

Minnesota Health Records Access Study Report to the Minnesota Legislature

Minnesota Department of Health
February 2013



Division of Health Policy
Office of Health Information Technology
PO Box 64882
St. Paul, MN 55164-0882
651-201-3662
www.health.state.mn.us/e-health

As required by Minnesota Statutes, Section 3.197, this report cost approximately \$119,953.00 to prepare, including staff time, printing and mailing expenses.

Upon request, this material will be made available in an alternative format such as large print, Braille, or digital audio.

Printed on recycled paper.



Protecting, maintaining and improving the health of all Minnesotans

February 19, 2013

The Honorable Tony Lourey
Chair, Health and Human Services Finance Division
Minnesota Senate
Room 120, State Capitol
75 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155-1606

The Honorable Tom Huntley
Chair, Health and Human Services Finance Committee
Minnesota House of Representatives
585 State Office Building
100 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155-1606

The Honorable Kathy Sheran
Chair, Health, Human Services and Housing Committee
Minnesota Senate
Room 120, State Capitol
75 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155-1606

The Honorable Tina Liebling
Chair, Health and Human Services Policy Committee
Minnesota House of Representatives
367 State Office Building
100 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155-1606

To the Honorable Chairs:

As required by Minnesota Laws 2012, Regular Session, Chapter 247, Article 2, and Section 10, this report outlines findings from a Health Records Access Study conducted by the Minnesota Department of Health, in consultation with the Minnesota e-Health Advisory Committee, on the following topics raised by the Legislature during the 2012 session:

- (1) The extent to which providers have audit procedures in place to monitor use of representation of consent and unauthorized access to a patient's health records in violation of Minnesota Statutes, sections 144.291 to 144.297;
- (2) The feasibility of informing patients if an intentional, unauthorized access of their health records occurs; and
- (3) The feasibility of providing patients with a copy of a provider's audit log showing who has accessed their health records.

The Minnesota Health Records Access Study is unique in the nation by evaluating these three topics, which are regulated by both state and federal law. These topics influence the management of protected health information and are fundamental safeguards to ensure sound electronic health information security practices.

Minnesota has long supported protecting patients' privacy while leveraging the benefits of new technology to ensure that health information follows the patient across the health care continuum. The enclosed study findings and recommendations address some of the policies, procedures, and technical requirements that are needed to foster patient trust and enable meaningful health information exchange.

Sincerely,

A handwritten signature in black ink, appearing to read "Edward P. Ehlinger".

Edward P. Ehlinger, M.D., M.S.P.H.
Commissioner
P.O. Box 64975
St. Paul, MN 55164-0975

Acknowledgements

The Minnesota Department of Health thanks the many members of the Minnesota e-Health Advisory Committee and workgroups for their time, leadership and expertise in consulting with MDH to design and complete the Minnesota Health Records Access Study.

Minnesota e-Health Advisory Committee Co-Chairs

Bobbie McAdam
Advisory Committee Co-Chair
Senior Director, Business Integration
Medica

Marty Witrak, PhD, RN
Advisory Committee Co-Chair
Professor, Dean
School of Nursing, College of St. Scholastica

Minnesota e-Health Privacy and Security Workgroup Co-Chairs

Laurie Beyer-Kropuenske, JD
Director, Information Policy Analysis Division
Minnesota Department of Administration

LaVonne Wieland, RHIA, CHP
System Director Compliance & Privacy Compliance
HealthEast Care System

A full list of Minnesota e-Health Advisory Committee members and alternates is available in Appendix G.

Other Advisors and Project Support

M. Kate Chaffee, Esq., Chaffee Law

Ralph Brown, Management Analysis & Development Division, Minnesota Management & Budget

Mark Scipioni, Management Analysis & Development Division, Minnesota Management & Budget

Barbara Tuckner, Management Analysis & Development Division, Minnesota Management & Budget

Office of Health Information Technology

Minnesota Department of Health

Diane Rydrych, MA

Martin LaVenture, PhD, MPH

Lisa Moon, BSN

Bob Johnson, MPP

Karen Soderberg, MS

MINNESOTA HEALTH RECORD ACCESS STUDY

TABLE OF CONTENTS

Acknowledgements	2
List of Tables and Figures.....	4
Executive Summary	5
Introduction	8
Background Context: Electronic Health Record Adoption, Use and Exchange in Minnesota	8
• Weaving a Strong Trust Fabric to Ensure Effective Use of EHRs and Secure HIE	9
Methodology and Data Collection	10
• Survey of Minnesota Hospitals and Clinics	11
• Focus Groups at Hospitals, Clinics and Health Systems	12
• Public Comments	13
Comparison of Minnesota State and Federal Privacy and Security Laws.....	13
• Minnesota and Federal Law Related to Use and Disclosure: Table 3	16
Health Record Access Study Findings	17
• The Process for Monitoring Unauthorized Access to Patient Health Records.....	19
• The Feasibility of Providing Patients with a Copy of their Audit Log	29
• The Feasibility of Informing Patients when Unauthorized Access is Detected.....	36
• The Monitoring of Representation of Consent	39
Recommendations and Considerations	46
Bibliography	48
Environmental Scan of Available Literature and Sources	50
Glossary of Selected Terms	61
Appendix A: Legislative Request for Study	63
Appendix B: Survey Responses	64
Appendix C: Focus Group Responses	86
Appendix D: Public Participation and Comments.....	98
Appendix E: Overview of Minnesota Health Records Act and Federal Law	102
Appendix F: Example Workflow: Representation of Consent	119
Appendix G: Minnesota e-Health Advisory Committee Members	110

LIST OF TABLES AND FIGURES

TABLES	PAGE NUMBER
Table 1: Summary Study Methods and Approach	11
Table 2: Summary of Minnesota and Federal Law Related to Use and Disclosure of PHI	16
Table 3: List of Departments that May Access a Health Record Outside of the Treatment Team	31
Table 4: Audit Log Generated by Focus Group Participant’s Health Care Organizations	32
FIGURES	
Figure 1: Percent of Minnesota Providers Using Electronic Health Records	9
Figure 2: Study Participant Geographic Distribution by Type of Facility	11
Figure 3: Methods for Monitoring, Compliance Checks, and Audit Procedures to determine Unauthorized Access to Patient Electronic Health Records	19
Figure 4: Challenges in Acting to Ensure Privacy and Security of Electronic Health Information	21
Figure 5: Ability of Facility’s EHR System to Generate an Audit Log that Documents Every Access to the Patient EHR	30
Figure 6: EHR Systems’ Capabilities to Provide a Patient with a Copy or Version of the Audit Log	32
Figure 7: Reason for Generating an Audit Log at least Once in Past 12 Months by Type of Facility	33
Figure 8: Policies and Practices Used to Inform Patients if Intentional, Unauthorized Access to their Health Records Occurs	37
Figure 9: Method of Communication Used to Inform a Patient of any Intentional, Unauthorized Access to their Health Record	38
Figure 10: Percent of Facilities that Request a Copy of Patient Electronic Health Records by Using Representation of Consent	40
Figure 11: Methods used for Communicating to Another Provider with whom the Facility has Patient Consent to Share Patient Health Data	41
Figure 12: Methods Used for Monitoring, Compliance Checks, and Audit Procedures to ensure that the Appropriate Patient Consent is on File	42
Figure 13: Facilities Able to Capture Patient Consent Transaction in the EHR by Facility Type and Geography	43

EXECUTIVE SUMMARY

Minnesota health care providers, clinics and hospitals have made great progress in adopting electronic health records (EHRs). This movement toward the adoption and effective use of EHRs, as well as the secure, standards-based exchange of health information, will continue to accelerate as Minnesota and the nation implement federal meaningful use standards for the use and exchange of electronic health information. A critical piece of this progress is that patients must be able to have confidence in the integrity of the data being shared, and trust that providers using the data have procedures in place to keep their information safe and secure.

To achieve this level of confidence and trust, all providers of health care services, regardless of size or specialty, must implement standards for securing electronic health information to ensure that appropriate safeguards are in place to protect that data from unauthorized access. These administrative, technical and physical safeguards, together with sound policies, procedures and practices for how health care providers can effectively use technology to deliver patient care, will create a framework in which patient trust and confidence can grow, and meaningful health information exchange can take place.

In spring of 2012, the Minnesota legislature directed the Minnesota Department of Health (MDH), in consultation with the e-Health Advisory Committee, to conduct a study of specific questions pertaining to the current use of Representation of Consent, electronic health information security practices, and patient notification procedures when unauthorized access to an electronic health record occurs. Regulated by both state and federal law, these three elements influence the management of electronic health information and exchange, and are a part of the activities necessary to ensure sound privacy security practices for electronic health information.

The Minnesota Health Records Access Study used four methodologies to study the questions posed by the legislature: a survey of 25% of Minnesota hospitals and clinics, three regional focus group meetings, a public meeting and comment period, and an environmental scan of relevant literature. The summary of findings contained in this report is organized by common themes that emerged during the analysis of data. These findings are linked to recommendations that will help guide interventions to address needs identified through the study.

HEALTH RECORD ACCESS STUDY FINDINGS

Topic 1: The Process for Monitoring Unauthorized Access to a Patient Health Record: Monitoring unauthorized access to a patient's health record is completed through proactive and reactive methods that are not standardized. Monitoring is most often completed in response to a patient complaint. Proactive monitoring procedures are in various stages of development and are impacted by competing

organizational priorities, the inability of the EHR to flag unauthorized access, and complex requirements for managing patient privacy preferences.

Recommendations:

- A. Identify best practices and existing national standards for proactive and reactive monitoring procedures to detect unauthorized access to electronic protected health information, and develop guidance that can be shared with health care organizations statewide.
- B. Create and disseminate user-friendly informational materials for patients on consent and release of information practices, including common ways that health information may be used and/or accessed within a health care organization.

Topic 2: The Feasibility of Providing Patients with a Copy of a Provider’s Audit Log: Audit logs, or records of all instances when a patient’s electronic record has been accessed, can be generated by most health care entities but are not formatted in a standardized and readable format for patients and often include voluminous amounts of data. This makes them not useful for patients in their current form. Audit logs are rarely requested by patients; when they are the request is usually based on a patient complaint. Privacy officers report that collaborating directly with patients is often a more effective way to investigate patient complaints of unauthorized access than the production of an audit log.

Recommendations:

- A. Identify and/or develop and implement consumer-friendly audit log standards for Electronic Health Records (EHRs).
- B. Collect and share best practices and guidance on consumer / provider collaboration in cases of suspected unauthorized access, including standard processes and actions.
- C. Endorse federal actions that improve EHR certification criteria for standardized and improved EHR capabilities to produce patient-readable audit logs.

Topic 3: Feasibility of Informing Patients When Unauthorized Access is Detected: Notification of patients affected by unauthorized access of their personal health information usually follows the standards set by federal notification requirements; however, some providers report that they do not have patient notification procedures in place. For those that have notification procedures in place, the procedures are consistent across the state but remain largely paper processes even though electronic encrypted technology exists.

Recommendations:

- A. Identify and share best practices for notifying patients when unauthorized access to an EHR is detected, and provide technical assistance to providers as necessary to implement best practices.

Topic 4: The Monitoring of Representation of Consent: Representation of Consent (ROC) is a unique aspect of the Minnesota's Health Records Act, which allows providers to electronically notify other providers that they hold the patient's consent to share information. Representation of Consent, which is designed to facilitate the secure, consent-based sharing of electronic health information, is not widely understood or used, and in some instances creates the perception of mistrust between providers. The process of obtaining patient consent remains largely a paper process and few EHRs have incorporated electronic consent features. Some gaps in auditing the use of ROC at the provider level were reported by survey respondents.

Recommendations:

- A. Develop consensus standards for monitoring the use of representation of consent.
- B. Support education of the health care workforce on representation of consent to ensure widespread understanding of the provision.
- C. Ensure that processes are in place for appropriate and efficient use of ROC transactions, and for monitoring that use of ROC is in compliance with the requirements of the Minnesota Health Records Act.

Other Recommendations and Considerations:

To further address findings of this report, the Minnesota Department of Health should:

- A. Convene stakeholders to use Health Record Access Study findings as a basis for considering modifications to Minnesota statutes to reduce complexities due to disparate state and federal privacy and security rules.
- B. Use its annual health information technology surveys of hospitals and clinics to monitor progress towards implementation of best practices and state/federal requirements related to privacy and security of electronic health information.
- C. Expand efforts to develop and deliver training to healthcare providers and other staff in health care facilities on electronic privacy and security issues surrounding health information including: creating a culture of awareness of risk related to unauthorized access, knowledge of individual accountability for the handling and disclosure of health information, foundational knowledge base of the current EHR mechanisms that deter unauthorized access, and outline permissible and impermissible uses and disclosures of electronic protected health information.

MINNESOTA HEALTH RECORD ACCESS STUDY

INTRODUCTION

Minnesota has long had a goal of ensuring a balance between protecting an individual's electronic health information and assuring that such information is available in a secure and authorized way to those who need it to provide treatment across the continuum of care. The rapid adoption of electronic health records (EHR) and electronic health information exchange has created an environment of ongoing change in the delivery of health care across Minnesota. This can present new challenges and opportunities for both health care providers and patients, one of which is the security of electronic protected health information (ePHI).

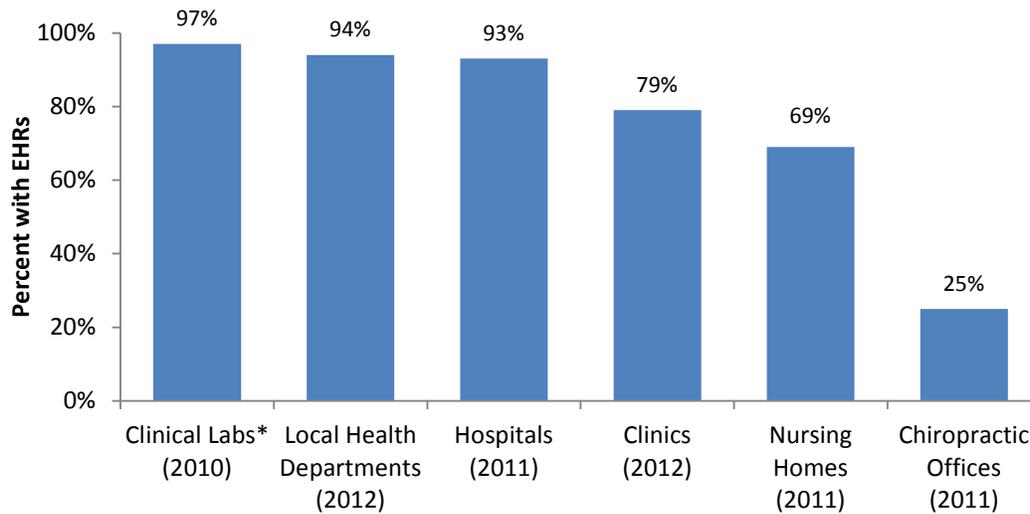
In the spring of 2012, the Minnesota legislature directed the Minnesota Department of Health (MDH), in consultation with the Minnesota e-Health Advisory Committee, to study three questions related to the current landscape of health information security pertaining to the representation of consent, monitoring for unauthorized access of electronic health records and notification of patients when unauthorized access occurs. Regulated by both state and federal law, these three elements influence the management of electronic health information and exchange, creating a framework on which sound privacy and security practices can be built. The legislature's questions regarding the security of ePHI are listed in Appendix A.

The study was conducted by MDH's Office of Health Information Technology. This study report provides context regarding security practices for electronic health information and exchange in Minnesota, summarizes the methodology used for data collection through a survey of Minnesota hospitals and clinics, focus groups at hospitals, clinics, and health systems, and a public comment period to solicit the consumer perspective. This report includes a comparison of Minnesota state and federal privacy and security laws, study findings and recommendations.

BACKGROUND CONTEXT: EHR ADOPTION, USE AND EXCHANGE IN MINNESOTA

Minnesota health care providers, clinics and hospitals have made great progress in adopting electronic health records and facilitating exchange of health information. Figure 1 below shows that 93% of hospitals and 79% of clinics have implemented and are using EHRs. The adoption and use of EHRs are driven by the need for access to information for better care and is fueled by federal mandates and incentives; the need to connect health care data across all health care settings has become a high-priority objective at both the state and national level. The movement towards adoption and effective use of EHRs, as well as secure, standards-based exchange of health information, will continue to accelerate as Minnesota and the nation moves toward new models of care delivery, such as Health Care Homes and Accountable Care Organizations (ACOs).

Figure 1: Percent of Minnesota Providers Using Electronic Health Records



Source: Minnesota Department of Health, Office of Health Information Technology, 2010-2012 Annual Health IT Surveys.

Despite the many benefits of electronic health records, and the substantial progress that has been made in Minnesota towards the adoption and effective use of EHRs and other health information technology (HIT), challenges persist. For example, rates of effective use of EHRs, as measured by the use of such tools as clinical decision support and computerized provider order entry, continue to lag behind EHR adoption rates. Achieving effective use of EHRs is complex and is impacted by user behavior, organizational processes and practices, and EHR functionality.¹ The full benefits of EHRs will not be realized until the use of these and other tools for improving quality of care are consistently in place. The core success of the health care system in Minnesota relies on developing and supporting effective use and exchange of clinical information between providers that need the data for patient care.

Weaving a Strong Trust Fabric to Ensure Effective Use of EHRs and Secure HIE

The real value in EHR systems comes from using them effectively to support efficient workflows and effective clinical decisions that have a positive and lasting effect on the health of individuals and populations. To accomplish this, a health care system must support a framework for patient trust and confidence that is built on preserving the integrity of the data, and facilitating the secure exchange of health information between providers to promote optimal health care.

Providers, clinics and hospitals need to have accurate and complete information at all times in order to deliver high quality patient care that is coordinated across the care continuum. Without patient trust and confidence, the sharing of health information may be limited or nonexistent, increasing the opportunity for negative care results, poor quality, gaps or delays in the delivery of care, and increased redundancy – and costs – in the health care system. To establish this trust relationship, the patient must

¹ Minnesota eHealth Initiative 2012 Legislative Report <http://www.health.state.mn.us/e-health/legprpt.html>

be confident in the security measures that have been applied for the protection and exchange of their ePHI.

The secure exchange of health information between providers is achievable when well-documented standards and tools for health information security are implemented in all care settings. When these administrative, technical and physical safeguards are present, they can protect data from inappropriate access and impermissible use. It is within this framework that the fabric of patient trust and confidence can grow, and meaningful exchange of health information can take place.

METHODOLOGY AND DATA COLLECTION

The study focus: Because the legislature’s charge to MDH focused on issues related to access to electronic health records (EHRs), the study scope included only Minnesota hospitals and clinics that have EHRs. Excluded from the study scope were other health care settings, such as dental offices, chiropractic offices, nursing homes, correctional health, and local health departments, as well as those hospitals and clinics that have not fully adopted an electronic health record system.

Study questions focus: The study focused on the three broad questions posed in the legislative request (see Appendix A). A number of potential questions were received from the public and from providers regarding privacy and security of health information and EHRs; however, most of the questions were considered out of scope of this study.

Study Design: Four methods were used to obtain qualitative and quantitative data for the study, including: a literature review and environmental scan and key word search of existing laws and practices, an electronic survey of a sample of 25% of Minnesota hospitals and 25% of ambulatory clinics that have adopted an EHR, three focus group sessions to seek in-depth qualitative information from privacy professionals in Minnesota, and input from the public via a public meeting and online comment solicitation. Table 1 summarizes the study design methods and approach used.

