).

Challenge: How do you screen emails for Personal Health Information?

The use of email pervades both business and personal communication. Many healthcare organizations now provide their employees with individual email accounts. In this environment PHI can be transmitted via email to both appropriate and inappropriate recipients.

HIPAA requires that email containing personal health information (PHI) be transmitted securely. In order to comply with this requirement, healthcare organizations must either

apply encryption to all emails or have the means to screen unencrypted email for PHI and prevent its transmission.

Possible Solutions:

Technology and practices for screening the text content of email messages is emerging. Commercial products to enable the screening of emails for user specified terms or numeric patterns are entering the marketplace. Healthcare organizations are beginning to implement these products to enhance their control over email communication.

This project addresses HIPAA privacy requirements for access controls and HIPAA security requirements for access management, access controls, transmission security, and authentication.

Institutions Addressing the Challenge

Humana, a for profit health plan, is utilizing information technology to enable secure communications with health plan members, employer groups, physicians and other healthcare providers, and agents and brokers as well as other business partners. All Humana associates have access to email. As part of their job functions, many of Humana's associates must access PHI for Humana's 6.6 million members.

In 2002, to prepare for compliance with the HIPAA Privacy Regulation, Humana undertook an analysis of all outbound email content and found that about 1500 outbound email per day contained some type of personal health information. Managers at Humana realized that they would have to either block all email messages to external entities or find an automated solution for identifying email messages that might contain PHI.

Humana has created a secure web portal that allows members to access messages from Humana associates. Members must register on the portal and must use a personal ID and password in order to access their personal message center. When sending emails, Humana associates must select a secure mail option if the message is to be sent to the member's personal message center on the portal. If they do not select the "secure" option the email would be sent to a personal email address. The portal email method was selected to provide secure messaging without requiring that all senders and receivers have compatible encryption and decryption software.

If an email is sent without using the "secure" option, there is the possibility that PHI could be sent without appropriate security protections. In response to this challenge, Humana's approach is to scan all emails before they leave Humana's controlled environment. No email messages that contain PHI are to be delivered to a member's regular email address. Instead, members are notified that Humana has a message waiting for them at their Humana email message center. This helps to ensure that no PHI information is sent outside Humana unsecured. Rather, messages that contain PHI are placed in the members personal message center, for the member to access. The system automatically sends an alert email message to the member's regular email providing them with a link to their Humana personal message center, where the member can authenticate themselves and receive the message. Members may also send secure messages to Humana via their personal message center.

The filter or lexicon program looks for terms or numeric strings that indicate PHI may be included in the email. The master dictionary allows the user to specify terms and patterns of numbers, e.g., SSN, lab results that should be applied to outgoing email message including the message subject line, body of the message and any attachments. If the program detects specified text or numeric patterns, the email message is will be returned to the associate. All returned emails are logged and reports are generated for review by the Privacy & Security departments.

Humana is applying the scanning process to all email messages that are being sent via an unsecured format.Humana's email application allows associates to select the secure mail function when sending an email message. When an email with possible PHI is returned, the sender is instructed to resend the email with the "secure" setting.

Implementation of this capability is currently underway. The scanning software is integrated with Humana's routine email management processes. The service selected by Humana does have a standard health lexicon however, Humana staff has enhanced this lexicon, and expects to modify and refine it as they gain experience with the email screening process.

The service used by Humana can be scaled to different user environments. The lexicon software works in coordination with the security component and will allow the user to configure their own dictionary of terms and numeric patterns.

Conclusions:

The use of a lexicon to screen emails to protect patient privacy is a promising technology that is in use at some sites today and may be introduced by additional vendors. Products may emerge with pre-packaged lexicons. With additional competition, a broad range of users may find these applications affordable and easy to implement in a variety of environments. The screening lexicon may be useful for other healthcare applications, e.g., identifying records with specific chief complaint text. Standardization of terminology will enhance the value of a lexicon by reducing the error rate in records identified as meeting the specified criteria.

Challenge: How do you make medical records accessible for patients who do not have a regular source of care?

Patients with high mobility and no consistent source of medical care find that each new provider must ask them about their medical history, conditions, and treatments. Providers treating these patients are dependent on the patient's memory and knowledge of their conditions and treatments. Patients who do not have a regular source of care are especially at risk, as no institution is responsible for maintaining their record. Medical tests may be duplicated since the patient may forget (or not know) that a test was performed or where to get the results. Patients may not report all medications they are taking; possibly with serious consequences. In addition, some patients want direct access to their own medical records, *without* having to request it from a clinic, payer or provider. Worse yet, some physicians may

discard records when the statute of limitations from the last patient visit has passed. Therefore, there is a need to create a mechanism for individual patients to take control of and maintain their own medical record in a manner that is safe, secure and easily accessible.