Beginning in July 2012, the study team also worked closely with the Minnesota e-Health Advisory Committee and a variety of Minnesota stakeholders including; the Minnesota Medical Association, Minnesota Hospital Association and the e-Health Advisory Committee’s Privacy and Security Workgroup co-chairs. These groups were instrumental in development of the survey tool, recruitment of focus group participants, and support of the efforts to attain a high survey response rate.

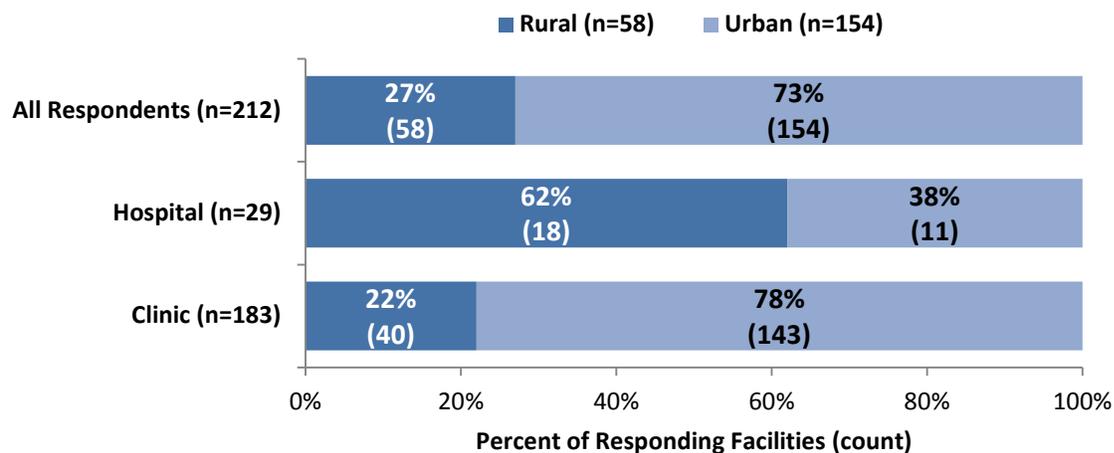
Table 1: Summary Study Design Methods and Approach

STUDY METHOD	DESCRIPTION
Survey of Minnesota Hospitals and Clinics	Electronic Survey of 25% of Minnesota hospitals and 25% of ambulatory clinics- launched November 7, 2012
Focus Groups	Three hours; professionally facilitated Health Systems: Bloomington, MN at HealthPartners on November 8, 2012
	Hospitals and Clinics: Willmar, MN at Rice Memorial Hospital on November 13, 2012 Duluth, MN at St. Luke’s Hospital on November 16, 2012
Public Comments	Public Comment period December 6-20, 2012
Literature Review	Environmental scan and key word search of existing data and literature
Federal / State Comparison	Summary of seven topics and differences between MN and federal laws

SURVEY OF MINNESOTA HOSPITALS AND CLINICS

The survey was conducted in November-December of 2012, with a random sample of 25% (31) Minnesota hospitals and 25% (234) of ambulatory clinics that use electronic health record systems. Responses were received from 212 facilities, representing 183 clinics and 29 hospitals, for an overall response rate of 77%. Of the facilities that responded, 52% of hospitals and clinics identified themselves as being part of a health system. Figure 2 shows the geographic distribution of respondents by type of facility.

Figure 2: Study Participant Geography by Type of Facility



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Two versions of the survey tool were created; one for hospitals and clinics and a second survey for health systems. The questionnaires are nearly identical and, for this analysis, are presented as a single survey.

An analysis of the survey data included distribution tables for each question and, when appropriate, comparison across questions. A complete set of tables can be found in Appendix B.

FOCUS GROUPS FOR HOSPITALS, CLINICS AND HEALTH SYSTEMS

The study used three in-person focus group meetings to gain in-depth understanding of the study questions. The three hour format allowed for question and response dialogue between the participants and the meeting facilitators. Answering the study questions required a detailed understanding of privacy law, policy, and local practices. Privacy officers by definition are expected to have this level of knowledge and experience and thus were recruited as focus group participants.

All focus group participants were employed by health care organizations as privacy officers² or information management officers. Some, but not all, focus group participants worked for a health care organization that was included in the random sample of hospitals and clinics that received the online survey tool.

Three focus group meetings were conducted in November 2012 and held in Bloomington, Willmar and Duluth to achieve a level of regional representation. Attendance was by MDH invitation and sought to include a cross-section of health systems, as well as large and small, urban and rural health care facilities. Two of the meetings included representatives from hospitals and clinics; the metro area meeting included health systems and hospitals. A total of 21 people participated, representing 18 health care organizations in Minnesota. The number of participants ranged from six to nine for each of the three sessions.

A structured protocol was used and the discussions were led by an attorney who specializes in the privacy and security of health information. The agenda and discussion were facilitated by professionals from the Management Analysis Division (MAD) of Minnesota Management and Budget. Comments were not associated with any one individual or health care organization.

Analysis of the focus group results included a thematic analysis across all three focus groups. Major themes were identified by meeting participants and refined and validated by the study team. In

² The role of the Privacy Officer as defined by Health Information Portability and Accountability Act of 1996²(HIPAA), is to oversee all ongoing activities related to the development, implementation and maintenance of the organization's privacy policies in accordance with applicable federal and state laws. Privacy officers have a deep understanding of the workflow and processes for both the clinic and hospital settings and thus were critical participants in the qualitative discussions.

addition, stories, examples, and comments were collected and used to support the themes identified in the survey data. The full report of focus group responses is available in Appendix C.

PUBLIC COMMENTS

MDH sought public input and comment at several points in the study process. Opportunities for public input included a public in-person meeting and invitation to provide comments via electronic communications. The public meeting was held on December 6, 2012, with a goal of better understanding the patient perspective as it applies to the questions posed by the legislature in the Health Records Access Study, and to provide an opportunity in which public comment could be received. A public conference call option was also made available during this meeting.

MDH made at least 12 public announcements related to the study during the study period. These included announcements for the public meeting using the Minnesota e-Health Weekly Email Update (received by over 4,200 individual subscribers), and known Minnesota consumer advocacy groups were notified to give them an opportunity to comment on the legislative questions. At the public meeting, MDH staff presented draft emerging themes from both focus group meetings and the electronic survey. Twenty individuals attended the meeting; only one public comment was received at that time. The public comment period continued for a fifteen day period following the public meeting and a summary of public comments received is included as Appendix D.

Findings from the Public Comment Period

Public comments received during the 15 day comment period expressed general concern for topics related to patient privacy, security of health information and patient ownership of their data and included numerous comments in favor of privacy protection to the fullest extent possible. These comments were mostly sent via email, and most were in form letter format. Prominent themes relating to the legislative study questions from the responses received during the public comment period were 1) a desire for patients to be informed if unauthorized access of their health information occurs and 2) a desire to be able to access a patient-friendly audit log listing the individual and the roles of those who accessed their records and for what purpose.

COMPARISON OF MINNESOTA STATE AND FEDERAL PRIVACY/SECURITY LAWS

In order to place the findings of this study in an appropriate context, it is essential to understand the federal and Minnesota laws and approaches to protecting health information, including how the approaches differ and how the sometimes divergent federal and state requirements interact to impact patient interests and provider practices. Table 2 shows a comparison of the applicable Minnesota state and federal laws as they relate to the use and disclosure of PHI; a more in-depth analysis is in Appendix E.

Federal Privacy and Security Law: In 1996 the Federal government enacted the Health Information Insurance Portability and Accountability Act (HIPAA)³ to improve the efficiency and effectiveness of the American health care system through, among other strategies, implementing national standards to facilitate electronic data exchange. Because of concerns that, as the electronic exchange of health information increases, so can the likelihood of inappropriate access of that health information, in 2000 Congress added privacy and security requirements to the Administrative Simplification provisions of HIPAA.⁴ These regulations include the HIPAA Privacy Rule, which establishes a set of national standards for the use and disclosure of protected health information as well as standards for providing individuals with privacy rights, and the HIPAA Security Rule, which establishes national standards to protect individuals' electronic protected health information that is created, received, used or maintained by a covered entity (Office of the National Coordinator, 2012).

Additional guidance for privacy and security requirements were added to HIPAA as part of the Health Information Technology for Economic and Clinical Health Act (HITECH) enacted as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

In January 2013, the final HIPAA rule⁵ was announced, strengthening and expanding patient rights as well as enforcement. Provisions of the final HIPAA rule include;

- Limitations on the use and disclosure of PHI for marketing and fundraising;
- Prohibition on the sale of PHI without authorization;
- Expanded rights to receive electronic copies of health information and to restrict disclosures to a health plan concerning treatment paid out of pocket in full;
- Requirement to modify and redistribute notice of privacy practices;
- Modification of the individual authorization and other requirements to facilitate research, disclosure of child immunization verification to schools, and access to decedent information by family members/others.

The final HIPAA rule also increases privacy protection for genetic information, includes changes to HIPAA enforcement incorporating higher penalties, and includes the adoption a new Breach Notification Rule that replaces the previous rule's "harm" threshold with a more objective standard.

Minnesota Law: The Minnesota Health Records Act, a state law that provides guidance for the management of health related information, outlines standard elements that must be present in the patient consent transaction for the disclosure of individually identifiable health information to take place. The Minnesota Health Records Act does not address the security of electronic health records,

³ Pub. L. No. 104-191, 110 Stat 1936 (codified in sections of 18, 26, 29, and 42 U.S.C.).

⁴ 65 Fed. Reg. 82,474 (Dec. 28, 2000).

⁵ 45 C.F.R. 160 and 164 modifications made for the HIPAA final rule effective March 26, 2013

monitoring of unauthorized access, or notification practices when unauthorized access occurs; many of these issues are covered in HIPAA. The Minnesota Health Records Act was amended in 2007 to include what has come to be known as the *Representation of Consent* provision,⁶ which decreases the manual process of obtaining and sharing the patient consent to release information by allowing providers to electronically indicate that they hold a patient’s consent to release or share information with another provider.

Federal and State Interplay: HIPAA’s Privacy Rule and the Minnesota Health Records Act establish different requirements regarding what permissions a health organization must secure before it discloses (releases) health information to a third party for treatment purposes. HIPAA allows an individual’s health information to be exchanged among providers treating an individual without the patient’s express permission for treatment, payment and health care operations. The Minnesota Health Records Act, on the other hand, prohibits exchange for treatment purposes unless the patient has provided a signed, written permission (consent). This consent to release health information form is valid for a period of one year, unless otherwise specified by the patient.

Minnesota is nearly unique among states in requiring patient permission to disclose any type of health information to other providers for treatment purposes,⁷ only Minnesota and New York do not align their requirements with HIPAA. Because most states have standardized their approach to patient consent for release of health information for treatment purposes on the HIPAA model, national or multi-state EHR technology and HIE structures and systems are typically designed and built to meet the HIPAA requirements. Because Minnesota law differs on this issue, health care organizations must customize standard technological systems (for example, EHRs), administrative procedures, and patient care workflows to accommodate Minnesota consent requirements before they can release information for treatment purposes.

⁶ *The Representation of Consent* provision language (in bold below) was added to the MN HRA to modify the “consent to release” requirements:

Unless an exception applies, a provider, or a person who receives health records from a provider, may not release a patient’s health records without: (1) a signed and dated consent from the patient or the patient’s legally authorized representative authorizing the release; (2) specific authorization in law; or (3) **a representation from a provider that holds a signed and dated consent from the patient authorizing the release.**

Minn. Stat. 144.293, subd. 2

A provider who **releases** health records in reliance upon a requesting provider’s *representation of consent*, must document: (1) the provider requesting the health records; (2) the identity of the patient; (3) the health records requested; and (4) the date the health records were requested. Minn. Stat. 144.293, subd. 9.

⁷ “Only two states (Minnesota and New York) appear to generally require patient permission to disclose all types of health information.” *Privacy and Security Solutions for Interoperable Health Information Exchange Report on State Law Requirements for Patient Permission to Disclose Health Information*, prepared for RTI, International; Section 4-3

Table 2: Summary of Minnesota and Federal Law Related to Use and Disclosure

Topic	Minnesota Law <i>MN Health Records Act of YEAR (§§144.291-144.298) and Data Practices Act (Chapter 13)</i>	Federal Law <i>HIPAA regulations of 1996 (45 CFR Parts 160 and 164); HITECH Act (P.L. 111-5, Titles XIII and IV)</i>	Differences and Policy Considerations
Release of Health Information (ROI)	144.293 Patient must consent for each <i>disclosure</i> of their health information for any purpose, before health records can be shared. Providers may use representation of consent to facilitate the ROI process.	164.502 (a) Covered Entity cannot <i>use or disclose</i> PHI except for the purposes of treatment, payment health care operations (TPO). Exceptions do apply in 164.512 and 164.514	Minnesota Law is more restrictive and protective of individual privacy rights, pre-empting federal HIPAA privacy law as a result
Release of Health Information to Other Providers	144.294 Patient consent is not needed for ROI to other providers within a related health care entity when it is necessary for treatment of the patient	164.506 Except where patient authorization is required by 164.508, a covered entity is not required to obtain consent to disclose PHI for use in TPO.	Minnesota Law is more restrictive in that it is protective of individual privacy rights, pre-empting federal HIPAA privacy law as a result
Required or Permitted Releases Without Consent	144.291 Patient consent is not needed for ROI in a medical emergency when medical/mental health is needed to preserve life and prevent serious impairment to bodily functions, or when a court order or subpoena requires release of PHI, or for public health purposes through MDH activities	164.512 PHI may be disclosed when specifically authorized by law for public health activities, disclosures about violence/abuse, health oversight activities, judicial and administrative proceedings, law enforcement purposes, organ donation, certain research purposes, to avert serious health threats, special government functions, workman’s compensation and disclosures to HHS secretary to investigate compliance	Minnesota Law is more restrictive in that it is protective of individual privacy rights, pre-empting federal HIPAA privacy law as a result
Minimum Necessary	No mention in MN Health Records Act	164.502 (b) and 164.514 (d) Covered Entity must make reasonable efforts to limit PHI to “minimum necessary” to accomplish the intended purpose of the use, disclosure or request.	No conflict - non-government providers comply with HIPAA
De-Identified Health Information and Limited Data Set	No mention in MN Health Records Act §13.05 subd. 7, discusses summary data for government entities.	§164.514. De-identified information may be shared. §164.514(e). A limited data set (removal of specified identifying data elements) may be released only for research, public health or health care operations purposes. A data use agreement must be in place.	No conflict - non-government providers comply with HIPAA
Access/Copies of Health Information	§144.292, subd. 5 & 6 describes the process for how to request a copy of your health records	§164.524 Individual has a right to access to inspect and obtain a copy of PHI in a designated record set(DRS), as long as the PHI is maintained in the DRS; excepts may apply and the new notification rule specifies that patients have access to their own health record.	No conflict - non-government providers comply with HIPAA
Accounting of Disclosures	§144.293, subd. 9 documentation requirements for ROI and ROC as they apply to health records.	§164.528 Outlines specific guidelines for individual rights to receive an accounting of disclosures or PHI made by covered entity based on the way PHI is used	Both focus on individual rights of patient to accounting of disclosures
Security Safeguards (Security Breaches)	No mention in MN Health Records Act	§164.530(c); These are the administrative requirements and safeguards that a covered entity must have in place to ensure privacy of health information. 164.302 HIPAA security rule for protection of electronic PHI. HITECH widens the scope of privacy and security protections available under HIPAA and increases legal liability for non-compliance, and enforcement and the new Breach Notification Rule of 2013 outlines risk analysis criteria that must be completed.	No conflict - non-government providers comply with HIPAA

HEALTH RECORD ACCESS STUDY FINDINGS

The following is a summary of findings that emerged during the analysis of data from the survey of hospitals and clinics, focus group meetings, public comment and literature review of relevant topics. Each section begins with a high-level topic based on the legislature's questions followed by the subsequent theme(s) supported by survey data, focus group discussion points, and literature sources that apply.

TOPIC 1: THE PROCESS FOR MONITORING UNAUTHORIZED ACCESS TO PATIENT HEALTH RECORDS

CONTEXT AND DEFINITIONS

Unauthorized access to electronic health records occurs when a clinician or other health care workforce member accesses the patient's health record for personal or criminal purposes. This act of unauthorized access may include obtaining, retrieving, or viewing electronic health records in violation of Minnesota or federal laws or regulations, or a hospital or provider office's policies or procedures. An EHR system can log each access into the patient record with an electronic date, time, and employee identifying information. This chronological event log forms an audit trail or tracking mechanism that can be used for security risk analysis in compliance programs and can be reviewed should unauthorized access be suspected.

Unauthorized access into the health record occurs for a variety of reasons, but most often is because of employee curiosity. A recent survey by Veriphyr™ (an Identity and Access Intelligence software application) of 70 U.S. healthcare providers found that the majority of hospitals in the study had experienced a breach in the last year, and that breaches were most often classified as snooping into medical records of fellow employees (35%), snooping into records of friends and relatives (27%), loss/theft of physical records (25%), and loss/theft of equipment holding ePHI (20%) (Gendron, 2011). This same study found that when a breach occurred it was detected 30% of the time in one to three days, and most cases were resolved with some administrative action within four weeks. The act of unauthorized access into a patient record, per the Veriphyr™ also noted that unauthorized access can diminish the trust of the patients who are affected by the breach.

Example of Suspected Unauthorized Access into Electronic Health Record (EHR)

Ms. Smith has her first appointment at the doctor's office to confirm that her pregnancy is on track, and that both she and her baby are healthy in the first trimester. When she arrives at the doctor's office, she notices that her neighbor and fellow church member is working behind the reception desk at one of the providers work stations. The neighbor looks up and notices Ms. Smith standing at the front desk. Ms. Smith is nervous, and aware that no one in her family and certainly no one in her small community know that she is expecting a child. She proceeds with the new patient intake procedure supplying personal data, insurance information and the reason for her visit today. The visit goes as planned and she leaves the office that day feeling that her treatment plan for the remainder of her pregnancy is on track.

Time passes, and she and her husband have determined that they will not share their good news with anyone until the pregnancy is further along, since a previous pregnancy ended tragically with the loss of the baby. Later that week, Ms. Smith is caught at the grocery store by another church member and congratulated on her new pregnancy. Puzzled and a bit confused as to how this information would be common knowledge, Ms. Smith thinks back through all of her interactions and carefully considers who may have known and how the information could have been shared. It is then that she realizes that the only time that she has shared her pregnancy news with anyone is at the doctor's office during her first visit. Though she does not want to make any quick conclusions, she is suspicious that her neighbor may have accessed her record at the doctor's office even though she was not authorized to do so, and may have shared her pregnancy news with others that they both knew at church.

The Minnesota Health Records Act has specific language that addresses the disclosure of a health record and requires that a patient's consent be obtained each time that that information is shared or exchanged between health care providers.⁸ The Minnesota Health Records Act, however, is silent on monitoring for unauthorized access and patient notification requirements. The HIPAA security rule includes two provisions that require organizations to perform security audits. They are:

- **Section 164.308 (a) (1) (ii) (c)**, states that organizations must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."
- **Section 164.312 (1) (b)**, states that organizations must "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

⁸ 144.293 MN Health Records Act The Release or Disclosure of Health Records

Subdivision 1 Release or disclosure of health records

Health records can be released or disclosed as specified in subdivisions 2 to 9 and sections [144.294](#) and [144.295](#).

Subdivision 2: Patient consent to release of records. A provider, or a person who receives health records from a provider, may not release a patient's health records to a person without: (1) a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release;(2) specific authorization in law; or (3) a representation from a provider that holds a signed and dated consent from the patient authorizing the release.

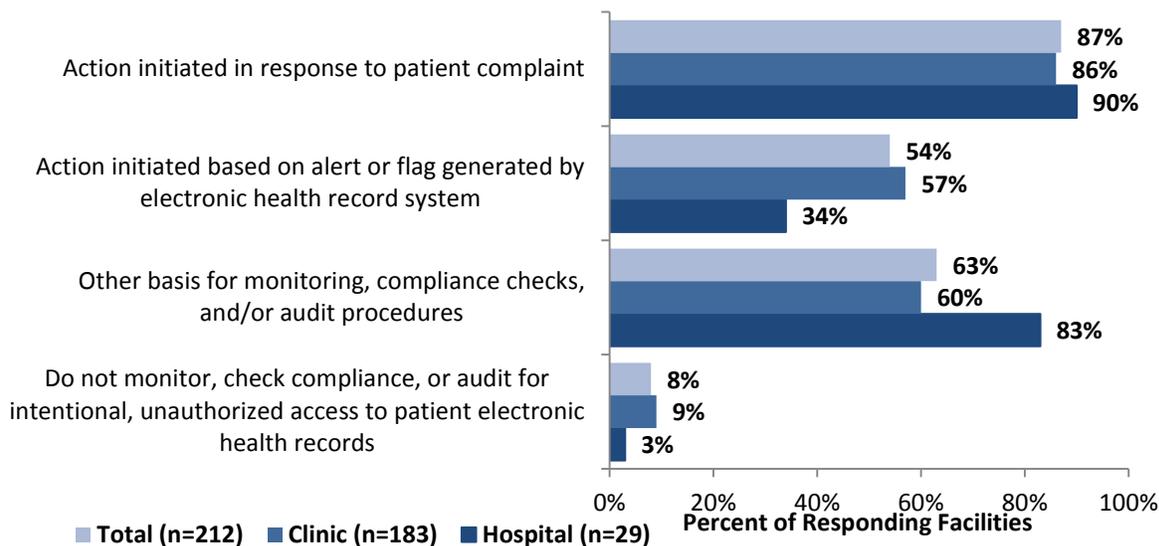
Privacy, security and compliance functions are necessary so that the patient, who is at the center of the data exchange transaction, can have trust and confidence that their individually identifiable health information is safe within the EHR system and when shared with other providers.

A. Theme: Monitoring is completed through proactive and reactive methods that are not standardized. Monitoring is most often completed in response to a patient complaint.

The HRA survey data showed that most (92%) responding facilities monitor, check compliance, or audit to determine the occurrence of intentional, unauthorized access to patient electronic health records (commonly referred to as a “breach”). The most common procedure is an action initiated in response to a patient complaint, with 87% of all respondents reporting this (Figure 3).

In addition, more than half of all respondents (54%) initiate action based on proactive monitoring of alerts or flags generated by an electronic health record system, with 57% of clinics and 34% of hospitals reporting that they perform monitoring, compliance checks and audits based on this information. Nine percent of clinics and eight percent of hospitals indicated that they do not monitor, check compliance, or audit to determine whether intentional, unauthorized access to a patient’s EHR has occurred, which may indicate that some EHRs are still not fully implemented or do not have the system generated alerts available in their EHR, or that tools and processes are not in place to complete the needed process at these sites.

Figure 3: Methods for Monitoring, Compliance Checks, and Audit Procedures to determine Unauthorized Access to Patient Electronic Health Records



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey

When monitoring for unauthorized access into a patient’s record, 63% of HRA survey respondents reported they use other methods, like systematic random audits to monitor unauthorized access of their electronic patient records. The open-ended comments indicate however that these random audits have

proven to be an inefficient means of detecting unauthorized access and that the only way for some organizations to detect such access is through a manual review of access logs which requires significant resources, or by purchasing third party auditing software which is fairly new and emerging technology.

HRA survey shows that respondents prefer to rely on systematic random audits and specific triggers as an approach to monitoring, because automated tools within the EHR are not very efficient. Eighty-three percent of hospitals and 60% of clinics noted they use other methods to audit for unauthorized access into a patient record. Their open-ended comments identify common approaches that may be used:

- Systematic random audits based on employee last name and address looking for matches with relatives that are patients
- Monitoring of any access to the records of high profile patients (such as public figures and celebrities)
- Random audits on a specific number of employees or records each month
- Automated tools within the EHR that flag potential cases of unauthorized access

The HRA survey respondents were also asked about monitoring, compliance checks and auditing with respect to non-employees. For the purpose of this study, non-employees are those who work for a covered entity on contract for services and because of the nature of their work would require access into the EHR system. The procedures used to monitor unauthorized access by non-employees are quite similar to those used to monitor for potential breaches by employees. Ninety-two percent of HRA survey respondents monitor non-employees in some way, with the most common trigger being a patient complaint (84%). Just one in three (33%) respondents relied on an alert or flag generated by the EHR system to monitor suspected unauthorized access by non-employees.

Many respondents (61%) indicated other methods are used when monitoring for breaches by non-employees; similar to their responses for internal breaches, they often rely on employee complaints and conduct random audits more frequently among non-employees. Three percent of hospitals and nine percent of clinics reported they do not have processes in place for monitoring unauthorized non-employee access to patient records.

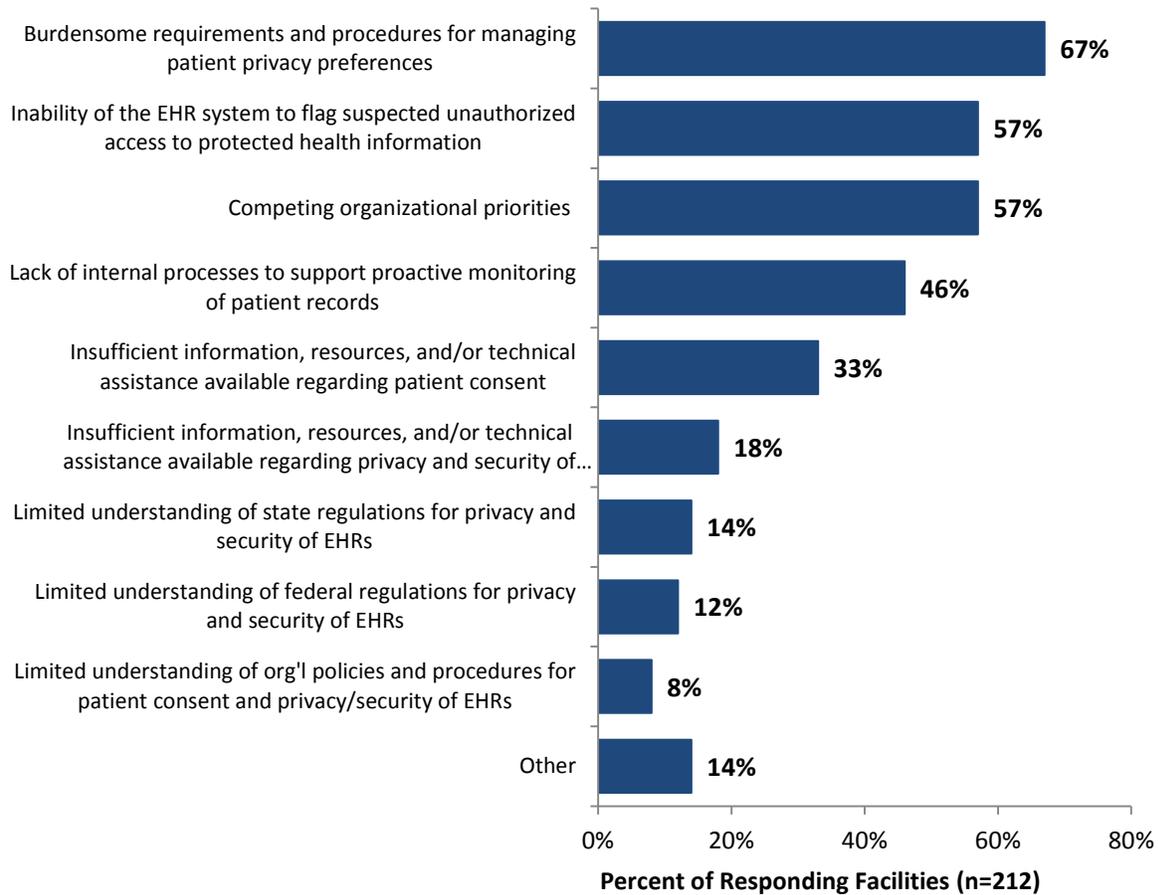
Focus group participants also shared examples of monitoring processes that go beyond what is currently required in the law, including setting up daily Google alerts based on local news websites for medical cases that may have been routed to their hospitals, setting up alerts based on employee names and addresses to screen for relationships and matches that may create an atmosphere of curiosity, encouraging employees to use their own personal health record that links them through their primary care physician to their personal medical information to avoid suspicious activity from getting logged onto the audit system because they used their employee ID to access their medical chart, and running searches based on “high utilizers” of the EHR system looking for abnormal patterns of access. In focus group discussions, participants noted they are always seeking robust and creative ways to safeguard patient information and that learning from what other organizations are doing can be very helpful.

Participants also noted they have systematic auditing, monitoring and compliance policies and procedures in place for both internal and external unauthorized access to patient health records. The core procedures for securing health information appear to be more similar than different across organizations. The processes for monitoring and auditing may differ from one health care entity to the other based on organizational policies, but most reported they go above and beyond the regulations that govern monitoring of electronic health information to “always do what is right for the patient.” Privacy officers in the focus group acknowledged it is the Covered Entity’s responsibility to have controls in place to prevent unauthorized access; however, with more sophisticated EHR vendor capabilities for detection, the act of discovery may be less manual and more targeted.

B. Even though health care organizations are monitoring for unauthorized access of EHRs, multiple challenges persist.

The survey data shows that 67% of those responding identify burdensome or complicated requirements and procedures for managing patient privacy preferences as a key challenge to ensuring the privacy and security of ePHI. Other key challenges to privacy and security of ePHI include the inability of the organization’s EHR system to flag suspected unauthorized access to ePHI (57%), competing organizational priorities (57%), and the lack of internal processes to support proactive monitoring of patient records (46%) as shown in figure 4. These challenges will be explored in the following four sub-themes.

Figure 4: Challenges to Ensure Privacy and Security of Electronic Health Information



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

1. Complicated requirements and procedures for managing privacy preferences

Sixty-seven percent of facilities that responded to the HRA survey reported that the current regulations for managing patient privacy preferences pose a challenge. Their open comments indicate that the challenge is not just in operationalizing the processes and procedures around patient consent management, but also in getting their EHR system to incorporate Minnesota patient privacy requirements and individual patient privacy preferences. Finding available resources for this customization on a large scale, while still being able to deliver seamless health services to patients is a particular challenge. Comments by HRA survey respondents also stated that “maintaining patient privacy and patient control over access and disclosure of their information in conjunction with regulatory initiatives for sharing information is complex.” Respondents also noted multiple times that “state and federal laws do not line-up,” which leads to confusion and variability across health care organizations. This confusion was also noted in the comments from focus group participants.

2. EHRs pose challenges to monitoring unauthorized access, because of system fragmentation and the inability of some EHRs to identify and send a system alert when unauthorized access occurs

Responses from for both focus groups and the HRA survey data noted that EHR capabilities for monitoring unauthorized access differ depending on the EHR vendor, with 57% of hospitals and clinics reporting this as a challenge to ensuring privacy and security of ePHI. Focus group participants stated that their EHR systems are custom built based on the unique needs of the clinic, hospital or health system. Some EHR vendors do not support alerts or flags in the system for unauthorized access into a patient record, and even when an EHR vendor module is available and can provide these alerts, organizations may not have purchased or implemented the feature in their current system.

Larger entities in the focus groups reported having more automated tools and organizational practices, more resources overall, and better capabilities to conduct broader and more in-depth follow-up activities. Examples of applications that act as automated tools that detect unauthorized access of a health record include; *Break the Glass* (BTC)⁹ an add-on software application that is used with EHR systems to detect unauthorized access, and FairWarning,^{TM10} an automated health technology privacy monitoring tool that allows care providers to centralize audit management into a single portal solution. These detection applications are expensive and require additional resources to manage. “False positive” results are frequent from the voluminous automated reports that are run within organizations and that are generated from deterrent applications. Below is an example of how the BTC software application works in an EHR.

Example of How the “Break the Glass” Software Application Works in an HER

“Break the glass” refers to the act of breaking the glass to pull a fire alarm—making it clear to the user that the person entering a health record without authorization is “breaking into” a medical record and that the access is temporary and for a specific purpose.

The “break the glass” alert prompts the user with a warning that they do not have the access or authorization that is required to access the information in the patient record. The software application requires that the user provide an explanation why they are accessing the record, at which time the system date and time stamps the access, and generates an alert that is then immediately reported to the privacy officer or information technology staff for auditing. The user then clicks “continue” in the software to obtain access to the patient’s information.

Each “break the glass” occurrence is attributed to an authenticated user; it is time-limited, and audited to ensure appropriate accounting of the disclosures. This provides an audit trail that facilitates post-event review. (Healthcare Information and Management Systems Society (HIMSS), 2009)

Modern electronic health records systems are modular, made up of sets of software applications that can be integrated. The modules for detecting unauthorized access are important but often these

⁹ Break the Glass (BTC) Accessed at: <http://www.himss.org/content/files/090909BreakTheGlass.pdf>

¹⁰ FairWarning Patient Privacy Monitoring for Healthcare Accessed: <http://www.fairwarning.com/>

modules are not integrated with the rest of the system, which can cause further challenges when investigating suspected unauthorized access. For example, the certified EHR may have many modules for the laboratory, pharmacy, scheduling, and follow-up. These may not be from the same vendor and often may not have combined audit logs causing fragmentation of the information system. Focus group participants noted that information system fragmentation negatively impacts efforts to investigate suspected unauthorized access of a health record and requires a search of multiple, disparate systems.

Another limitation of EHRs reported by focus group participants is that not all EHR systems are interoperable, and in some health systems there are multiple EHR systems being used. The 2012 Minnesota Health Information Technology Survey shows that more than 35 different certified EHR vendors are currently used in Minnesota ambulatory clinics and hospitals. One focus group participant represented 50 affiliated health care entities, with 18 different EHRs being used in that one system. The number of disparate EHR systems presents challenges to the complex process for capturing relevant information that can be used for the detection of suspicious access into a patient health record.

Emerging technologies also pose challenges to monitoring unauthorized access. Focus group participants noted that reports generated by deterrent applications in EHR systems capture all types of access, but do not include alerts or notification for mobile technologies and social media. Focus group participants also noted the landscape of health information technology is quickly changing, impacting the sophistication of the privacy staff's ability to monitor information and creating a climate that is in multiple stages of development, change and adaptation depending on the size of the organization, available resources and EHR vendor.

3. Competing Organizational Priorities

Seventy-six percent of hospitals and 54% of clinics reported that competing organizational priorities are a challenge to ensuring the privacy and security of ePHI. Open comments state that most of this challenge is related to securing the appropriate resources to complete the needed work when there are multiple and competing priorities, often demanding involvement of the same team members. One competing priority noted in the open comments by a HRA survey respondent is "there are so many EHR changes occurring and at the same time (there are) challenges in ensuring proper systems are in place." This implies it is difficult to accomplish all of the specified requirements at a time when there is rapid adoption of EHR technology, new federal mandates for ICD 10, and the attestation of the meaningful use of health information technology.

4. Lack of Internal Processes to Support Proactive Monitoring

HRA survey data shows that 52% of hospitals and 45% of clinics report that the lack of internal processes to support proactive monitoring is a challenge for ensuring privacy and security of ePHI in their organization. Open comments from survey respondents indicate that some organizations continue to deploy new EHR technology and are in the process of completing internal policies and procedures that

relate to the protection of ePHI. Other facilities note they are bringing in consultants to help them with their risk analysis and to help develop the processes which are required.

Focus group participants noted that automated reports can be generated from the EHR for unauthorized access, but they require manual internal processes for follow up and resolution to separate activities that are actual unauthorized access from those that are false positives. These internal processes are based on organizational procedures, and are most often completed as part of reactive monitoring following a patient complaint.

A focus group participant noted “the system application for detection may be automated in the EHR system, for example, generating a report of suspected unauthorized access into a patient record; but the investigation of each case of suspected unauthorized access remains largely manual.” This manual process of investigating each system alert was explained by focus group participants as requiring privacy officers and their compliance teams to research each individual case which can take several hours or several days depending on each unique case and requires the support of internal processes and organizational resources. An example of a typical follow up process for investigating unauthorized access into a patient’s record is shown below.

Example of a typical process required when unauthorized access into a patient record is suspected:

1. Determine which information systems need to be audited (may be multiple systems to get the whole story/picture).
2. Determine the timeline for the audit
3. Request audit reports to be run
4. Analyze audit reports to determine if any inappropriate access.
5. May have to read the medical record to determine who has the right to be in the record (who was treating the patient, who was assisting other staff – for example, an RN may be documenting in the record but a LPN or MA was assisting the RN and the LPN/MA needed to read information to know what was happening with the patient but had no need to document in the medical record.
6. Create a list of “not sure” if access appropriate.
7. Have Manager and/or Human Resources assist in determining if the “not sure” access is appropriate.
8. Sometimes a more detailed audit report needs to be run and analyzed
9. Human Resources and employee’s Manager may conduct an investigation to determine if access was appropriate
10. Corrective action may be taken

These actions of monitoring, compliance and auditing require that systematic and planned procedural steps be completed to ensure that each incident of suspected intentional unauthorized access of an electronic patient record is investigated to the full extent and that an outcome is established.

C. Theme: Electronic Health Records, despite some limitations, provide far superior capabilities for monitoring suspected unauthorized access compared to paper charts.

The Office of the National Coordinator for Health Information Technology, in its 2008 privacy and security report, notes that “organizations using electronic health record systems are able to protect patient information in more ways than if they used a paper record system. Privacy and security controls include: EHR systems that have the ability to monitor which health care professionals are accessing patient information and when; access can be limited to only certain authorized individuals and health information is encrypted so that it cannot be read by an unauthorized viewer (Office of the National Coordinator for Health Information Technology, 2008).”

Electronic health records provide multi-layered security protections that look for intrusion from unauthorized users. Modern EHR systems provide documentation of the date, time and individual who accessed record, by stamping the record with data that can be tracked, thus creating a chronology of events in each patient record. Focus group participants describe these security features as deterrents to unauthorized access, elaborating that with EHRs an incidence of unauthorized access or breach of individually identifiable information can be more easily and thoroughly tracked, and has legal requirements based on HIPAA for breach notification processes. Paper charts, on the other hand, cannot be easily tracked.

One focus group participant indicated: “In the era of increased access to electronic health records, the naïve and trusting notion that was present with paper charts is gone.” Another participant commented that, “the policies and processes at the time of paper charts were good, but there was no real monitoring, and if there was monitoring there was no mechanism for audit trails or tracking.” Another remarked that the “paper chart could be left in a doctor’s trunk of their car for weeks, and no one would notice until the chart was needed again.”