Possible Solutions:

Technology has emerged that allows patients to control their own Web-based medical record. Non-profit organizations are offering this resource to transient populations and chronically ill patients. These solutions allow patients to own their medical record and allow healthcare institutions and clinicians to access and update their records whenever necessary.

This project addresses HIPAA privacy requirements for access controls and HIPAA security requirements for access management, access controls, transmission security, and authentication.

Institutions Addressing the Challenge

In California, **Medical Management Resources** (MMR) offers a bilingual version of its software application *FollowMe* to migrant farmer workers in Sonoma County. Many migrant workers in California have significant healthcare needs, including chronic medical conditions. Many of these workers rely on rural health clinics and Federally funded migrant clinics for their healthcare. Because they move around the healthcare system, there is no way to track their medical history, current health status or treatment plan including prescriptions. This population would not have the benefit of institution-based EHRs. The Visitantes Información Acceso (VIA) Program provides FollowMe to this mobile population of patients, allowing migrant workers to store their medical information online and access it via the Web.

Funded by an $80,000 grant from HRSA Rural Communities Assistance, Visitantes Información Acceso (VIA) establishes an email account and a secure Web-based archive for their medical record. This allows migrant workers to access their record from any location with Internet access. The VIA system does not require individuals to have an address.

Migrant workers subscribe to the service by filling out a form on the *FollowMe* Website. The application authenticates the individual. Workers can select a password and change it at any time. VIA email accounts and patient data are encrypted and stored separately on MMR's server. VIA makes immunization records, prescriptions, treatment plans, illnesses, allergies, physicians and contact information for the last clinic the patient visited instantly available. VIA does not make the information available to any third parties, including the INS.

Families enroll voluntarily in the program. In effect, the family "owns" their own website. The patient must give permission to enable a provider to access the information. Patients must notify their providers that their record is available online. Therefore, it is up to the family and their current provider to access and update their record. Providers can enter information on patients to the Web-based medical record, and other providers can then review the information on the patient—regardless of their location.

The software supports HIPAA regulatory requirements. Because the site is owned by the patient, the site is not considered a "covered entity" under current HIPAA regulations.

Although not considered a covered entity, VIA is still following an approach consistent with the HIPAA Privacy and Security regulations. In an effort to ensure confidentiality of patient information, they require all providers who access the system to sign a confidentiality agreement.

The *FollowMe* program is still evolving. An initial pilot with UC-Davis was completed in early in 2003. Currently, there are about 30 families enrolled. Medical records for the 30 families are included in the system. 200 additional slots exist for more families. A small number of physicians associated with the 30 families actively use the system.

As a result of the program, VIA has experienced many anecdotal positive experiences. For example, after enrolling in the program, a family was able to receive access and information about "healthy families" and was enrolled in the healthy family program on the same day. In other examples, VIA administrators have been able to step in and assist workers with hospital admission issues. The availability of an email account has enabled these migrant workers to have a consistent point of communication with their healthcare providers and insurance.

The project as it stands is funded through 2004 for Sonoma County. Currently, VIA is seeking additional grant and program dollars to expand over the next two years. MMR is planning to develop a regional or national collaborative that will enable them to roll VIA out on a large scale.

Conclusion

- **Making medical records accessible for patients who do not have a regular source of care –** The use of a web-based personal medical record is an accessible practice for both organizations and consumers. Once the record is set up, the patient controls the updates. Early testing suggests that this can be done without a high level of IT capacity or expertise. Because the responsibility to update the clinical record lies with the patient, there is little activity required for maintenance of this practice. The practice does require that the patients and providers have access to the Internet and be willing to review the web-based record and add information regarding their care for the patient. While the program is still evolving, the simple technology required for this practice could allow it to flourish in many different settings.

Challenge: How do you control access to Personal Health Information?

Controlling access to personal health information requires an organization to develop a careful balance between making available the information needed to provide quality clinical care, and ensuring that information is made available only to those with a need to access it.

In a paper chart, access control is managed by limiting where the record is available. If a provider or staff member has access to a paper chart, they can review all of the information it contains.

Possible Solutions:

In an electronic health record, access control can be refined to limit the data and patients each user can view or update. The refinement of these access privileges requires careful analysis and ongoing maintenance. Software can support the definition of access privileges for a large number of user categories and can control access to specific elements within a record.

To address the problem of not being able to predict the needs of clinicians in all situations override functions can allow access to records or data that are not within the users normal privileges. These overrides can be tracked and monitored.

Providers can also be required to document the reason for accessing a record. This can be particularly useful if the record is not for a patient for whom the provider has clinical responsibilities.

These projects address HIPAA privacy requirements for access controls and HIPAA security requirements for access management, access controls, and provisions for emergency access.