D. Theme: Providers often do not know about successful strategies being used in other organizations to effectively safeguard protected health information.

Best practices and standards are beginning to emerge around successful strategies for securing ePHI. For instance, a 2011 report on security audits of ePHI from the American Health Information Management Association (AHIMA) suggests that it is best if providers review user activities within clinical applications monthly, at a minimum, and as close to real time as possible. These EHR-generated reports of user activities, from AHIMA’s perspective, can be useful not just for detecting unauthorized access to patient information, but to establish a culture of responsibility and accountability, to reduce the risk associated with inappropriate access, to provide early detection of potential problems, and to assess security policy effectiveness (AHIMA, 2011). Covered entities are discovering real time solutions that increase the effectiveness of security practices for the protection of health information that, when shared, can be generalized across other health care populations and EHR technologies.

E. Theme: Continuous and enhanced education of employees and patients is essential to ensure baseline knowledge about requirements for maintaining the security of patients’ health information and who may have authorized access to a patient’s information, as well as to foster a culture of mutual trust.

One focus group member noted “good controls in an organization may be the only mechanism to prevent unauthorized access to patient medical records; however targeted education of staff and patients may have a greater effect on deterring internal unauthorized access.” This targeted and repeated education on the “why,” “when” and “how” of privacy and security policy may increase overall awareness of the need to protect ePHI by each employee in a health care organization. This strategy suggests that arming employees with an understanding of the larger context for what drives the need to ePHI may lead to increased awareness and decrease the urges that create curiosity, while building a culture of awareness within the health care setting.

Focus group participants noted that this internal commitment to a culture of awareness by employees can then act as a catalyst for patients who seek care within these institutions, creating a fabric of trust that is woven across the care continuum and that supports the business case for the appropriate and secure sharing of health information. Below is an example of the education and retraining on privacy and security of health information topics in a clinic setting, as explained by a focus group participant:

Example of education and retraining on privacy and security of health information in a clinic setting:

A small rural health system acquired several local clinics, noting that there were some gaps in employee knowledge on the use and protections necessary for health information. An assessment was completed, the gaps were noted, and a plan was put in place to address the specific needs of this new employee population which included initial privacy and security training for electronic health information. This training was then added to the annual education requirements for each employee and one to one support was completed for any employee who required additional training on specific targeted topics related to their need or knowledge gap. The education of employees was aimed at helping them understand the connection between their defined roles on the health care team and access to the specific information required to do their job.

Focus group participants noted that it is crucial that all employees understand the requirements for ensuring security of patient information as well as their role in carrying out these requirements. However, they also noted that each organization must commit to responding appropriately in cases where employees do not follow these requirements. The commitment to sound policy and follow-through at the employee level was consistently noted by focus group participants, who gave several examples of the actions taken when employee behavior was not changed through education. These action steps included a range of disciplinary actions for the employee per organizational policy, up to and including termination. AHIMA recommends “that organizations must be consistent in the application of their security and privacy audit policies and sanctions with no exceptions (AHIMA, 2011)” and that these sanctions should allow management some limited flexibility so that the punishment fits the incident and reduces the impact to patient care and business operations.

Rural settings reported that broad and overarching policies for monitoring of unauthorized access can be detrimental to patient care, causing employees to become afraid to do their job or contribute to patient care outside of their assigned department or role for fear of being found accessing a patient’s

record for which they were not assigned. Smaller clinics, where the employees may perform multiple job duties, indicated even though clinic staff would be accessing a patient record for their job duties, that staff members are sometimes “scared to perform their jobs” and have many questions about access because they feel unprotected in their hometown where they work and may be related to many of the patients that they serve. In this case, the staff member fear arises from needing to access the patient record of family or friends in their small community because of their job role, and not wanting their actions to be misconstrued or looked at as making an unauthorized access into that record. This fear may be the result of a lack of knowledge and indicate a need for more or better education for employees, or may reflect internal processes that need to be updated or made clearer, or perhaps definitions need to be strengthened for terminology like unauthorized access, and breach to provide better understanding.

Focus group participants noted that employee education was perhaps the single most important variable in preventing unauthorized access to records, yet education of the consumer/patient may be just as necessary so that the consumer/patient can understand all of the different individuals who have authorized access to their record because their health care job duties require it. The HRA survey comments also suggest it is important to educate the consumer/patient on what constitutes a breach of a patient health record as well as what the standard procedures are for investigating a patient complaint.

This process of education for patients, from the focus group participants’ perspective, may need to start at the provider-patient level, where there is already a trusted relationship. Participants noted it may be helpful for the patient to understand what kind of information is available to the care team and the difference in the information that an office staff or lab worker may be able to access. Focus group participants also reported that authorization and access to a patient health record is granted based on the role of the employee, and that all information is not available to all employees. Health-related information is not the only information that is accessed when a patient requires health care across any site within the care continuum.

TOPIC 2: THE FEASIBILITY OF PROVIDING PATIENTS WITH COPY OF THEIR AUDIT LOG

CONTEXT AND DEFINITIONS

Audits of access to a patient’s records are conducted within an organization using audit trails and audit logs that offer a back-end view of electronic health record system use and show key activities related to patient records. The audit log is a record of sequential activities, such as access to or revision of a patient’s record, maintained by the application or electronic health record system. The components of an audit log in the context of the HRA study are found below and in the Glossary of Common Terms at the end of the report.

Audit log, for the purpose of the Health Record Access Study, means a report that indicates who has accessed a patient's electronic health record that may include some or all of the following data elements:

- Date of access;
- Time of access;
- Name of natural person, if available, otherwise name of entity accessing the electronic designated record set;
- Description of what information was accessed, if available; and
- Description of action by the user if available, e.g., "create," "modify," "access," or "delete."

The HIPAA security rule requires that covered entities maintain proof that they have been conducting audits for at least six years, and at a minimum an organization is required to: 1) protect and retain audit logs and records on a separate server from the system that generated the audit trail; 2) restrict access to audit logs to prevent tampering or altering of audit data; and 3) retain audit trails based on a schedule that meets operational, technical, and risk management requirements (AHIMA, 2011).

These security measures are also noted by the Office of the National Coordinator's EHR certification criteria for Meaningful Use and include the following EHR audit requirements. Section 170.302(r)¹¹ outlines the audit log required elements including the ability to:

- A. **Record actions.** Record actions related to electronic health information in accordance with the standard specified in §170.210(b)
- B. **Generate audit log.** Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at §170.210(b)

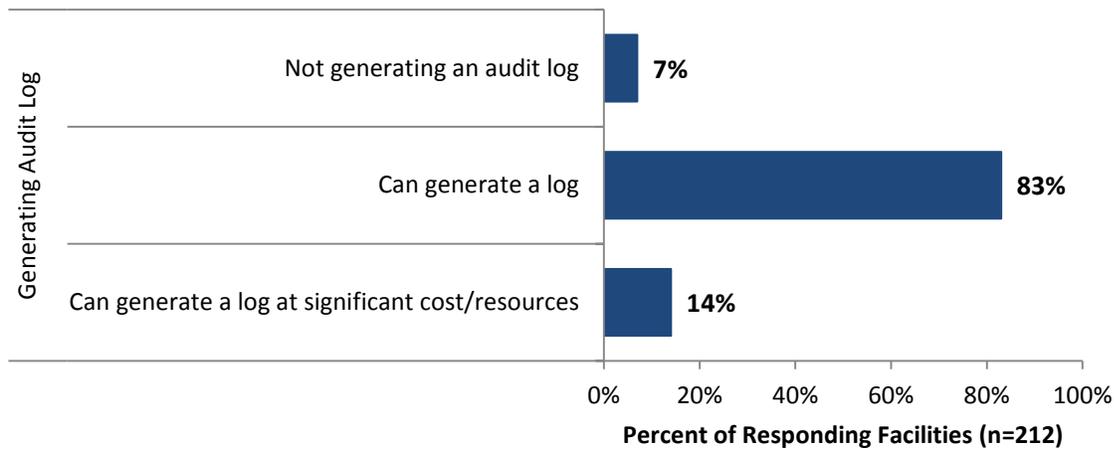
These legal requirements are meant to give guidance upon which sound organizational policies and procedures can be built for security practices such as audit logs. Minnesota law is silent on the legal requirements for audit logs and monitoring of unauthorized access.

¹¹ HIPAA Audit Log 45 CFR Section 170.302 (r) Audit log. (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in § 170.210(b).
(2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at § 170.210(b).
(s) Integrity. (1) Create a message digest in accordance with the standard specified in § 170.210(c).
(2) Verify in accordance with the standard specified in § 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.
(3) Detection. Detect the alteration of audit logs.
(t) Authentication. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.
(u) General encryption. Encrypt and decrypt electronic health information in accordance with the standard specified in § 170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for Certified EHR Technology.
(v) Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in § 170.210(a)(2).
(w) Optional Accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).

A. Theme: Audit logs can be generated, but they are not formatted in a standardized way across EHR vendors. Even if the formatting was standardized, these reports may not help providers or patients in detecting unauthorized access.

Audit logs are a record of anyone who has accessed an electronic health record. Respondents in the HRA survey report that 92% of their EHR systems can generate an audit log and seven percent cannot generate a log (Figure 5).

Figure 5: Ability of Facility’s EHR System to Generate an Audit Log that Documents Every Access to the Patient EHR



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Focus group participants also remarked that this level of detail and type of formatting makes the reports cumbersome and not useful to even privacy staff in some circumstances, requiring them to ask for help from information technology analysts who understand the coded data. Reports are not standardized and do not indicate the role of the individual who has accessed the health record. Some reports may include the hospital or clinic department where the health record was accessed; however, all access into the record is noted on the report, including those individuals who work outside of the treatment care team. This can include a number of individuals or departments, all of whom might have authority to access a health record in any particular case. Table 4 shows a sample list of departments that may access a health record but are not part of the health care treatment team.

Table 4: List of departments that may access a health record outside of the treatment team

<ul style="list-style-type: none"> • Admission Department • Infection Control • Quality Management • Compliance/Privacy • Registries- Cancer, Trauma, etc. • Health plans for review of total cost, quality management
--

- *Staff from physician offices*
- *Billing Department and Medical Coding Team*
- *Dietary Personnel*
- *Case Management Team*
- *Auditors: Internal and External*
- *Managers, Supervisors and Division Directors*
- *Legal Team, Information Technology Management Staff, Medical Records Department*
- *Contract Workers*

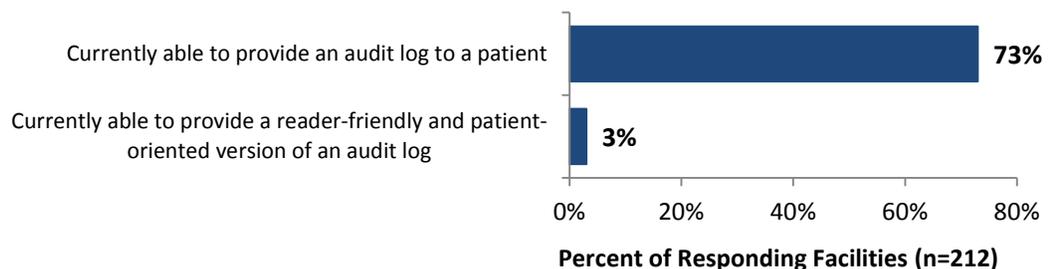
The focus groups also noted that diversity of EHR systems and multiple monitoring practices that are used present an ongoing challenge because of information fragmentation within health care organizations. In small and/or rural healthcare facilities employees often “wear many hats” for their various roles requiring broader access to information within the EHR system. In these circumstances AHIMA has recognized in a recent security audits update that the current complexities of the health care environment make it extremely challenging to limit worker access to the minimum necessary information, especially in smaller organizations and community-based hospitals where workers perform multiple functions (AHIMA, 2011). This suggests that audit logs that identify employees by role may be beneficial in some organizations, but may not fit in smaller and/or rural care settings.

Focus group participants reported that organizations do try to customize reports, download the information to another database, or make the report contents “more granular” to improve usability in their particular care setting. This increases the manual work in monitoring unauthorized access and leads to customization of processes and procedures that guide this work. It should be noted that there is add-on software can provide additional detection functionality, but it is expensive and has other potential drawbacks when layered with other customized solutions (AHIMA, 2011).

B. Theme: Audit logs can be generated, but may not be helpful or useful to a patient in their current form.

HRA survey respondents indicate that 59% of hospitals and 75% of clinics can provide an audit log to a patient, but only three percent indicate the ability to produce an audit log that is user-friendly and patient-oriented (Figure 6).

Figure 6: EHR Systems’ Capabilities to Provide a Patient with a Copy or Version of the Audit Log



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Focus group participants indicate that the audit reports currently generated from the EHR include large amounts of coded information and datasets that are not easily mapped to user access patterns in the EHR or to other information systems used in the care of patients. Table 4 gives two examples cited by some of the focus group participants of a typical audit log that is generated by their EHR system.

Table 4: Audit log generated by focus group participant’s health care organizations

Large health system in the Metro	<i>Generated a report from their EPIC EHR system for a 4 day in-patient hospital stay. The report contained over 500 pages and more than 8000 line-items of data.</i>
A health care system in Minnesota	<i>Went back 3 years into a patient’s record to create an access report as a demonstration of feasibility. The report was imported to Excel, shutting down the EHR system. The final report was more than one ream of paper.</i>

Focus group participants reported that patients who request audit logs often want to know what kinds of people have been accessing their electronic health record, or the names of individuals who have accessed their record. However, only eight percent of respondents are able to provide a log with individual staff member names redacted or coded. Some reports may list employees by name, but most use coded language which may diminish their value to patients. In addition, for compliance with data privacy laws and internal policies, as well as for employee safety and security, the content of audit logs that identify individuals by name must be reviewed before release. HRA survey respondents also noted that current EHR-generated reports do not automatically redact employee names, so this process of eliminating employee identifying information is manual.

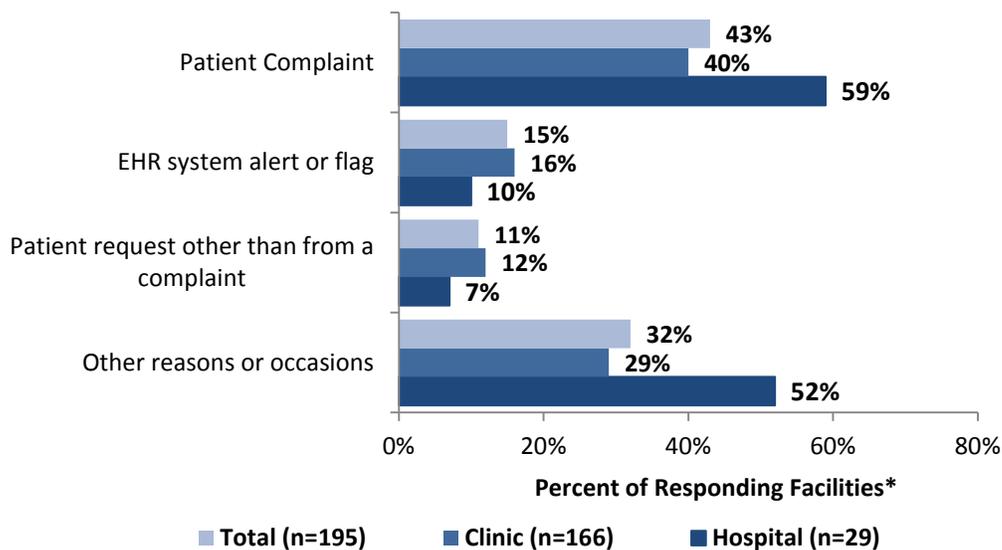
As a result, while audit logs can be generated from most EHR systems and provided to patients, focus group participants are not convinced that patients will be satisfied when they realize that the information is coded and difficult to decipher, which may lead to increased frustration on the part of the patient.

No standards currently exist for logs that are more consumer/patient friendly such as a subset set of the log, a summary profile or other leading practices for making logs more consumer/patient friendly.

C. Theme: Audit logs are most often generated based on a patient complaint, but are rarely requested by patients.

Figure 7 shows that in the past twelve months 59% of hospitals and 40% of clinics that are able to produce an audit log have generated an audit log because of a patient complaint. Only 15% of respondents have generated an audit log based on a system alert from their EHR. Of the responding facilities, 11% have generated an audit log because of a patient request other than a complaint.

Figure 7: Reason for Generating an Audit Log at least Once in Past 12 Months by Type of Facility



*Respondents who indicated that they cannot generate an audit log are not included in the base.

Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Focus group participants also reported that audit logs are rarely requested by patients, and most often what a patient really wants to do is validate that there was or was not unauthorized access to their record. Focus group participants noted that there are outlined procedures for investigating suspected unauthorized access into an electronic health record that should be followed when a patient suspects that their record may have been breached. These procedures are improved however, when a patient can give focused information to the investigator, allowing the auditing of the record to also be more targeted.

D. Theme: Consumer/patient collaboration is essential to successful investigation of suspected unauthorized access; when a patient provides specific information related to the incident, a targeted investigation can be completed more easily.

Given that the output from most audit logs can be voluminous, with results that are so comprehensive or so cryptic as to be useless to patients, some study participants noted that a better approach has been to meet with the patient/requester to narrow or focus the request and concerns. Respondent comments from both the HRA study and focus group participants reported that the few times that an audit log of an electronic health record is requested, the patient usually has a good idea of who it is that they suspect may have accessed their record without permission. This conversation with a patient was noted to be more helpful to the health care organization and to the patient than the actual audit log without this targeted information. Once a source of the suspected data breach has been identified, the privacy officer can narrow the scope of their internal investigation and focus on the suspected unauthorized access by that individual to either verify or refute the allegation by the patient. An example of a patient request for an audit log when unauthorized access is reported by a patient is provided below.

Example: Patient request for audit log to detect suspected unauthorized access to EHR

Mr. Jones is admitted to the local hospital for an acute illness. His case is unusual requiring that he be put into an isolation room to avoid cross contamination with other patients. The sign on the door says “Contact Precautions” and the hospital personnel caring for Mr. Jones have to enter the room with gowns and gloves when caring for him. The dietary aide thinks that she may know Mr. Jones, but it is difficult to see him from the hallway because of the anteroom that is between his hospital room and the hallway. To satisfy her curiosity she decides to stop at one of the standing computer stations that are for hospital personnel and logs on to check the census of patients on the floor before heading back to her work area in the kitchen.

A visitor for Mr. Jones sees the dietary aide access the computer and pulls up the list of patients on the floor, and watches as she opens the record of Mr. Jones and reviews his medical problem list. This may not appear unusual, but today the visitor notices that the dietary aide is someone that she knows, and in fact is a distant relative to Mr. Jones and that the information accessed is not necessary for the dietary aide to complete her job. The visitor reports the action of the dietary aide to Mr. Jones, who is too ill to care at the time, but after hospital discharge he makes calls to the hospital privacy officer to request a report that details everyone who has accessed his electronic health record when he was in the hospital. Mr. Jones refuses to tell the privacy officer who it is that he thinks may have accessed his record, and only acknowledges his suspicion that it is a hospital employee.

Investigation: *The Privacy Officer documents the complaint, and generates an audit log of all instances of access into Mr. Jones’ electronic health record during his most recent hospital stay. The report is hundreds of pages long and most of the information is coded and not readable, requiring hours of manual work. The privacy officer calls Mr. Jones to see if he can narrow down the person at least to their role on the health care team to decrease the manual process required to search all of the data elements in the report. This time the privacy officer explains to Mr. Jones the process for investigating suspected unauthorized access of electronic health information, including the large amount of information that needs to be manually processed.*

Outcome: *Giving Mr. Jones the right information to help him understand what information an audit log can supply and how the manual investigation process for suspected unauthorized access of an EHR is completed enables him to trust that the risk management process is in place to protect his health related information. This additional information allows Mr. Jones to understand what details are needed from him to help facilitate a complete investigation into his complaint.*

Conclusion: *The Privacy Officer is able to narrow the scope of the investigation and verify that indeed his record was accessed inappropriately, because the information reviewed was not needed for the dietary aide to do her job. Mr. Jones was notified by the Privacy Officer, and the investigation and employee follow-up were completed per hospital procedures.*

It was generally agreed upon by focus group participants that follow-up resulting from discussions with patients who suspect unauthorized access of their electronic health record may lead to quicker and

more satisfying results for the patient. Other focus group participants suggested that patients be told that an internal investigation will be conducted as a result of their complaint, and that results will be sent when completed. They also suggested that proactive educational information for patients regarding privacy practices and the roles of persons who access patient records may reduce the need for more specific information in audit logs. Other participants were not convinced that requesters would be satisfied with this more general information about the roles of people who need to access patient records.

TOPIC 3: THE FEASIBILITY OF INFORMING PATIENTS WHEN UNAUTHORIZED ACCESS IS DETECTED

CONTEXT AND DEFINITIONS

A breach or unauthorized access into an EHR includes the acquisition, access, use or disclosure of protected health information in a manner that compromises the security or privacy of the protected health information. The Minnesota Health Records Act does not include guidance for the notification of patients when unauthorized access of ePHI is detected. However, the HIPAA security rule (45 CFR 164.302) requires that a covered entity notify a patient when there is a breach that poses a significant risk of financial, reputational, or other harm to the individual.

The most recent changes to the HIPAA breach notification rule in January 2013 include modifications and requirements that were not previously included as part of HIPAA. The criteria to be used when conducting a post-breach risk assessment include:

1. Nature and extent of ePHI breach
2. To whom ePHI may have been disclosed
3. Actual breach of ePHI vs. possible breach of ePHI
4. Mitigating factors that need to be considered

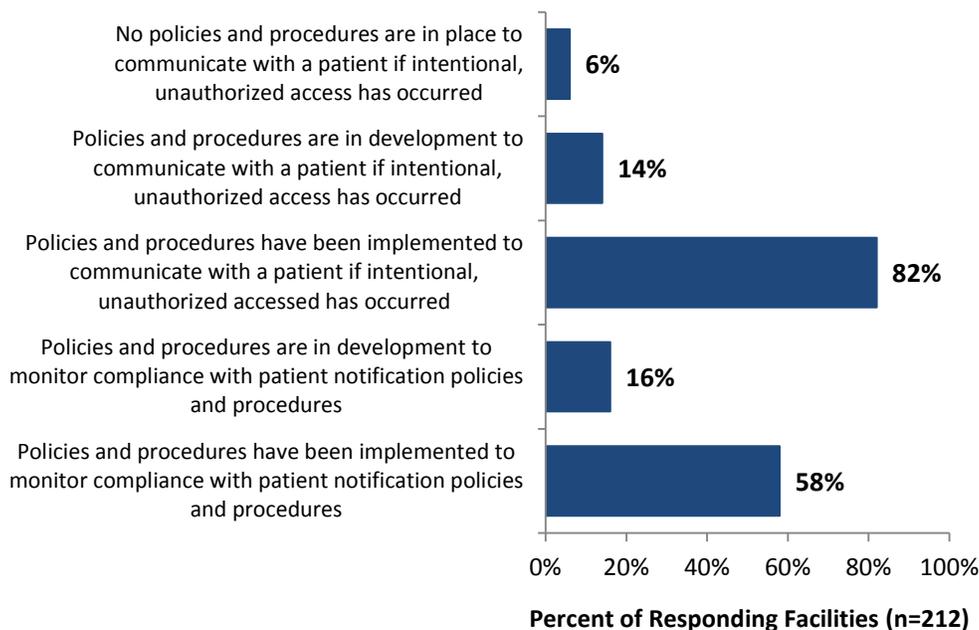
These new guidelines replace the previous determination of risk to a patient that was based on the notion of “significant harm”, providing a more objective measure of the risk associated with breach of ePHI. When a breach is confirmed and the post-breach risk assessment is completed, a covered entity must follow the HIPAA patient notifications requirements.

A. Theme: Notification of patients affected by unauthorized access usually follows the standards set by federal notification requirements, but gaps in policy and process remain.

Figure 8 shows that among HRA survey respondents, 82% report that they have implemented policies and procedures to communicate with patients in the event of a breach when the breach reaches the limits set by HIPAA for significant harm to the patient; this includes 86% percent of hospitals and 81% of clinics. An additional 14 percent of respondents indicated that notification policies and procedures are in development; while ten percent of hospitals and five percent of clinics indicate that they don't have

policies or procedures in place for notification of a patient when unauthorized access occurs indicating that there are still gaps in the process for notification of patients when unauthorized access of ePHI occurs.

Figure 8: Policies and Practices Used to Inform Patients if Intentional, Unauthorized Access to their Health Records Occurs



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

In addition, the HRA survey data shows that 86% of hospitals and 60% of clinics have implemented policies and procedures to monitor compliance with patient notification policies and procedures.

Comments from HRA survey respondents indicate that notification practices follow the federal HIPAA/HITECH breach notification requirements, and that each incident is assessed to measure the risk of significant harm to the patient per HIPAA requirements. Once the significant risk threshold is determined, that finding then mandates the notification of the patient, noting that “any additional patient notification requirements that do not incorporate the same federal standards of significant risk, would add additional burden to organizations.”

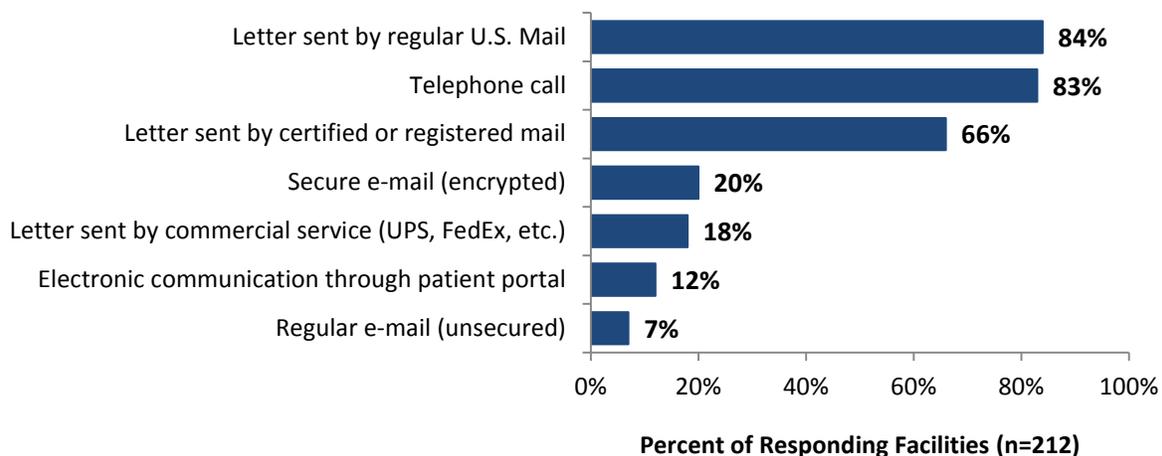
Focus group participants noted that the current HIPAA/HITECH breach notification requirements provide sound parameters from their perspective. However, further clarification of how to measure significant harm to a patient may be needed. Focus group participants also noted that the Minnesota Health Records Act is more restrictive when disclosure of health information takes place, which then encourages covered entities to create their own customized risk management protocols to manage

differences between state and federal law increasing variability in the management of suspected unauthorized access of an EHR across the state, and from one organization to another.

B. Theme: Processes for notifying patients of unauthorized access follow consistent patterns across Minnesota and have not moved to electronic encrypted forms at this time.

Most focus group participants noted that a letter is the usual or standard method of notification when unauthorized access of an electronic health record occurs. Notification letters may be preceded by or followed up with a phone call or other personal contacts. Survey data (Figure 9) confirmed that the most common methods for informing a patient of an intentional unauthorized access to their health record are through a letter sent through the mail (84%), a telephone call (83%), or a letter sent by certified or registered mail (66%). Just 20% of responding facilities use secure email and 12% use electronic communication through a patient portal.

Figure 9: Method of Communication Used to Inform a Patient of any Intentional, Unauthorized Access to their Health Record



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

None of the focus group participants described using email (secured or unsecured) to communicate breach notifications. The notion that secure email included an encryption feature that would provide additional safeguards did not change the view of focus group participants, who cited that they did not trust secure email for notifying a patient of a breach into their health record. The reasoning for not making this communication electronic was founded on fear of email account hacking, the patient not receiving the secure email because they would have to access the contents of the email through a secure portal which is sometimes tedious, and not being able to confirm that the patient received the email and was actually notified.

Patient portals were also discussed as an avenue for patient notification, but participants believed these to be suboptimal for communicating notification information because: 1) other individuals may have access to the portal; and 2) it would require that the patient access the portal before they would know that there was a message regarding unauthorized access of their electronic health record. “With mail, we know we have made a best faith effort,” said one participant. One participant noted that certified mail, when used, gets the patient’s attention but others in the focus group felt that making a phone call to the patient should always be considered, so that the patient can ask questions and get information first hand.

TOPIC 4: THE MONITORING OF REPRESENTATION OF CONSENT

CONTEXT AND DEFINITIONS

Traditional processes for the release of information require that a patient or authorized legal representative of the patient sign and date a digital or hard copy of the consent form to authorize the release of their electronic health records. Minnesota’s Health Records Act includes a unique provision called “Representation of Consent,”¹² which enables the electronic exchange of individually identifiable health information, thereby decreasing the cost, process and care delay burden of the manual paper process of patient consent for the release of information and health record sharing.

Representation of Consent (ROC) is a process in which the provider that holds a signed and dated consent form from the patient, authorizing the release of protected health information with another provider, uses the electronic health record to indicate to another provider that he or she has the patient’s consent to release information for treatment purposes. This provision reduces the need for providers to use a paper version of the consent form to show that they have the patient’s authorization to share protected health information, thereby enabling the smoother flow of electronic health data. In the absence of ROC, providers need to scan or fax paper consent forms to other treating providers, which can lead to delays in treatment. Under Minnesota consent requirements, Representation of Consent is necessary in order to efficiently move data electronically. An example workflow for Representation of Consent can be found in Appendix F.

Providers who fraudulently represent that they have a patient’s consent to exchange data may be held liable under Minnesota Statutes; the Minnesota Health Records Act states that they are liable to the patient for compensatory damages, plus costs and attorney’s fees.

¹² Minnesota Health Records Act Section 144.293 Accessed at <https://www.revisor.mn.gov/statutes/?id=144.293>

Example of Representation of Consent in practice

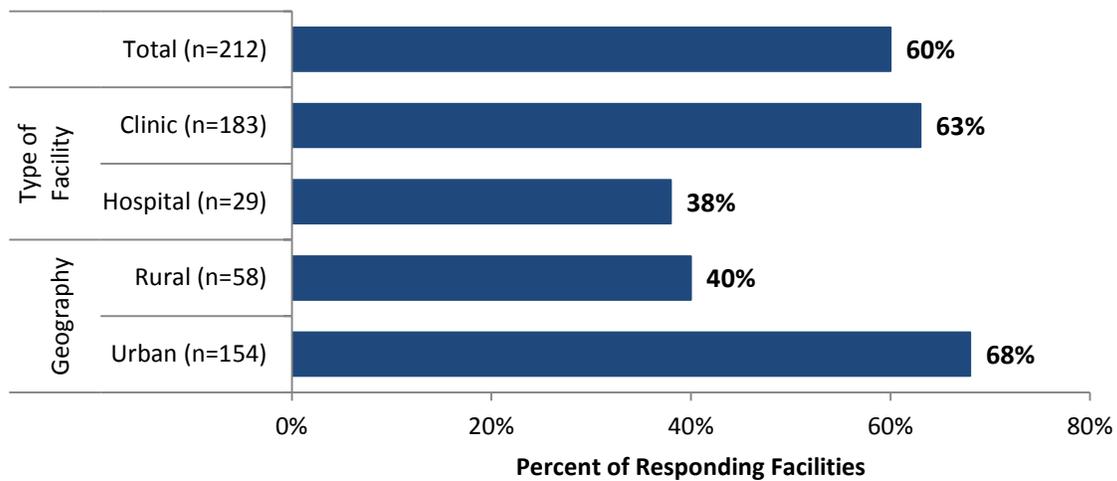
While at the Oncologist office, Mrs. Larkin finds out that she will need to have her electronic protected health information (ePHI) sent from her Primary Care Provider in Edina, MN to the office of her Oncologist in Minneapolis, MN. The Oncology office has Mrs. Larkin sign consent to release health information form which gives them permission to obtain her ePHI. The Oncology office then goes into their EHR system and opens Mrs. Larkin’s chart, noting in the EHR that they have obtained consent. A call is made to the Primary Care Provider office, which uses the same EHR system as the Oncology Office. The health information management teams at the Primary Care Provider office access the records of Mrs. Larkin to verify that the consent to release health information form is on file, and then release the electronic medical record to the Oncology office.

For ROC to be successful there must be widespread knowledge of the provision, an active procedure in place for managing patient consent preferences for each covered entity and an EHR system that is interoperable (connected to all other providers that may need patient records). Without these foundational elements it may be difficult to operationalize the ROC transaction, requiring “clunky” and inefficient work around processes to be created.

A. Theme: Representation of Consent is not widely understood or used by providers.

Figure 10 shows that HRA survey respondents indicate that just 60% of HRA survey respondents have providers (e.g., physicians) who are using representation of consent. Only 38% of hospitals and 63% of clinics currently use Representation of Consent, and the use of ROC is higher in urban areas (68%) than in rural areas (40%).

Figure 10: Percent of Facilities that Request a Copy of Patient Electronic Health Records by Using Representation of Consent



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

ROC allows for the communication of patient authorization to release health information without having to fax a copy of the consent to the requesting or receiving provider. For electronic records, focus group members that used ROC found that it is the best way to indicate consent, “there is not another way to show consent,” as stated by one focus group participant; however HRA survey data shows that 82% of respondents still use faxing to provide proof that patient consent to release health information was obtained.

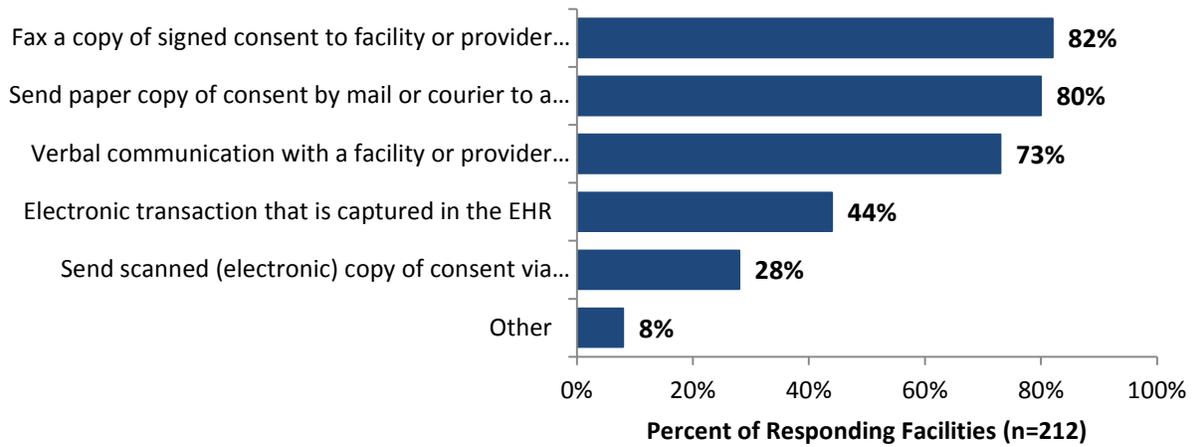
The use of ROC varied between focus group participants, with some noting that they did not use it and some stating that they did not understand the concept. When a description of ROC was provided at the focus group meeting, these same participants believed that ROC would allow for better data sharing practices, and noted that they would go back to their organizations and educate others on its usefulness, with the goal of potentially developing ROC policies and processes. One participant noted that they had considered ROC, but decided as a health system to use a multi-layered consent process that begins with a comprehensive consent form and continues with individual authorization based on the patient specific health care needs while they are inpatient during their episode of care. Still other participants are considering the use of ROC, but had not yet formally adopted its use within their provider offices.

B. Theme: Though Representation of Consent should increase electronic health information exchange; health care providers continue to use other non-electronic methods to communicate patient consent to share health information.

There are several allowable methods for communicating patient consent, including verbal, fax, paper copy, scanned copy sent via secure email, and electronically through the EHR. Because paper copies of patient consent are still in broad use, it is not uncommon for providers to use more than one method to indicate patient consent, as the communication mode may depend on the preferences and/or capabilities of the receiving party.

Figure 11 shows that HRA survey respondents report that the most common mode of communicating patient consent is by faxing a paper copy of the signed consent form (82%) or sending it by mail or courier (80%). Verbal communication is also used by 73% of the survey population. Less than half (44%) of responding facilities use electronic transmission of patient consent through the EHR, and just 28% use secure email to send a scanned copy of the consent. In other words, while electronic mechanisms are in place to capture patient health information, current consent and release of information practices have not fully moved to electronic processes.

Figure 11: Methods used for communicating to another provider with whom the facility has patient consent to share patient health data.

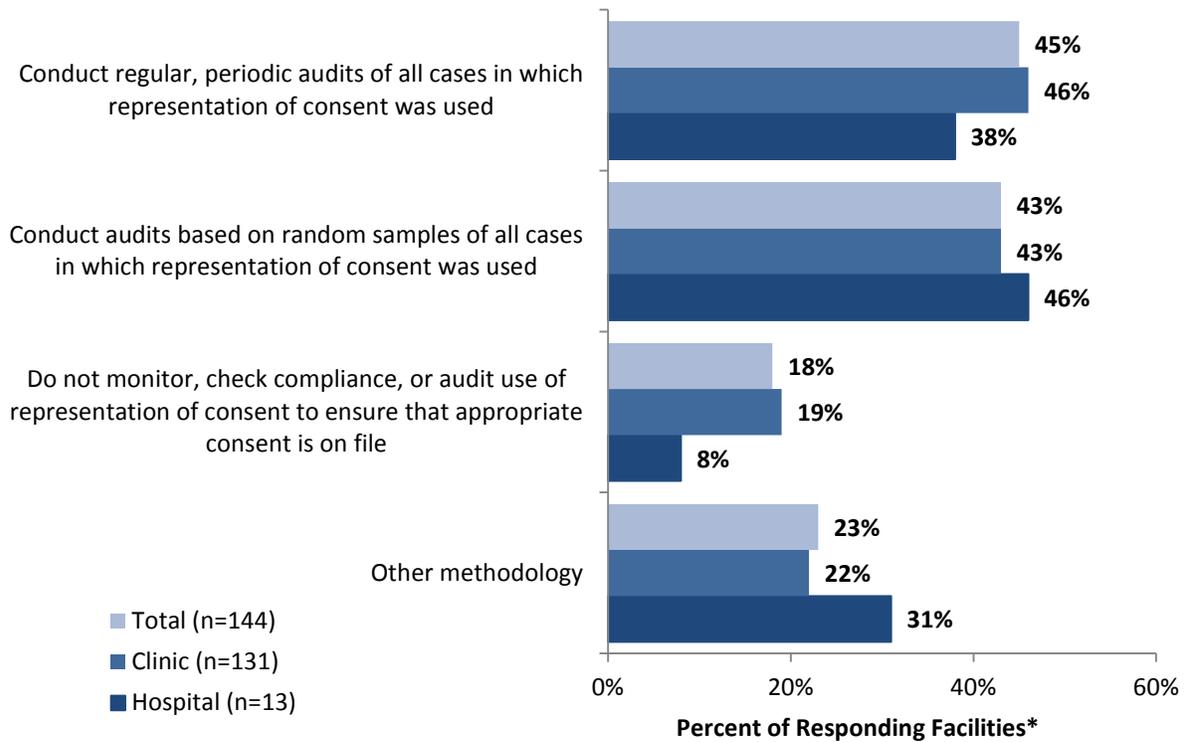


Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey. This information reflects communication with providers outside of their health system.