Institutions Addressing the Challenge

Access controls are commonly incorporated into many software applications. The value of these controls is in part determined by the extent to which they can be refined and the extent to which the using organization implements the full power of the controls. Access controls can be refined in several ways. User privileges can be defined based on the type of access: read, create, update, delete. Privileges can also be defined based on the application functions that a user has a right to access, e.g., a registration clerk may be limited to registration functions and excluded from lab functions. Functional privileges can be refined down to the level of a specific screen display within an application. An additional level of access control can be defined at the data field level. Users may be allowed to access a specific screen, but some data elements may be excluded from view. Finally, access may be limited to specific patient records or specific elements within a patient record. In this case the controls are driven by the values of a specific data type, e.g., positive HIV lab results, or restrictions requested by a patient or legally mandated for categories of patient information.

Not all software applications provide all of these access controls and even when they are available within a software application, users may find the implementation and maintenance of highly refined access privileges to be complex and cumbersome.

Palo Alto Medical Foundation has adopted an electronic health record (EHR) that uses role-based access control to help enforce its confidentiality policies. Using role-based access, they can control the types of information that employees and providers view and update. As part of their implementation of the EHR they developed an extensive matrix of access privileges or "security points". Each user role is assigned a set of access and update

privileges within the EHR according to the matrix. For example, only mental health providers can view mental health records.

For each role, access privileges are clearly defined---to the level of the screen display. Assigned roles determine the features that are available to an individual when he or she views something on the screen. Users are assigned to various levels of functionality with the information, such as "view only," "update" and or "order."

In addition to role-based access, Palo Alto Medical Foundation has implemented a special "break-the-glass" restriction within their EHR. Under specific circumstances, certain patient records may be designated for the "break the glass" restriction. If someone other than the patient's physician attempts to access the record of a restricted patient, an alert appears asking for the reason the record is being accessed and warning the user that the privacy officer will be sent a notification of access. The user can proceed to open the record, but he or she has in effect "broken the glass." This ensures that clinicians can access PHI that they need, while limiting general access to these records.

The Mayo Clinic EHR also has a "break the glass" function. At Mayo, the clinician determines when to employ this added security feature. For example, when a provider writes a clinical note or progress note, they can mark the note "confidential." Each "confidential" flagging creates a "break the glass" control on that segment of the record. If another clinician pulls up that record, a prompt appears that says "This note is marked confidential, please proceed at your own discretion." The clinician then needs to supply a reason that they need to access that information. The system allows clinicians to flag a specific patient or document. Mayo is investigating how to apply this flag to other portions of the record or a specific piece of data, such as, HIV results. Clinicians can access this restricted data using the "break the glass" function. Any access to the system is logged. Questionable accesses are referred to the appropriate department for review. The heaviest users of this feature are behavioral health clinicians.

Partners HealthCare has begun to implement a function that requires users to specify the reason for accessing a record. A pilot roll out of this capability highlighted the importance of minimizing the impact on work flow, offering a menu of pre-defined reasons for access, and not requiring access when a provider is known to be responsible for a patient's care. When fully implemented, Partners will be able to document and monitor the reason for each access to a patient PHI.

Conclusions

Controlling access to electronic medical information using extensive specifications of an individual's roles and functions is feasible. This type of system can offer a highly refined level of control over data access. When these controls are embedded into an Electronic Health Record they can limit access to information in sophisticated ways that would not be possible in a paper based environment. Even in a highly automated environment, the adoption of these practices requires a commitment to careful implementation, ongoing maintenance, and routine audit activities. It is important to balance the need for

appropriate access with protecting patient privacy and limiting access to those with a need-to-know.

Challenge: How do you track access to Personal Health Information?

Logging access and modification of patient records has been seen as complex, expensive, and a potential impediment to system performance. Audit trails of record creations and changes have been implemented to ensure recovery of data in the case of system failure. These audit trails did not always include information on the user who created or changed the record. Some software packages do not include the capability to track users who only access "read-only" views of PHI. These "look-ups" of patient records are often the source privacy breaches.

Possible Solutions:

Audit trails that track both accesses and updates of PHI by user can provide the means for detecting and investigating potential security breaches.

These projects address HIPAA privacy requirements for complaint investigation and HIPAA security requirements for audit controls.

Institutions Addressing the Challenge

Kaiser Permanente of Northern California undertook the development and implementation of a full audit trail in 1994 as part of its development of its clinical data repository. With its 3.2 million members, Kaiser had a large volume of data and users to manage. Its clinical data repository includes over 1 Terabyte of data. Their system tracks the activities of 16,000 users per day accessing over 140,000 unique medical records. The audit log tracks over 900,000 accesses per day. The size of the audit log is 1.2 GB per month. Yet, this tracking of accesses and updates has not caused any degradation in system performance.

The actual design of the log and the software to create it, were relatively simple. It did not require a significant investment in development or maintenance. This is in part a result of the audit log being developed and incorporated into the application at the outset. It was not an add-on or modification to an existing application.

The primary use of the audit log is to support the investigation of potential privacy breaches. Most investigations are a result of an employee report. Examples of items included in the audit log are logon ID, access date and time, terminal ID and subject category. When a patient registers a complaint about a possible privacy breach, the audit log can be used to generate a report that can be reviewed with the patient.. The generated report cites the different users and departments that accessed the patient's record. The Health Information Manager will review the report with the patient and explain the reasons for access by different departments. The log is examined to determine if a privacy breach has occurred. Kaiser in Northern California conducts 15-20 of these investigations per month. Half of the

investigations identify a privacy breach. One quarter of the investigations result in a termination. In addition to supporting investigations, the audit log has enabled Kaiser to analyze system performance and determine where adjustments should be made.

Kaiser has also developed a trending report that monitors the occurrence of privacy breaches and the actions taken. These reports are used to determine where to improve controls, training needs and management actions that should be taken. These reports track the number of reported breaches, investigations, and confirmed breaches.

CareGroup has made its audit log accessible to patients. The audit log is a standard library function called by all clinical systems. It records the time, place, person, system accesses and reason for access for every clinical transaction. Development of this capability took 6 months and implementation took one year. Through CareGroup's *PatientSite* application, patients can access their medical information, add to their medical records, send and receive email, access drug interaction references, and review an audit trail of who has accessed their record and the information that was accessed. Employees can also view these audits through the web portal and view their own audit trails. CareGroup monitors these audits to identify any inappropriate access taken by employees. This has resulted in 2-3 terminations each year for inappropriate access by employees.

Conclusions

Large institutions with electronic health records can implement audit trails that track both accesses and changes to records without degrading system performance. Addressing the use of an audit trail early in the system's development life cycle can simplify the implementation of this practice. Audit trails can be an important tool for identifying and investigating possible security incidents. The existence of an audit trail ensures that charges of privacy incidents can be investigated based on documented records and not rely solely on the word of one employee against another. Audit systems can also deter employees from inappropriately accessing information, because employees are aware their data access is being monitored. Audit trails must be coupled with effective reporting, investigation and follow-up, including sanctions if appropriate.

Challenge: How do you authenticate users of Personal Health Information?

User authentication across multiple applications can require the entry of different user IDs and passwords for each application. User IDs and passwords can be shared and cause potential breaches in security.

Possible Solutions:

User authentication across applications can be simplified with the adoption of a single sign-on process. The single sign-on is accomplished through the use of a hardware token that the user must place in a reader linked with the device they are using. The hardware token can

have ever changing passwords that are recognized by the receiving application, but are not useful beyond their limited period of validity. This prevents users from exchanging passwords associated with the token. In addition to the token, the user will also have a personal password that they enter manually.

Public Key Infrastructure (PKI) is another form of secure authentication for remote users. Each user is issued a digital certificate to them and their device. The user password and certificate must match and be recognized by the system in order to obtain access to an application or data.

These projects address HIPAA privacy requirements for access controls and HIPAA security requirements for access management, access controls, and authentication.

Institutions Addressing the Challenge

Denver Health is in the process of implementing single sign-on. Denver Health has an EHR that integrates seven different applications. Prior to the adoption of single sign-on users would have to sign-on separately to each of the seven applications. When a new facility was getting ready to open, Denver Health took the opportunity to introduce single sign-on with the use of hardware smart cards. They also selected this facility, because the clinicians had some experience with using computers for patient results viewing. It was hoped, that the computer experience of clinicians, would make them more comfortable with the single sign-on process. Subsequent clinics are receiving the single sign-on solution as part of either a CPOE project or as clinics transition to a "chartless" environment.

Each device in the facility is equipped with a smart card reader. When a clinician enters the exam room they place their smart card in the reader and after entering a single password they are given access to all authorized applications. The single-sign-on includes applications for lab results, dictations, patient immunization registry, women's care database, patient clinical results from an electronic lifetime clinical record, hospital mainframe patient management system, and medical record imaging.

During the initial implementation, Denver Health found that the time for the applications to recognize the smart card and provide access to the applications was too long. The log-on process time is determined by a number of components, including: card recognition, authorization, logging onto the workstation, scanning for viruses, logging onto personal portal applications, and launching applications within the personal portal system. This disrupted the provider's workflow and caused dissatisfaction. Denver modified their access programs to get the log-on time down to a range from 20 – 45 seconds. They are continuing to work on reducing this response time.