C. Theme: Some facilities have process in place to monitor the use of ROC, including auditing procedures. Gaps do exist, however, in how the auditing procedures are conducted.

Figure 12 shows that 38% of hospitals and 46% of clinics conduct regular, periodic audits of all cases in which ROC was used. Of those that use ROC, 19% of clinics and eight percent of hospitals do not monitor, check compliance, or audit use of ROC to ensure that appropriate patient consent is on file. Overall, 43% of those that use ROC conduct audits based on random samples of cases in which ROC was used, and 23% use other methodologies to complete audits, indicating that guidance may be needed to identify and implement best-practice monitoring procedures for verifying that patient consent is on file.

Figure 12: Methods Used for Monitoring, Compliance Checks, and Audit Procedures to ensure that Appropriate Patient Consent is on File

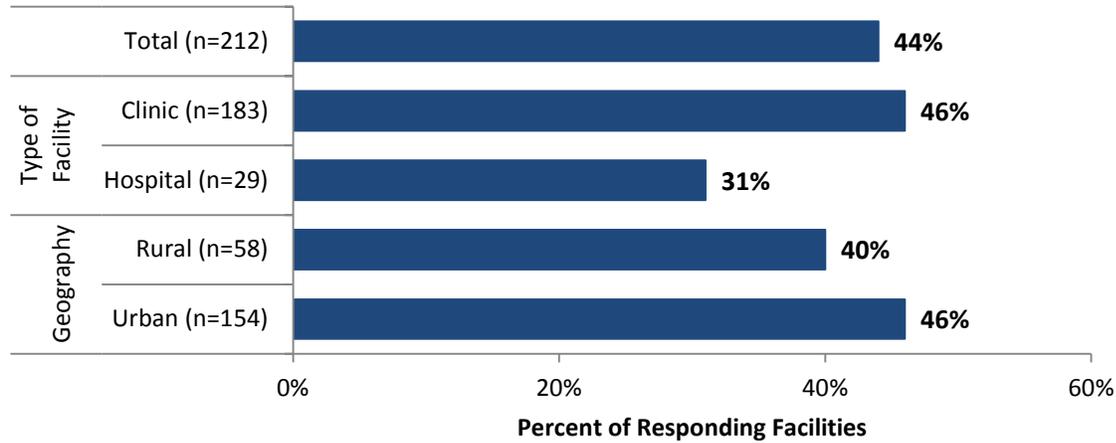


*Respondents who indicated that they do not use representation of consent are not included in the base.
 Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

D. Theme: Few EHR vendors have incorporated requirements for electronic consent features.

Figure 13 shows that significantly more clinics are able to capture patient consent directly in their EHR system (as opposed to capturing a scanned copy of a consent form), at 46%, compared to 31% for clinics and hospitals. Among responding facilities that do not capture patient consent within the patient record, almost half (49%) have plans to implement this in the future. Another 42% do not know the answer to this question.

Figure 13: Facilities Able to Capture Patient Consent Transaction in the EHR by Facility Type and Geography



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey

All others who use ROC need to audit individual patient health records to find documentation of the patient consent and any disclosures that had been made. Some participants noted that their organizations “audit” their partners when they receive ROC, to ensure that proper consent is on file to share ePHI.

Survey and focus group participants noted that only one EHR vendor currently has a mechanism in its EHR to confirm that patient consent to release ePHI was obtained, as a way to track and substantiate that permission was obtained. *Care Everywhere*, an interoperable feature of the *EPIC* EHR system, allows an authorized user to check a box that represents that the health care workforce member has permission to request electronic records within the EPIC system. This feature is only for EPIC users and was added at the request of Minnesota EPIC users; a paper copy is still obtained, scanned into the EHR and then the box is checked in the patients’ electronic health record to indicate that the paper process has been completed.

Others that use ROC document permissions in the health record along with details that state why the disclosure was made, according to the requirements in the Minnesota Health Records Act. The participants that were not EPIC users noted that “vendor requirements need to change to better match our needs” since the age of paper records has passed, and the era of electronic and interoperable health records has arrived. It was also noted that consent practices overall for the sharing of health information remain in a hardcopy manual form, and that many providers continue to fax hard copies to other providers to show proof of patient authorization to release health information. For EHR users that had the “check the box” feature, monitoring ROC was found to be much less manual.

E. Theme: Challenges prevent some providers from using Representation of Consent

1. ROC can create a perception of distrust between providers

Under current Minnesota law, liability for misrepresentation of consent falls on the provider of the record. With so many different EHR systems that are not connected and that are not interoperable, focus group participants report that providers feel that they have to rely on the written communication of consent and not the electronic version of ROC.

Focus group participants were quick to note that in most cases they are willing to trust each other as the holders of patient consent under some conditions, but because of the liability on the provider that holds the consent in the “representation of consent” transaction trust may be limited, which decreases the use of representation of consent.

Focus group participants also pointed out that HIPAA rules for use and disclosure of ePHI are more easily operationalized because they cover the work of health care for treatment, health care operations and payment, meaning that it is much easier to share information that is needed at the point of care as opposed to Minnesota Health Records Act, which requires that patient consent be obtained each time that patient information is going to be disclosed, no matter what the reason.

2. Interstate patient consent transactions are not feasible

Focus group participants indicated that process issues exist when sharing ePHI with other states, as the Minnesota Health Records Act law does not apply to providers outside the state of MN. EHR vendors, and the providers that use them, provide services across state lines, but even those EHR vendors that are interoperable from one state to another report that this interstate patient consent process is difficult to manage and operationalize. Even those who have the “check the box” feature to show patient consent for sharing health records report that the current consent laws in Minnesota are more stringent, so the patient consent to release health information to a provider in another state requires that a new paper version of the release of information form must be signed by the patient who needs health care services in another state, which in essence reverts the electronic consent process back to a manual paper process.

Health care organizations that have EHRs and that support electronic consent processes in their record systems report that they would need to take on additional capital budget costs to develop custom solutions, and they would need to connect to multiple EHR vendor types to operationalize this solution.

3. Multiple customized patient consent to release information forms exist

Focus group participants report that most health care organizations have created their own notice of privacy protections forms based on the unique needs of their organization, and that part of that customization includes the patient consent to release information forms. Participants noted that form standardization (including the ROC information) across covered entities may be one solution; however other participants reported that they prefer their customized solution for consent forms. Focus group participants noted that non-standardized forms may increase confusion on the part of the patient who must sign multiple forms to consent and authorize health care treatment, operations and payment. A standardized consent to release health information form endorsed by the Commissioner of Health and MDH does currently exist and is available on the MDH website.

RECOMMENDATIONS AND CONSIDERATIONS

These recommendations are key actions necessary to further strengthen privacy and security of electronic protected health information in Minnesota. Recommendations are broad and implementation may include action by some or all e-Health stakeholders, including the legislature, state agencies, consumers, hospitals, clinics, health care providers, health information exchange service providers and electronic health information technology vendors.

1. RECOMMENDATIONS REGARDING THE PROCESS FOR MONITORING UNAUTHORIZED ACCESS TO PATIENT HEALTH RECORDS

- A. Identify best practices and existing national standards for proactive and reactive monitoring procedures to detect unauthorized access to electronic protected health information, and develop guidance that can be shared with health care organizations statewide.
- B. Create and disseminate user-friendly informational materials for patients on consent and release of information practices, including common ways that health information may be used and/or accessed within a health care organization.

2. RECOMMENDATIONS REGARDING THE FEASIBILITY OF PROVIDING PATIENTS WITH A COPY OF THEIR AUDIT LOG TO DETECT UNAUTHORIZED ACCESS OF THEIR HEALTH RECORD

- A. Identify and/or develop and implement consumer-friendly audit log standards for Electronic Health Records (EHRs).
- B. Collect and share best practices and guidance on consumer / provider collaboration in cases of suspected unauthorized access, including standard processes and actions.
- C. Endorse federal actions that improve EHR certification criteria for standardized and improved EHR capabilities to produce patient-readable audit logs.

3. RECOMMENDATIONS REGARDING THE FEASIBILITY OF INFORMING PATIENTS WHEN UNAUTHORIZED ACCESS IS DETECTED

- A. Identify and share best practices for notifying patients when unauthorized access to an EHR is detected, and provide technical assistance to providers as necessary to implement best practices.

4. RECOMMENDATIONS REGARDING THE MONITORING OF REPRESENTATION OF CONSENT

- A. Develop consensus standards for monitoring of the use of representation of consent (ROC)
- B. Support education of the health care workforce on representation of consent (ROC) to ensure widespread understanding of the provision.
- C. Ensure that processes are in place for appropriate and efficient use of ROC transactions, and for monitoring that use of ROC is in compliance with the requirements of the Minnesota Health Records Act.

5. OTHER RECOMMENDATIONS AND CONSIDERATIONS

To further address findings of this report, the Minnesota Department of Health should:

- A. Convene stakeholders to use Health Record Access Study findings as a basis for considering modifications to Minnesota statutes to reduce complexities due to disparate state and federal privacy and security rules.
- B. Use its annual health information technology surveys of hospitals and clinics to monitor progress towards implementation of best practices and state/federal requirements related to privacy and security of electronic health information.
- C. Expand efforts to develop and deliver training to healthcare providers and other staff in health care facilities on electronic privacy and security issues surrounding health information including: creating a culture of awareness of risk related to unauthorized access; knowledge of individual accountability for the handling and disclosure of health information; foundational knowledge base of the current EHR mechanisms that deter unauthorized access; and outline permissible and impermissible uses and disclosures of electronic protected health information.

BIBLIOGRAPHY

- AHIMA. (2011, March). *Security Audits of Electronic Health Information (Updated)*. Retrieved November 14, 2012, from American Health Information Management Association: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048702.hcsp?dDocName=bok1_048702
- California Office of Privacy Protections. (2012). *Recommended Practices on Notice of Security Breach Involving Personal Information*. State of California.
- Chhanabhai, P. H. (2007). Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine*, 8.
- Department of Health and Human Services. (2007, March). *Health and Human Services; HIPAA Security Series: Topic 1: Security 101 for Covered Entities*. Retrieved December 13, 2012, from [hhs.gov](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf): <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>
- Department of Health and Human Services. (2003). *45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule*. HHS.
- Department of Health and Human Services. (2013, January 25). *Federal Register; HIPAA Final Rule 45 CFR Parts 160 and 164*. Retrieved January 29, 2013, from United States Government Printing Office: <http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>
- Dimitropoulos, L. e. (2011). Public attitudes toward health information exchange: perceived benefits and concerns. *American Journal of Managed Care*, SP111-6.
- Dunlevy, S. (2012, August 10). *AustralianIT*. Retrieved Sept 20, 2012, from The Australian: <http://www.theaustralian.com.au/australian-it/government/experts-brand-e-health-audit-trail-as-gobbledegook/story-fn4htb9o-1226447421780>
- Eramo, L. (2011). Keys to Effective Breach Management. *For the Record*, Vol. 23 No. 2 P. 14.
- Healthcare Information and Management Systems Society (HIMSS)*. (2009). Retrieved January 22, 2013, from HIMSS.org: <http://www.himss.org/content/files/090909BreakTheGlass.pdf>
- FairWarning White Paper. (2012). *Evaluating Care Provider Readiness for an External HIPAA Audit How and Why Privacy Breach Detection Provides a Sustainable Foundation for HIPAA and ARRA HITECH Compliance*. Retrieved October 14, 2012, from Fairwarning.com: <http://www.fairwarning.com/whitepapers/2012-02-WP-FAIRWARNING-AUDIT-READINESS.pdf>
- Gendron, M. (2011, August 31). *Veriphyr Identity and Access Intelligence*. Retrieved October 14, 2012, from Hjort, B. (2011, March). *Security Audits of Electronic Health Information (Updated)*. Retrieved November 14, 2012, from AHIMA: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048702.hcsp?dDocName=bok1_048702
- Hodach, R. M. (2012). *ACOs and Population Health Management; How Physician Practices Must Change to Effectively Manage Patient Populations*. Retrieved December 17, 2012, from American Medical Group Association: AMGA.org: http://www.amga.org/AboutAMGA/ACO/Articles/CaseStudy_final.pdf
- Horowitz, B. (2011, March 16). *Half of Americans Distrust Privacy of EHRs: CDW*. Retrieved September 20, 2012, from eWeek Enterprise IT Technology News, Opinion and Reviews: <http://www.eweek.com/c/a/Health-Care-IT/Half-of-Americans-Distrust-Privacy-of-EHRs-CDW-789600/>

Minnesota Legislature- 85th Legislative Session. (2007-2008). *Minnesota Health Records Act Section 144.293*. Retrieved September 25, 2012, from Minnesota State Government: <http://www.health.state.mn.us/e-health/mpsp/healthrecordsact2007.pdf>

O'Donnel, H. e. (2011). Healthcare consumers' attitudes towards physician and personal use of health information exchange. *Journal of Gen Internal Medicine*, 1019-26.

Office of the National Coordinator for Health Information Technology. (2008). *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*. U.S. Department of Health and Human Services.

Office of the National Coordinator for Health Information Technology. (September 30, 2012). *Consumer Engagement in Health Information Exchange*. Audacious Inquiry .

Patient Privacy vs. the urge to snoop. (2012, June 8). *Health Beat; A Blog about all things Health*. Minneapolis, MN, United States: Wordpress.

Patel, V. A. (2011). Consumers attitudes toward personal health records in a beacon community. *American Journal of Managed Care*, e104-20.

PR Newswire. (2012, November 29). MiHIN to Integrate HIPAAT Consent Management and Auditing Tools. Lansing, Michigan, United States.

Roney, K. (2013, January 10). *ONC Investigates Patients' Concerns About Health Information Exchanges*. Retrieved January 11, 2013, from Becker's Hospital Review: <http://www.beckershospitalreview.com/healthcare-information-technology/onc-investigates-patients-concerns-about-health-information-exchanges.html>

Simmons, J. (2011, June 2). *FierceEMR.com*. Retrieved September 20, 2012, from FierceEMR: <http://www.fierceemr.com/story/hhs-patients-should-know-who-views-their-ehr/2011-06-02#ixzz25W16D6C6>

Environmental Scan of Available Literature and Sources

California Office of Privacy Protections. (2012). *Recommended Practices on Notice of Security Breach Involving Personal Information*. State of California

http://www.privacy.ca.gov/business/recom_breach_prac.pdf

Cost of a Data Breach A benchmark study of breaches at 51 organizations found that the average cost of a data breach in 2010 was \$214 per record, making it the fifth year in a row that such costs have risen.⁴ The study found that direct costs, such as printing, postage and legal fees, accounted for 34 percent of the total cost. Indirect costs, primarily lost customers, represented 66 percent. The study also found that for the first time, malicious or criminal attacks, which accounted for nearly a third of the incidents, were the most costly. Such breaches cost an average of \$318. The impact of a data breach on reputation can also be significant. In a 2011 study, senior-level managers estimated that the loss or theft of confidential customer information diminished the value of their brand by an average of 21 percent and restoring the damaged reputation took an average of a year.

Document reviews breach notification practices similar to HIPAA, but at the state policy level

Chhanabhai, P. H. (2007). **Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures.** *Medscape General Medicine*, 8.

BACKGROUND: Healthcare has entered the electronic domain. This domain has improved data collection and storage abilities while allowing almost instantaneous access and results to data queries. Furthermore, it allows direct communication between healthcare providers and health consumers. The development of privacy, confidentiality, and security principles are necessary to protect consumers' interests against inappropriate access. Studies have shown that the health consumer is the important stakeholder in this process. With the international push toward electronic health records (EHRs), this article presents the importance of secure EHR systems from the public's perspective.

OBJECTIVE: To examine the public's perception of the security of electronic systems and report on how their perceptions can shape the building of stronger systems.

METHODS: A cross-sectional survey (September-November 2005) of people attending healthcare providers (n = 400) was conducted in the 4 major cities in New Zealand. Participants were surveyed on computer use, knowledge of EHR-proposed benefits and issues, security issues, and demographics.

RESULTS: A total of 300 surveys were completed and returned (a 75% response rate), with 180 (60%) being women. One hundred eighty-eight (62.6%) had not heard of EHRs, with those who had heard of them indicating that they were a positive innovation in the health sector. However, 202 (73.3%) participants were highly concerned about the security and privacy of their health records. This feeling was further accentuated when participants were asked about security of electronic systems. Participants were worried about hackers (79.4%), vendor access (72.7%), and malicious software (68%). Participants were also introduced to various security systems, and in each case, over 80% of participants believed that these would make EHR systems more secure. A number of chi-square tests were carried out with each variable, and it was found that there were strong relationships between age, location, computer use, EHR knowledge, and the concern for privacy and the security of medical records (P < .05). The survey also showed that there was a very small difference (9.8%) between health consumers who believed that paper records are more secure than EHRs and those who believed otherwise.

CONCLUSIONS: The findings showed that for the EHR to be fully integrating in the health sector, there are 2 main issues that need to be addressed: The security of the EHR system has to be of the highest level, and needs to be constantly monitored and updated. The involvement of the health consumer in the ownership and maintenance of their health record needs to be more proactive. The EHR aims to collect information to allow for "cradle to the grave" treatment; thus, the health consumer has to be seen as a major player in ensuring that this can happen correctly. The results from this study indicated that the consumer is ready to accept the transition, as long as one can be assured of the security of the system.

Department of Health and Human Services. (2003). **45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule.**

HHS. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>

The Federal Register, volume 68, No. 34 citing the HIPAA security rule, the safeguards, protections and enforcement of the final rule.

Dimitropoulos, L. e. (2011). **Public attitudes toward health information exchange: perceived benefits and concerns.** *American Journal of Managed Care*, SP111-6.

OBJECTIVES: To characterize consumers' attitudes regarding the perceived benefits of electronic health information exchange (HIE), potential HIE privacy and security concerns, and to analyze the intersection of these concerns with perceived benefits.

STUDY DESIGN: A cross-sectional study

METHODS: A random-digit-dial telephone survey of English-speaking adults was conducted in 2010. Multivariate logistic regression models examined the association between consumer characteristics and concerns related to the security of electronic health records (EHRs) and HIE.