The IDEATel project uses both a hardware token and PKI. Mobile clinicians are issued a time-based hardware token. The token along with the user's password allows access to both the Columbia Presbyterian Medical Center EHR and the case management applications. Patient access is based on Public Key Infrastructure (PKI). Unique PKI certificates are issued by a vendor to each patient. The patient certificate is pre-loaded on the home monitoring unit prior to installation. Certificates are monitored through standard functionality in

commercial software. In order to access the web the patient must initiate access from their home monitoring unit and enter their password. The same PKI authentication is applied to the case managers when they access the case management website.

Conclusions

Both single sign-on and Public Key Infrastructure (PKI) can be implemented to enhance user authentication. Adoption of single sign-on has a greater chance of success when it is coupled with enhanced system capabilities, such as, computerized physician order entry. It is important that the single sign-on process be compatible with user work flow.

Challenge: How do you train users of Personal Health Information in privacy and security policies and practices?

Both initial and ongoing training have been one of the major challenges of implementing HIPAA privacy and security regulations. Providers of all types and sizes must train employees, students, and volunteers in their privacy policies and practices. During the initial HIPAA implementation, this was a significant undertaking for many organizations. Training new employees and providing refresher training for existing staff must be addressed by all entities covered by HIPAA.

Possible Solutions:

Internet based distance learning has become established as an effective means of delivering training and education to large numbers of people. Web-based training is independent of location and can be accessed at any time. It also allows the user to move at their own pace. Using web-based training programs standardizes both the content and presentation of the training components. Web-based training eliminates costs associated with sending trainers to sites or employee travel to training programs.

These projects address HIPAA privacy and security requirements for training.

Institutions Addressing the Challenge

The **Department of Veterans Affairs** is required to train the 300,000 members of its workforce in its privacy policy and practices. The VA workforce includes employees, medical students, and volunteers. To meet this need the VA developed and implemented a web-based training program.

The training was developed in a three month timeframe and required one month for implementation. A contractor was used to develop the training. Approximately 7 FTEs were involved during the development and implementation phases. Training began on January 22, 2003. By April 14, 2003 the entire VA workforce was trained.

The training program consists of 7 modules: Privacy and release of information, Veteran's rights, uses of information within the VA, purposes requiring authorization, release of

information outside of VA, operational privacy requirements, Freedom of Information Act. Users can start and stop the training process when convenient. If a user stops the training, the system will return them to where they left off. The average time to complete the training is 45 minutes for all 7 modules. A separate optional Q&A component requires an additional 30 minutes.

The current training package covers all privacy policies and practices. It is not tailored to the roles of different employees. The VA intends to develop a role-based version of their training in future releases. The training module generates management reports that enable each VA facility to track who has been trained. These reports were used to ensure that training was completed by the HIPAA deadline.

One key lesson learned by the VA was that its volunteers were not experienced computer users. As a result they were not able to use the web-based training program. A separate classroom based training program was designed and implemented for the VA volunteers.

Humana Also implemented role based training. The training was tailored to different departments; this was one of the biggest challenges of the training. All employees received a general overview, and then specific information about how the privacy policies pertained to their area. The majority of their training for their 13,000 associates was completed on-line. They were able to automatically track which employees took the training, and provide regular reports back to the managers. They developed the training so that it could occur within one hour. Humana developed all of the content for the training in 3 months. It took 2 IT associates to set up the management process to deliver content to the users. All staff was able to use the intranet based training.

Conclusions

Large institutions will be able to afford and justify the investment in web-based training for their workforce. They can also design and implement training programs that address their specific policies and practices. Web-based training eliminates the need for distribution and installation of software on each work station. Users of web-based training can access the training at their own convenience rather than having to attend a classroom training program with fixed schedules. Smaller institutions may be able to use generic web-based training programs. In these cases they will need to supplement the web-based training with education about their specific policies and practices. Web-based training may not be feasible for populations who are not users of the Internet.

Challenge: How do you measure privacy and security performance?

Healthcare organizations have been immersed in meeting the immediate requirements of HIPAA privacy and security requirements. Modifying current operations and enhancing information technology have been the major focus of security and privacy efforts. As compliance with HIPAA requirements becomes routine, healthcare organizations can turn their attention to monitoring the results of their privacy and security practices.

Possible Solutions:

"Dashboard" reports for performance measurement have become tools in many areas of healthcare, such as, quality, utilization, staffing, and finances. "Dashboard" reports track key indicators to enable managers to quickly identify trends and areas needing further analysis and possibly correction. Providing managers with a privacy and security "dashboard" report could enable and organization to continuously monitor the effectiveness of their training, practices, policies, and technology. This would ensure that problems are identified as early as possible and that corrective action is taken in a timely manner.

This project goes beyond the HIPAA privacy and security requirements.

Institutions Addressing the Challenge

Mayo is in the process of developing an annual Privacy Compliance Workplan. The Workplan would encompass an assessment of current policy, current practices, patient complaints and compliments and other Privacy related legal requirements. Based on the plan, data will be reported for each Mayo site and aggregated into organization-wide report. An element of the plan is the privacy compliance "dashboard". The dashboard will be composed of standard tracking of data that could indicate potential breaches or gaps. Among other things, these would include unusual variances in the frequency of accessing certain data.

Mayo expects that the performance reporting will enable them to identify potential breaches, determine areas where additional training is needed, and highlight needed modifications to their policies and practices.

Conclusions

Implementation of an annual review and updating of an organization's privacy and security compliance plan has the potential to reinforce that privacy and security are ongoing organizational priorities rather than a one-time HIPAA compliance event. The use of a "dashboard" report can enable managers to routinely monitor their privacy performance. There may be opportunities for segments of the healthcare industry to come together to develop models and benchmarks of annual compliance plans and "dashboard" reports.

Lessons Learned

Conclusions from Noteworthy and Promising Practices

The set of practices presented in this report provide lessons specific to each practice and broader lessons about the potential for healthcare organizations to advance an interconnected health care system and maintain a high level of privacy and security.

- **Monitoring Patients Electronically –** Patient-provider messaging and remote monitoring of patient health status can be accomplished with full security and privacy protections. The secure patient monitoring program is an excellent example of using technology to monitor chronically ill patients. The use of this technology improves the communication between patient and clinician and allows for the regular exchange of clinical data.

- **Sharing patient care, public health monitoring and research data across enterprises --** Despite the complex and competing interests of hospitals and the minimal resources available, there are successful models of data sharing among enterprises. By focusing on improving health outcomes, competitors have been willing to share information electronically. These organizations have voluntarily instituted data use agreements and ensured that direct identifiers are removed. Many of these projects are currently sustained by grant funding. They will need sustainable funding sources over the long term. Further research is needed to demonstrate the value of the projects for the participants. This may provide the basis for long-term funding by the participants themselves.

- **Patient Provider Communications --** Secure email solutions are working well at a number of different institutions. However, the success of all of these projects has been a bi-product of the existence of an online medical record. These projects further emphasize the added benefit and value that can be derived from moving to an Electronic Health Record (EHR).

- **Screening email for personal health information** – The use of a lexicon to screen emails to protect patient privacy is a promising technology that is in use at some sites today may be introduced by additional vendors. Products may emerge with pre-packaged lexicons. With additional competition, a broad range of users may find these applications affordable and easy to implement in a variety of environments. The screening lexicon may be useful for other healthcare applications, e.g., identifying records with specific chief complaint text. Standardization of terminology will enhance the value of a lexicon by reducing the error rate in records identified as meeting the specified criteria.

- **Making medical records accessible for patients who do not have a regular source of care –** The use of a web-based personal medical record is an accessible practice for both organizations and consumers. Once the record is

set up, the patient controls the updates. Early testing suggests that this can be done without a high level of IT capacity or expertise. Because the responsibility to update the clinical record lies with the patient, there is little activity required for maintenance of this practice. The practice does require that the patients and providers have access to the Internet and be willing to review the web based record and add information regarding their care for the patient. While the program is still evolving, the simple technology required for this practice could allow it to flourish in many different settings.

- **Controlling access to Personal Health Information –** Controlling access to electronic medical information using extensive specifications of an individual's roles and functions is feasible. This type of system can offer a highly refined level of control over data access. When these controls are embedded into an Electronic Health Record they can limit access to information in sophisticated ways that would not be possible in a paper based environment. Even in a highly automated environment, the adoption of these practices requires a commitment to careful implementation, ongoing maintenance, and routine audit activities. It is important to balance the need for appropriate access with protecting patient privacy and limiting access to those with a need-to-know.

- **Tracking access to Personal Health Information --** Large institutions with electronic health records can implement audit trails that track both accesses and changes to records without degrading system performance. Addressing the use of an audit trail early in the system's development life cycle can simplify the implementation of this practice. Audit trails can be an important tool for identifying and investigating possible security incidents. The existence of an audit trail ensures that charges of privacy incidents can be investigated based on documented records and not rely solely on the word of one employee against another. Audit systems can also deter employees from inappropriately accessing information, because employees are aware their data access is being monitored. Audit trails must be coupled with effective reporting, investigation and follow-up, including sanctions if appropriate.

- **Authenticating users of Personal Health Information** -- Both single sign-on and Public Key Infrastructure (PKI) can be implemented to enhance user authentication. Adoption of single sign-on has a greater chance of success when it is coupled with enhanced system capabilities, such as, computerized physician order entry. It is important that the single sign-on process be compatible with user work flow.