RESULTS: A majority of the 1847 respondents reported they were either "very" or "somewhat" concerned about privacy of HIE (70%), security of HIE (75%), or security of EHRs (82%). Concerns were significantly higher ($P < .05$) among employed individuals 40 to 64 years old and minorities. Many believed that HIE would confer benefits such as improved coordination of care (89%). Overall, 75% agreed that the benefits of EHRs outweighed risks to privacy and security, and 60% would permit HIE for treatment purposes even if the physician might not be able to protect their privacy all of the time. Over half (52%) wanted to choose which providers access and share their data.

CONCLUSIONS: Greater participation by consumers in determining how HIE takes place could engender a higher degree of trust among all demographic groups, regardless of their varying levels of privacy and security concerns. Addressing the specific privacy and security concerns of minorities, individuals 40 to 64 years old, and employed individuals will be critical to ensuring widespread consumer participation in HIE.

Dunlevy, S. (2012, August 10). *AustralianIT*. Retrieved Sept 20, 2012, from The Australian:

<http://www.theaustralian.com.au/australian-it/government/experts-brand-e-health-audit-trail-as-gobbledegook/story-fn4htb9o-1226447421780>

<http://www.theaustralian.com.au/australian-it/government/experts-brand-e-health-audit-trail-as-gobbledegook/story-fn4htb9o-1226447421780>

E-Health consultant and medical Dr. David More accessed the audit trail on his own e-health record this week and revealed the "gobbledegook" result on his Health Information Technology blogsite.

The stream of confusing numbers that resulted showed the audit amounted to little more than a computer system log and that it was not designed for the purpose, he said.

"It's just not clear enough and not structured enough for ordinary citizens to work out what is going on," he said.

FairWarning White Paper. (2012). *Evaluating Care Provider Readiness for an External HIPAA Audit How and Why Privacy Breach Detection Provides a Sustainable Foundation for HIPAA and ARRA HITECH Compliance*. Retrieved October 14, 2012, from Fairwarning.com:

<http://www.fairwarning.com/whitepapers/2012-02-WP-FAIRWARNING-AUDIT-READINESS.pdf>

<http://www.fairwarning.com/whitepapers/2012-02-WP-FAIRWARNING-AUDIT-READINESS.pdf>

Best Practice Summary

Prior to ARRA HITECH of 2009, the consequences of a patient privacy breach were negligible and HIPAA was not enforced so most conscientious care providers made a reasonable effort to fulfill the above provisions by conducting manual investigations of audit logs for a limited number of critical systems. These activities were typically conducted on a patient complaint-driven basis by non-dedicated personnel. Some care providers also conducted semi-automated manual random patient audits by visually examining audit logs in an effort to fulfill the Information Systems Activity Review requirement. These manual processes prove to be unsustainable, immensely time consuming, monotonous and largely ineffective. For example, due to the time required to conduct a manual patient audit, it is only feasible for far less than 1 % of patient encounters to be randomly reviewed. In the case of complaint driven investigations, a reactionary care provider might dedicate days, weeks or even months of personnel to investigate a subset of the systems that access PHI. Almost always, the investigation is an "extra duty" to investigation team's full-time roles. Lastly, by definition care providers are non-compliant with HIPAA unless they are able to conduct these activities for **all** "information systems that contain or use electronic protected health information".

The semi-manual processes map to **Level 3** in this white paper's Best Practices Pyramid. At any given instance in time, a care provider may be compliant with the afore described HIPAA requirements, however, both the technology and business processes are non-sustainable and provide limited ability to scale with growing governmental privacy mandates. Leading care providers recognized the limitations of the semi-manual approach and began deploying Privacy Breach Detection technology that maps to **Levels 4 and 5** of the Best Practices Pyramid. Lastly, unconcerned care providers consider all of these efforts not worth the time, expense and energy and continue to map to **Level 1 and Level 2 of the Best Practices Pyramid**. These care providers have significant risk exposure to breaches and external audits that likely go well beyond Audit Controls and Systems Activity below.

As this white paper proceeds, there are several other general HIPAA provisions that should be considered as they can largely be addressed within the thread of effort of a Privacy Breach Detection deployment. Compliance minded care providers realize that the deployment of a technology is not sufficient for compliance. In fact, appropriate technology based on the care provider's size as well as sustainable appropriate business processes are required for compliance.

Eramo, L. (2011). **Keys to Effective Breach Management**. *For the Record*, Vol. 23 No. 2 P. 14.

<http://www.fortherecordmag.com/archives/013111p14.shtml>

Covers multiple aspects of PHI data breaches including audit procedures, informing patients of a breach, as well as proactive approach to monitoring.

“Every organization will experience breaches,” says Ali Pabrai, CISSP, CSCS, CEO of ecfirst, Inc, which specializes in delivering IT services to the healthcare and financial industries. “When you experience a breach, that’s not the time to discover you have a procedure that doesn’t work. You don’t want to be scrambling to figure out what to do. You just won’t have the time to go through that.”

The notification process under the HITECH Act can be extremely labor intensive and costly, says Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA, director of practice leadership at the AHIMA. “Breach notification requires a lot of expenditures. It takes a lot of money to respond,” he says.

The average cost of a data breach is \$204 per compromised customer or patient record, according to a January 2010 study conducted by the Ponemon Institute, which performs independent research on privacy, data protection, and information security. This includes \$144 in indirect costs and \$60 in direct costs. The cost per record of a data breach involving a laptop computer or other mobile device is \$225.

Perhaps far more damaging in the long run is the fact that breaches could cost organizations their reputations. Poorly executed or confusing data breach response efforts can lead to other negative consequences, such as patients who seek care elsewhere, says Rhodes.

“To come out and say that you have a breach can be really detrimental,” he says. Even in small communities, patients who are concerned about the privacy and security of their health information can avoid seeking care from a provider that encountered a breach and simply drive up the road to another provider with a better reputation for health information security, he adds.

In an April 2008 study conducted by the Ponemon Institute, 63% of survey respondents said notification letters they received offered no direction on the steps they should take to protect their personal information. As a result, 31% said they terminated their relationship with the organization, and 57% said they lost trust and confidence in the organization.

Gendron, Marc. (2011, August 31). **Veriphyr Identity and Access Intelligence**. Retrieved October 14, 2012, from Hjort, B. (2011, March). **Security Audits of Electronic Health Information** (Updated). Retrieved November 14, 2012, from AHIMA:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048702.hcsp?dDocName=bok1_048702

<http://blog.veriphyr.com/2011/08/over-70-of-healthcare-providers.html>

Some of the report’s key findings include:

- Top breaches in the past 12 months by type:
 - Snooping into medical records of fellow employees (35%)
 - Snooping into records of friends and relatives (27%)
 - Loss /theft of physical records (25%)
 - Loss/theft of equipment holding PHI (20%)
- When a breach occurred, it was detected in:
 - One to three days (30%)
 - One week (12%)
 - Two to four weeks (17%)

- Once a breach was detected, it was resolved in:
 - One to three days (16%)
 - One week (18%)
 - Two to Four weeks (25%)
- 79% of respondents were “somewhat concerned” or “very concerned” that their existing controls do not enable timely detection of breaches of PHI
- 52% stated they did not have adequate tools for monitoring inappropriate access to PHI

Hjort, B. (2011, March). ***Security Audits of Electronic Health Information (Updated)***. Retrieved November 14, 2012, from AHIMA:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048702.hcsp?dDocName=bok1_048702

Determining What to Audit

It would be prohibitive to perform security audits on all data collected. Good-faith efforts to investigate the compliance level of individuals educated on privacy and information security issues can be achieved through a well-planned approach.

In determining what to audit, organizations must identify and define "trigger events," or the criteria that will flag questionable access of confidential ePHI and prompt further investigation. Some triggers will be appropriate to the whole organization, while others will be specific to a department or unit. Once identified, trigger events should be reviewed on a regular basis, such as annually, and updated as needed.

Examples of trigger events include employees viewing:

- The record of a patient with the same last name or address as the employee
- VIP patient records (e.g., board members, celebrities, governmental or community figures, physician providers, management staff, or other highly publicized individuals)
- The records of those involved in high-profile events in the community (e.g., motor vehicle accident, attempted homicide, etc.)
- Patient files with isolated activity after no activity for 120 days
- Other employee files across departments and within departments (organizations should set parameters to omit legitimate caregiver access)
- Records with sensitive health information such as psychiatric disorders, drug and alcohol records, domestic abuse reports, and AIDS
- Files of minors who are being treated for pregnancy or sexually transmitted diseases
- Records of patients the employee had no involvement in treating (e.g., nurses viewing patient records from other units)
- Records of terminated employees (organizations should verify that access has been rescinded)
- Portions of a record that an individual's discipline would not ordinarily have a need to access (e.g., a speech pathologist accessing a pathology report)

Those individuals who review the audit logs should evaluate the number of trigger events and the breadth of the coverage chosen as well as the system's ability to log the data desired for such reviews.

Implementing Audit Tools

Certified EHRs that meet the stage 1 meaningful use criteria will also meet health IT audit criteria and may provide enough detail to determine if there was an unauthorized access into a patient's record.

These built-in audit logs can easily contain millions of entries of application transactions. Searching through these detailed logs to find the specific information needed when conducting an investigation regarding a particular encounter can take a significant amount of time and requires some specialized skills in reading and interpreting the data.

Breaches often go undetected in manual reviews of audit logs due to the sheer volume of data. Conducting random audits of user access is like the old cliché "searching for a needle in a haystack."

To help ensure greater efficiency in audit reviews, many organizations rely on third-party audit tools, which systematically and automatically analyze data and quickly generate reports based upon search criteria matching the organization's audit strategy or defined triggers.

Specialized audit tools can be programmed to:

- Detect potentially unauthorized access to a patient's record, often using a variety of prewritten queries and reports such as a match between the user's and the patient's last names.
- Collect and automatically analyze information in-depth.
- Detect patterns of behavior.
- Provide privacy and security officers or compliance personnel with alert notifications of potential incidents or questionable behavior.
- Collect the audit logs from other applications for correlation and centralized storage and analysis. For example, the logs from a time-keeping system may be used to verify if an employee was on the clock when an unauthorized access occurred.
- Present reports in an easy-to-read Web page or dashboard.

Third-party tools can be expensive to purchase and install. Up-front costs may include audit software, server and operating system for running the software, and labor costs for installation, training, and modification. In addition, there may be annual licensing and support fees, which must be factored into an organization's operating budget.

Some vendors offer audit tools as software as a service, or SaaS. This eliminates many of the up-front costs because the vendor supplies and owns the necessary hardware and software and provides the programming support. The healthcare organization pays a monthly fee to use the tool, usually through a Web interface.

Determining When and How Often to Audit

Due to a lack of resources, organizations typically examine their audit trails only when there is a suspected problem. Although this is a common practice, it is definitely not a best practice.

It is imperative an organization's security audit strategy outlines the appropriate procedure for responding to a security incident. However, it must also define the process for the regular review of audit logs. At a minimum, review of user activities within clinical applications should be conducted monthly. It is best to review audit logs as close to real time as possible and as soon after an event occurs as can be

managed.† This is especially true for audit logs, which could signal an unauthorized access or intrusion into an application or system. Automated audit tools can be helpful for providing near real-time reports.

Evaluating Audit Findings

Department managers and supervisors are in the best position to determine the appropriateness of staff access. Therefore, they should review the audit reports.

The organization's information security and privacy officials must provide education to the directors, managers, and supervisors responsible for reviewing security audit report findings so they are equipped to interpret results and determine appropriate versus inappropriate access based on defined and approved access permissions.†

Protecting and Retaining Audit Logs

HIPAA requires that covered entities maintain proof that they have been conducting audits for six years. Such documents may include policies, procedures, and past audit reports. State statutes of limitations relative to discoverability and an organization's records management policies may require that this information be kept longer.

Organizations must review pertinent regulatory requirements, including applicable federal and state laws, in determining the appropriate retention period for security audit logs. Security and privacy officials should collaborate to establish the most effective schedule for the organization

Hodach, R. M. (2012). *ACOs and Population Health Management; How Physician Practices Must Change to Effectively Manage Patient Populations*. Retrieved December 17, 2012, from American Medical Group Association: AMGA.org:

http://www.amga.org/AboutAMGA/ACO/Articles/CaseStudy_final.pdf

http://www.amga.org/AboutAMGA/ACO/Articles/CaseStudy_final.pdf

Overview of ACO model and impact to physicians, patients, payment structure and quality of care

Horowitz, B. (2011, March 16). *Half of Americans Distrust Privacy of EHRs: CDW*. Retrieved September 20, 2012, from eWeek Enterprise IT Technology News, Opinion and Reviews:

<http://www.eweek.com/c/a/Health-Care-IT/Half-of-Americans-Distrust-Privacy-of-EHRs-CDW-789600>

Americans are increasingly focused on protecting their personal information. According to Javelin Strategy & Research, the number of identity theft victims fell 27 percent during the last year," Bob Rossi, vice president of CDW Healthcare, wrote in an email to eWEEK. "People take their privacy seriously and want health care organizations to do the same."

Patients also hold doctors responsible for protecting their health information.

Of the patients CDW surveyed, 86 percent believed that health care organizations held responsibility for securing financial information, 93 percent thought providers were responsible for keeping personally identifiable information secure and 94 percent believed doctors should keep data about a patient's family private.

Meanwhile, doctors don't have some of the essential IT security measures needed to protect health information, with 30 percent of physician practices lacking antivirus software and 34 percent not running network firewalls, CDW reveals in its March 8 report.

O'Donnel, H. e. (2011). **Healthcare consumers' attitudes towards physician and personal use of health information exchange.** *Journal of Gen Internal Medicine*, 1019-26.

BACKGROUND: Health information exchange (HIE), the electronic transmission of patient medical information across healthcare institutions, is on the forefront of the national agenda for healthcare reform. As healthcare consumers are critical participants in HIE, understanding their attitudes toward HIE is essential.

OBJECTIVE: To determine healthcare consumers' attitudes toward physician and personal use of HIE, and factors associated with their attitudes.

DESIGN: Cross-sectional telephone survey.

PARTICIPANTS: English-speaking residents of the Hudson Valley of New York.

MAIN MEASURE: Consumer reported attitudes towards HIE.

KEY RESULTS: Of 199 eligible residents contacted, 170 (85%) completed the survey: 67% supported physician HIE use and 58% reported interest in using HIE themselves. Multivariate analysis suggested supporters of physician HIE were more likely to be caregivers for chronically ill individuals (OR 4.6, 95% CI 1.06, 19.6), earn more than \$100,000 yearly (OR 3.5, 95% CI 1.2, 10.0), and believe physician HIE would improve the privacy and security of their medical records (OR 2.9, 95% CI 1.05, 7.9). Respondents interested in using personal HIE were less likely to be female (OR 0.4, 95% CI 0.1, 0.98), and more likely to be frequent Internet-users (OR 3.3, 95% CI 1.03, 10.6), feel communication among their physicians was inadequate (OR 6.7, 95% CI 1.7, 25.3), and believe personal HIE use would improve communication with their physicians (OR 4.7, 95% CI 1.7, 12.8).

CONCLUSIONS: Consumer outreach to gain further support for ongoing personal and physician HIE efforts is needed and should address consumer security concerns and potential disparities in HIE acceptance and use

Office of the National Coordinator for Health Information Technology. (2008). ***Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.*** U.S. Department of Health and Human Services.

http://www.google.com/#hl=en&tbo=d&sclient=psy-ab&q=nationwide+privacy+and+security+framework+for+electronic+exchange&oq=nationwide+privacy+and+security&gs_l=hp.1.1.0l2j0i30.1285.7964.0.11785.35.16.2.16.18.3.256.2764.1j11j4.16.0.les%3B..0.0...1c.1.y51GX8LQSI&pbx=1&bav=on.2,or.r_gc.r_pw.r_qf.&bvm=bv.1357316858,d.b2l&fp=46a4dcd31275ad7e&biw=1280&bih=605

INDIVIDUAL CHOICE

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

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

OPENNESS AND TRANSPARENCY

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

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

SAFEGUARDS

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

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

PR Newswire. (2012, November 29). **MiHIN to Integrate HIPAAT Consent Management and Auditing Tools.** Lansing, Michigan, United States. <http://www.prnewswire.com/news-releases/mihin-to-integrate-hipaat-consent-management-and-auditing-tools-181395471.html>

The Michigan Health Information Network Shared Services (MiHIN) is pleased to announce completion of an agreement with HIPAAT International Inc., a leading provider of consent management and auditing software for healthcare, to provide HIPAAT's software services statewide. This agreement promises Michigan patients the opportunity to control the sharing of their electronic Protected Health

Information (PHI) based on personal preferences and will allow patients to view a record of every instance of access to their PHI.

Under the agreement, HIPAAT will provide its software services through MiHIN's service-oriented architecture (SOA) to create consistent privacy capabilities, manage consent and opt-out preferences, easily integrate with sub-state HIEs and EMR/EHRs, and implement real-time access control policies. MiHIN will also deploy HIPAAT auditing services enabling the creation of audit records of access to PHI, producing mandated audit reports and allowing patients the ability to request disclosure reports for their own electronic health records.

Patel, V. A. , et. al., (2011). **Consumers attitudes toward personal health records in a beacon community.** *American Journal of Managed Care*, e104-20.

<http://www.ncbi.nlm.nih.gov/pubmed/21774099>

OBJECTIVE: To characterize consumers' attitudes about personal health records (PHRs), electronic tools that enable consumers to securely access, manage, and share their health information, in a community participating in health information technology initiatives.

STUDY DESIGN: Cross-sectional study.

METHODS: A random-digit-dial telephone survey about PHRs was conducted among adult residents of New York State's greater Buffalo region. Multivariate regression analyses identified factors associated with potential PHR use.

RESULTS: We obtained a 79% (n = 200) response rate. Many respondents (70%) would potentially use PHRs. Consumers wanted PHRs to incorporate an array of information, including immunization records (89%) and providers visited (88%). They expressed interest in several online activities, including accessing their family members' healthcare information (71%). Potential PHR use was associated with perceptions that PHRs would improve privacy and security of medical information (odds ratio [OR] 4.7; 95% confidence interval [CI] 1.1, 20.1), understanding regarding health (OR 3.7; 95% CI 1.3, 11.1), and overall quality of care (OR 3.6; 95% CI 1.2, 10.6). Potential PHR use was associated with annual household income of more than \$30,000 (OR 3.9; 95% CI 1.3, 11.9) and experience looking up health information online (OR 3.0; 95% CI 1.1, 8.1).

Other findings revealed:

- 89% of all consumers would like PHRs to include immunization records
- 88% of all consumers would like PHRs to include a list of providers visited
- **95% of potential PHR users believe that a PHR will improve privacy and security of healthcare information, understanding regarding health and overall quality of care**

CONCLUSIONS: Consumers expressed great interest in using PHRs and wanted comprehensive PHRs. However, the "digital divide" between those with varying levels of Internet experience and concerns about PHRs' effect on privacy and security of medical information may limit use. Designing PHRs that incorporate consumer preferences and developing policies that address these barriers may increase consumers' PHR use.

Patient Privacy vs. the urge to snoop. (2012, June 8). *Health Beat; A Blog about all things Health*. Minneapolis, MN, United States: Wordpress.

Blog entry takes a look at the issue of patient privacy and the impact on the community when unauthorized access by multiple health care employees at a local hospital occurs. The blog considers both the impact to consumers of healthcare, and the damage caused to reputable health care organizations when they are in the news for this kind of incident.