- **Training users of Personal Health Information in privacy and security policies and practices --** Large institutions will be able to afford and justify the investment in web-based training for their workforce. They can also design and implement training programs that address their specific policies and practices. Web-based training eliminates the need for distribution and installation of software on each work station. Users of web-based training can access the training at their own convenience rather than having to attend a classroom training program with fixed schedules. Smaller institutions may be able to use generic web-based training programs. In these cases they will need to

supplement the web-based training with education about their specific policies and practices. Web-based training may not be feasible for populations, , who are not users of the Internet.

- **Measuring privacy and security performance** – Implementation of an annual review and updating of an organization's privacy and security compliance plan has the potential to reinforce that privacy and security are an ongoing organizational priorities rather than a one-time HIPAA compliance event. The use of a "dashboard" report can enable managers to routinely monitor their privacy performance. There may be opportunities for segments of the healthcare industry to come together to develop models and benchmarks of annual compliance plans and "dashboard" reports.

Lessons Learned

The practices discussed in this report share some common characteristics that can provide useful guidance to those seeking to establish high levels of security and privacy in their own organizations. These include:

- Adoption of an Electronic Health Record (EHR) can enable greater security and privacy than is possible in a paper-based record if these elements are built in to the application and fully implemented.

- Making privacy and security an upfront and integral part of adopting new information technology has the potential to decrease costs and increase the likelihood of successful implementation.

- The practices described in this report demonstrate that organizations adopting new healthcare information technology can achieve high levels of security and privacy.

- Coordination and commitment among internal and external stakeholders will enable organizations to agree on common policies and practices and take the steps necessary to implement them.

- Not all the practices in this report are readily scalable at this time. As information technology evolves and becomes more pervasive in healthcare, practices such as these may be realistic options for a broader range of organizations.

- Rigorous privacy and security practices enable sharing of clinical care information, public health data and research. These same security practices need not interfere with a clinician's access to the information needed to deliver patient care.

Acknowledgements

This report would not have been possible without the willingness, dedication and enthusiasm of many people. We owe special thanks to our Working Group members, and the staff that supported them.

Members of the Privacy and Security Working Group

Holt Anderson, Executive Director, North Carolina Healthcare Information & Communications Alliance, Inc.

Kirk C. Bailey, CISSP, Chief Information Security Officer, The City of Seattle; Manager of Strategic Computer Security Services University of Washington

Peter Basch, M.D., Medical Director, e-Health Initiatives, MedStar Health

William Braithwaite, M.D., Manager, Health Policy Department, PricewaterhouseCoopers

Paul D. Clayton, Ph.D., Chief Medical Informatics Officer, Intermountain Health Care

Ted Cooper, M.D., National Director of Confidentiality and Security, Kaiser Permanente

Jill Callahan Dennis, J.D., RHIA, Principal, Health Risk Advantage; Advisory Board Member, Journal of American Health Information Management Association

Lisa Gallager, Vice President of Information and Technology, URAC

Janlori Goldman, J.D., Director, Health Privacy Project, Georgetown University

Gail Graham, RHIA, Director, Health Informatics, Office of Information, U.S. Department of Veterans Affairs

Richard K. Harding, M.D., Professor of Clinical Psychiatry and Pediatrics/Vice Chair of Clinical Services, University of South Carolina

Captain Brian Kelly, M.D., MBA, Director, E-Business, Policy & Standards Information Management, Technology & Reengineering, TRICARE Management Activity, U.S. Department of Defense

Judith B. Krauss, MSN, R.N., Professor, School of Nursing, Yale University

Steve Lazarus, Ph.D., President, Boundary Information Group, Past Chair, Workgroup for Electronic Data Interchange (WEDI)

Bernard Lo, M.D., Director, Program in Medical Ethics, University of California San Francisco

Roger Meyer, M.D., Senior Consultant on Clinical Research, Association of American Medical Colleges

Thomas H. Murray, Ph.D., (Chair of Working Group), President, The Hastings Center

Kevin N. Nicholson, R.Ph., J.D., Director, Pharmacy Regulatory Affairs, National Association of Chain

Drug Stores

Robin K. Omata, J.D., Ph.D., Chief Privacy Officer, United Health Technologies

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

Elliot M. Stone, MUA, Executive Director, Massachusetts Health Data Consortium

John E. Wennberg M.D., Director, Center for Evaluative Clinical Sciences, Dartmouth Medical School

Staff

Jennifer Covich Bordenick, M.A., eHealth Initiative and Foundation

Virginia Riehl, Independent Consultant

In the early phases of this project staff support was provided by:

Joy Pritts, Assistant Research Professor, Health Policy institute, Georgetown University

Joanne Hustead, Senior counsel, Health Privacy Project

Angela Choy, Field Director, Health Privacy Project

APPENDIX

Information about Practice Sites

For additional information on the projects and practices described in this report, please contact the institutions directly.

Organization	Name of Project	For More Information
Visitantes Información Acceso (VIA)	VIA- Follow Me	http://www.followme.com
CareGroup Healthcare System	Patient Site	http://www.caregroup.org/
IDEATel	IDEATel	www.ideatel.org
Denver Health Hospital Authority	Single Sign-on	www.denverhealth.org andy.steele@dhha.org
Henry Ford Health System	Patient Website	http://www.henryfordhealth.org
Humana	PHI Net	privacyoffice@humana.com
North Carolina Emergency Department Database	North Carolina Emergency Dept Database	www.ncedd.org
Palo Alto Medical Foundation		www.pamf.org
Partners Health Care System	Patient Gateway	http://www.patientgateway.org/
Indiana Network for Patient Care	Indiana Network for Patient Care	www.inpc.org
Department of Veterans Affairs	Policy Privacy Training	http://www.va.gov/publ/direc/health/notice/ib10-163.pdf http://www.va.gov/publ/direc/health/notice/ib10-163lp.pdf .
Kaiser Permanente of Northern California	Comprehensive Audit Trail	ted.cooper@kp.org
Mayo Foundation		www.mayo.edu http://www.mayoclinic.org/contact/

Organization	Name of Project	For More Information
Montgomery County Electronic Surveillance and Notification System	National Capital Regional Surveillance Collaboration	Lynn L. Frank, FACHE Chief, Public Health Services Montgomery County Department of Health and Human Services 401 Hungerford Drive Rockville, Maryland 20850 240 -777- 3860

List of Interview Questions

Background & Description of policy/practice

1. Name of project/practice?
2. What is distinctive about the practice/policy?
3. What specific type of information is protected?
4. How specifically does the practice policy improve privacy or security in the organizations?
5. What is the scope of the implementation?
    a. How many users?
    b. Number of records included?
6. What types of individuals developed the practice/policy? Clinicians? Technology experts? Compliance officers?

Timeframe

7. What is the timeline for development?
    a. Length of time it took to develop
    b. Length of time it took to implement (training, etc.)
    c. How long has it been up and running?

Implementation Requirements

8. What requirements were necessary to implement the practice/policy?
    a. Hardware?
    b. Software?
    c. Consultant or Expert work?
    d. Employees required to get it up and running?

User Acceptance

9. What is the level of awareness about the policy/practice?
    a. Are patients aware of the policy/practice?
    b. Are clinicians aware of the policy/practice?
    c. How was it communicated to them?
10. How user friendly is the practice/policy?
    a. Was extensive training required?

Benefits

11. Are there benefits to the patient as a result of the practice/policy?
12. Has the practice or policy had an impact on clinical research?
13. How did the practice change operations.?
14. How does the practice/policy address HIPAA Compliance?
    a. Does it go beyond the scope of HIPAA requirements?
15. Is Quality of care directly or indirectly affected by the practice/policy?
16. Have any savings been recognized as a result of this practice/policy?
17. How does the organization measure the success of the practice/policy?
18. Have any performance measures been used to assess the success?

Risks and Costs

19. What types of risks are associated with implementing this policy/practice?
20. What types of costs are associated with this practice? (i.e., Is this a simple enhancement of software or an overhaul of the existing systems?)
    a. Time and labor of employees?
    b. Training costs?
    c. Hardware/software costs?
21. How has the practice/policy affected the daily operations of the organization? What has been the impact of implementation?
    a. Positive Effects?
    b. Negative Effects?
22. What have been the most difficult challenges to overcome in the following areas? Why?
    a. Policy
    b. Technology
    c. Legal
    d. Other
    e. How did/are you overcoming these challenges?

Transferability

23. Is the organization already sharing its policies and practices with other related organizations in its community?
    a. How willing are you to share information with other healthcare organizations?
    b. Are there materials from your project that could be made available through the Connecting for Health web site?
24. Following the release of the report, other organizations may want to find out more about the policy/practice. Is there a website, document or individual whom we could direct individuals to—if they want more information?

Post Interview

25. What types of institutions and settings could benefit from this policy/practice?

26. How practical is the policy/practice—could it be easily replicated at other organizations?
27. What requirements are necessary to replicate this practice/policy?
28. Length of time for development- Is the work of the exemplary site transferable? Will it help decrease development time for other organizations? (For example, mapping access privileges—could other organizations use the same work over again?)
29. After analyzing the practice/policy, can you think of other methods, types of institutions or systems that could benefit from it?
30. Could the practice/policy be applied differently that may make it more effective?
31. Is there some type of visual that could be incorporated into the final report to help explain the practice? (i.e,. a picture from their web-page, timeline, table, chart, etc.)
32. To what extent does the practice exhibit the characteristics identified by the PSWG?
    a. Trustworthy
    b. Scalable
    c. Balance of costs and risks
    d. Sustainable
    e. Interoperable
    f. Transparent
    g. User friendly
    h. Ubiquitous
    i. Enablers important healthcare capabilities