Simmons, J. (2011, June 2). *FierceEMR.com*. Retrieved September 20, 2012, from FierceEMR: <http://www.fierceemr.com/story/hhs-patients-should-know-who-views-their-ehr/2011-06-02#ixzz25W16D6C6>

<http://www.fierceemr.com/story/hhs-patients-should-know-who-views-their-ehr/2011-06-02#ixzz25W16D6C6>

Upon request, patients would get a chance to see a detailed report of who has accessed and viewed their electronic health records (EHRs) under a [proposed privacy rule](#) released by the Department of Health and Human Services on May 31.

Under current Health Insurance Portability and Accountability Act (HIPAA) rules, physicians, hospitals, health plans, and other healthcare organizations are required to track access to electronically protected health information. However, they currently are not required to share this information with patients.

If the proposed rule is approved, providers will be required to inform patients that they can request the detailed privacy report beginning Jan. 1, 2013, assuming the rule takes effect. The rule comes two weeks after audit reports by HHS's Office of the Inspector General criticized current federal efforts to enforce HIPAA security provisions.

The proposed privacy rule is divided into two separate rights for patients: The right to an access report includes information on who has accessed the electronic protected health information and for what purpose (such as treatment, payment, and healthcare operations). The right to an "accounting of disclosures" would provide additional information about whether the data was obtained through hard copy or electronically, and whether it was used for purposes, such as law enforcement, judicial proceedings and public health investigations.

GLOSSARY OF SELECTED TERMS

Access to electronic health records

Access to electronic health records is the act of obtaining, retrieving, or viewing electronic health records.

Audit log

Audit log is a report that indicates who has accessed a patient's electronic health record that may include some or all of the following data elements:

- Date of access;
- Time of access;
- Name of natural person, if available, otherwise name of entity accessing the electronic designated record set;
- Description of what information was accessed, if available; and
- Description of action by the user if available, e.g., "create," "modify," "access," or "delete."

Audit procedure

Audit procedure is a formal mechanism to evaluate, record, and report findings in order to assess compliance with requirements.

Consent

Consent means a digital or hardcopy record, signed and dated by a patient or a patient's legally authorized representative, authorizing the release of a patient's electronic health records (MN Health Records Act 62J.495).

E-Health

E-Health is the adoption and effective use of Electronic Health Record (EHR) systems and other health information technology (HIT) to improve health care quality, increase patient safety, reduce health care costs, and enable individuals and communities to make the best possible health decisions. Across the nation, e-health is emerging as a powerful strategy to transform the health care system and improve the health of communities.

Electronic Health Record (EHR) Systems

An Electronic Health Record is a computerized record of a person's health history over time, typically within and for a single health organization. EHR systems increasingly include tools that assist in the care of the patient or result in greater efficiency, such as e-prescribing, appointments, billing, clinical decision support systems, and reports. Because of such tools, EHR systems are much more than just computerized versions of the paper medical chart. Proper planning and implementation of an EHR system can typically take six-24 months in clinics, and three years or more in a hospital.

External access to electronic health records

External access to electronic health records means access to electronic health records by a person or entity other than the health care entity that controls the electronic health record or a related health care entity.

Health Information Exchange (HIE)

Health Information Exchange is the electronic, secure exchange of health information between organizations/information systems. The term can also be used to represent a regional or statewide organization whose purpose is to facilitate and support information exchange between member organizations.

Health Information Technology (HIT)

Health Information Technology means tools designed to automate and support the capture, recording, use, analysis and exchange of health information in order to improve quality at the point of care. HIT is a broad term that includes EHR systems (see above), e-prescribing, Personal Health Records, digital radiologic images, tele-health technologies, and many others.

Intentional access to electronic health records

Intentional access to electronic health records means access to electronic health records that resulted from actions taken with the purpose of obtaining, retrieving, or viewing that specific electronic health record.

Internal access to electronic health records

Internal access to electronic health records is access to electronic health records either by a health care entity that controls the electronic health records or by a related health care entity.

Interoperability

Interoperability is the ability of information systems to exchange data electronically, such that each system “understands” what the data are, the meaning of that data, and what to do with it. In everyday terms, interoperability is what is meant by the phrase, “computers can talk to each other.”

Monitoring

Monitoring is the on-going, process to routinely observe the application of policies and procedures.

Meaningful Use

Meaningful use defines the use of electronic health records and related technology within a health care organization, as defined by the Centers for Medicare and Medicaid Services (CMS). Achieving meaningful use helps determine whether an organization will receive payments from the federal government under either the Medicare Electronic Health Record Incentive Program or the Medicaid Electronic Health Record Incentive Program.

Minnesota e-Health Initiative

The Minnesota e-Health Initiative is a public-private collaborative that represents the Minnesota health and health care community’s commitment to prioritize resources and to achieve Minnesota’s mandates. The initiative is legislatively authorized and has set the gold standard nationally for a model public-private partnership.

Provider

Provider as per the MN Health Records Act 62J.495 is:

(1) any person who furnishes health care services and is regulated to furnish the services under chapter 147 (Board of Medical Practice), 147A (Physician Assistants), 147B (Acupuncture Practitioners), 147C

(Respiratory Care Practitioners), 147D (Traditional Midwives), 148 (Nursing and Other Public Health Occupations), 148B Social Work, Marriage and Family Therapy, Mental Health), 148C (Alcohol and Drug Counselors), 148D (Board of Social Work), 150A (Dentistry), 151 (Pharmacy), 153 (Podiatry), or 153A (Hearing Instrument Dispensing);

(2) a home care provider licensed under section [144A.46](#);

(3) a health care facility licensed under chapter 144A;

(4) a physician assistant registered under chapter 147A; and

(5) an unlicensed mental health practitioner regulated under sections [148B.60](#) to [148B.71](#).

Related health care entity

Related health care entity is an entity that controls, is controlled by, or is under common control with another entity (MN Health Records Act 144.291 sub 2. J).

Representation of consent

Representation of Consent (ROC) means a representation whether verbal or electronically captured in the electronic health record from a provider that holds a signed and dated consent from the patient authorizing the release of protected health information. (MN Health Records Act 144.293 sub 9 b).

Secure email

Secure email is an approach to protect sensitive data using industry standards. It includes security features that go beyond typical email to (1) protect the confidentiality and integrity of sensitive data transmitted between systems or organizations and (2) provides proof of the origin of the data. Secure messages are encrypted bi-directionally and are stored on network or internet servers that are protected by login. Secure messaging functionality may be integrated with the EHR or maintained in a system separate and distinct from the EHR.

Standards

A standard is a process (established by experts in a given field of study or industry) that is used to decrease and reduce variability so that a uniform result can be achieved. Privacy and Security standards are consistent, uniform processes used to safeguard protected health information. For instance; HIPAA regulations established guidelines requiring that physical, technical and administrative safeguards be in place to ensure appropriate protection of electronic health information; HITECH expanded the scope of HIPAA regulations. Together these laws formed standards that must be met for health information to be shared in a secure manner across the health care continuum.

Unauthorized access to electronic health records

Includes the obtaining, retrieving, or viewing electronic health records in violation of Minnesota or federal laws or regulations, or a hospital or provider office's policies or procedures; For example, a clinician or office personnel who views a health record for purposes outside of the treatment relationship, and is doing so for personal or criminal purposes.

The full Minnesota e-Health Glossary is available online at <http://www.health.state.mn.us/e-health/glossary.html>.

Appendix A:

LEGISLATIVE REQUEST FOR STUDY

<https://www.revisor.mn.gov/laws/?id=247&doctype=Chapter&year=2012&type=0>

Minnesota Laws 2012, Regular Session, Chapter 247, Article 2, and Section 10

HEALTH RECORD ACCESS STUDY

The commissioner of health, in consultation with the Minnesota e-Health Advisory Committee, shall study the following:

- (1) the extent to which providers have audit procedures in place to monitor use of representation of consent and unauthorized access to a patient's health records in violation of Minnesota Statutes, sections 144.291 to 144.297;
- (2) the feasibility of informing patients if an intentional, unauthorized access of their health records occurs; and
- (3) the feasibility of providing patients with a copy of a provider's audit log showing who has accessed their health records.

The commissioner shall report study findings and any relevant patient privacy and other recommendations to the legislature by February 15, 2013.

Appendix B:

SURVEY RESPONSES

Health Records Access Legislative Study Survey of Hospitals, Clinics and Health Systems

January 2013

Introduction and Background

The Minnesota Legislature requested the Minnesota Department of Health (MDH) and the e-Health Advisory Committee to study the current landscape of patient consent practices as they relate to the access and sharing individually identifiable electronic health information. The request was submitted during the 2012 legislative session to explore three issues:

- 1) The extent to which health care providers have audit procedures in place to monitor use of representation of consent and unauthorized access to a patient's health records in violation of Minnesota Statutes, sections 144.291 to 144.297;
- 2) The feasibility of informing patients if an intentional, unauthorized access of their health records occurs; and
- 3) The feasibility of providing patients with a copy of a provider's audit log showing who has accessed their health records.

(Minnesota Laws 2012, Regular Session, Chapter 247, Article 1, Section 10)

To explore these issues the MDH Office of Health Information Technology (OHIT) developed a project plan to analyze comprehensive information on the three legislative questions and provide commentary on current patient electronic health record consent practices in Minnesota. This study utilized mixed research methods, including a literature review and environmental scan, qualitative focus groups, a quantitative survey, and a public meeting to solicit comment from the community. This report presents the findings of the quantitative survey of healthcare facilities in Minnesota, conducted in November and December of 2012. It should be noted that this is a point-in-time assessment and that many health care providers are undergoing electronic health record (EHR) system upgrades as they prepare for Minnesota's Meaningful Use mandate (Minnesota Statutes 62J.495).

Methodology

OHIT secured an interagency contract with the Management Analysis Division (MAD), of the Minnesota Management and Budget (MMB) Department, to assist with development of the survey instrument and administer data collection using an online survey tool. OHIT provided a random sample of clinics that participate in OHIT's annual Ambulatory Clinic Survey, and a random sample of hospitals that participate

in the American Hospital Association Annual Survey for Minnesota. The sample for this survey included 275 hospitals and clinics in Minnesota, representing 25% of facilities that have implemented EHRs.

The scope of the study included Minnesota healthcare hospital and clinics that have adopted electronic health records and completed the 2010 Hospital or Clinic Health Information Technology Survey. Excluded from the study are other health care settings, dental offices, chiropractic offices, nursing homes, correctional health, local health departments, as well as those hospital and clinics that have not fully adopted an electronic health record system. It should also be noted that paper records were not the primary focus of this study.

The survey instrument included two profile questions and 15 questions relating to the legislative issues. These questions were developed from the concepts of representation of consent, monitoring for unauthorized access of personal health information, and the feasibility of generating and providing to patients a copy of the electronic health records (EHR) access log. Two versions of the survey instrument were created; one for hospitals and clinics, a second survey for health systems (Appendix B and C). The instruments are nearly identical and, for this analysis, are presented as a single survey.

Survey questions were vetted through an extensive iterative process within MDH and OHIT and included engaging outside health information privacy and security subject matter experts. A hard copy pilot test of the questions was conducted among privacy officers from healthcare organizations and the instrument was adjusted to reflect the feedback of the pilot respondents. The survey instrument was then converted to the online survey tool using Snap Surveys (<http://www.snapsurveys.com/>), with survey administration managed by MAD. Invitations to participate were emailed to the sample on November 7, 2012, with responses collected through December 14, 2012. A follow-up emails were sent to non-respondents on November 15, November 21 and December 10. Random phone call reminders were also made to non-respondents during the course of fielding. In some cases the respondents were sent, upon request, a PDF version of the instrument to complete by hand and fax back.

During the allotted fielding period responses were collected from 212 facilities, representing 183 clinics and 29 hospitals. The response rate for this study is 77%.

Table 1: Response Rate by Type of Facility

	Total Responding	Total Sampled	Response Rate
Clinic	183	241	76%
Hospital	29	34	85%
Total	212	275	77%

Data analysis was conducted using Microsoft Excel™ version 2010. In several cases multiple clinics within a health system or same ownership requested that a single response be applied to all clinics in the sample. These requests were honored and are documented in the data file and project notes. Data in this analysis were not weighted to adjust each respondent's contribution to the overall results.

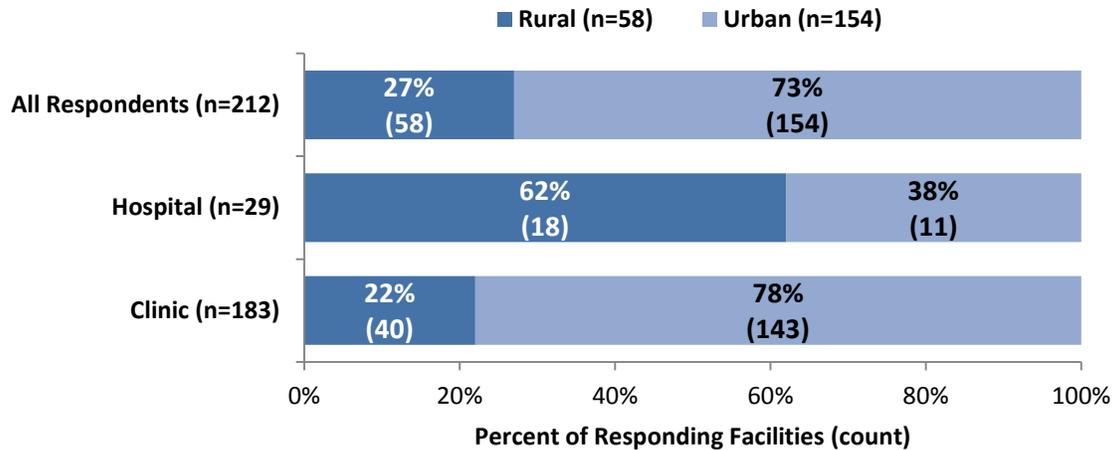
Full cross-tabulations are available upon request to the Minnesota Department of Health, Office of Health Information Technology, P.O. Box 64882, St. Paul, MN 55164, or by email to MN.eHealth@state.mn.us.

Respondent Profile

Responses were collected from 212 clinics and hospitals from across Minnesota. Almost three-fourths (73%) of respondents are based in urban areas of the state compared to 27% in rural areas. More than four in five (86%, or 183) of respondents represent clinics, and 14% (29) represent hospitals.

Figure 1 describes the geographic profile of responding facilities by type of facility.

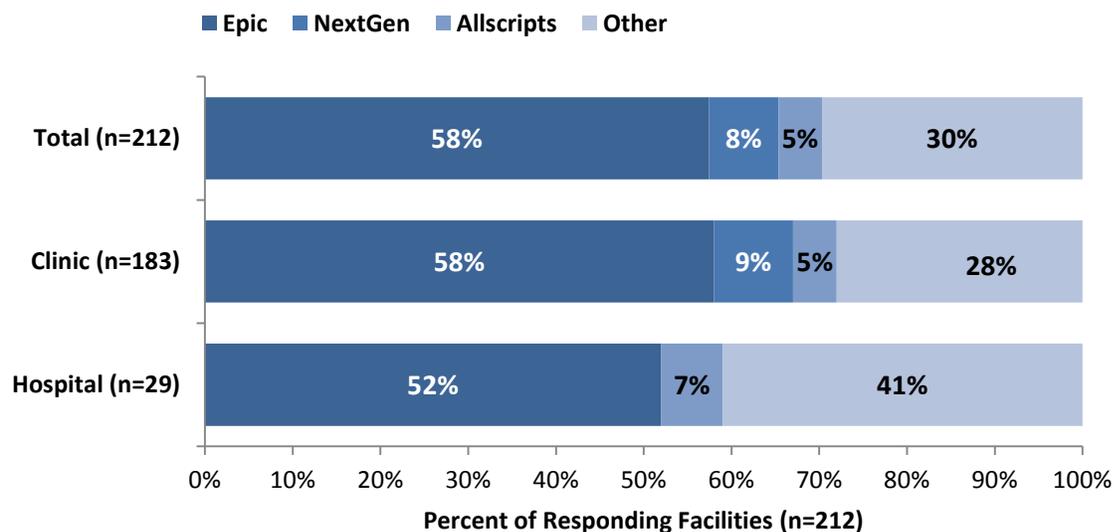
Figure 1. Study Participant Geography by Type of Facility



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

As described in the methodology, the sampled facilities were limited to those that have implemented an electronic health record (EHR) system. This survey asked respondents to indicate the EHR vendor used. As shown in Figure 2, Epic was indicated as the EHR vendor by 58% of respondents, whereas no other EHR system was used by more than 8%. Nearly nine in ten responding clinics (85%) use Epic, whereas 52% of hospitals use this EHR.

Figure 2. Electronic Health Record Vendor Used by Type of Facility



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Monitoring Patient Consent and Representation of Consent

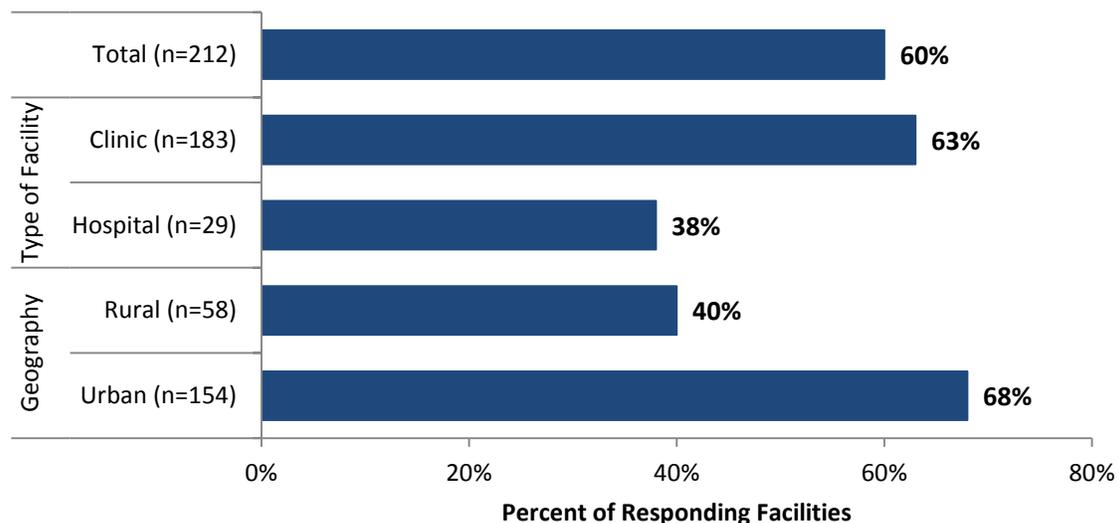
The privacy rules established in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) establish the foundation of Federal protection for personal health information as it relates to treatment, payment, and health care operations. As such, health care providers must, at a minimum, develop policies and procedures to protect patient's health information over the course of these functions. The provider may also obtain the patient's consent to use and disclose information, which is typically done in the form of a signed form at the time of the patient encounter.

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html>

Representation of consent (ROC) may also be used by providers. ROC is representation, whether verbal or electronically captured in the electronic health record, from a provider that holds a signed and dated consent from the patient authorizing the release of protected health information (Minn. Stat. §144.293 sub. 9(b)). In many cases this information would be released to another health care provider that is treating the patient (for example, a specialist).

Figure 3 shows that 60% of responding facilities have providers (e.g., physicians) who are using representation of consent. Use of this ROC is higher among clinics (63%) and in urban areas (68%).

Figure 3. Percent of Facilities that Request a Copy of Patient Electronic Health Records by Using Representation of Consent



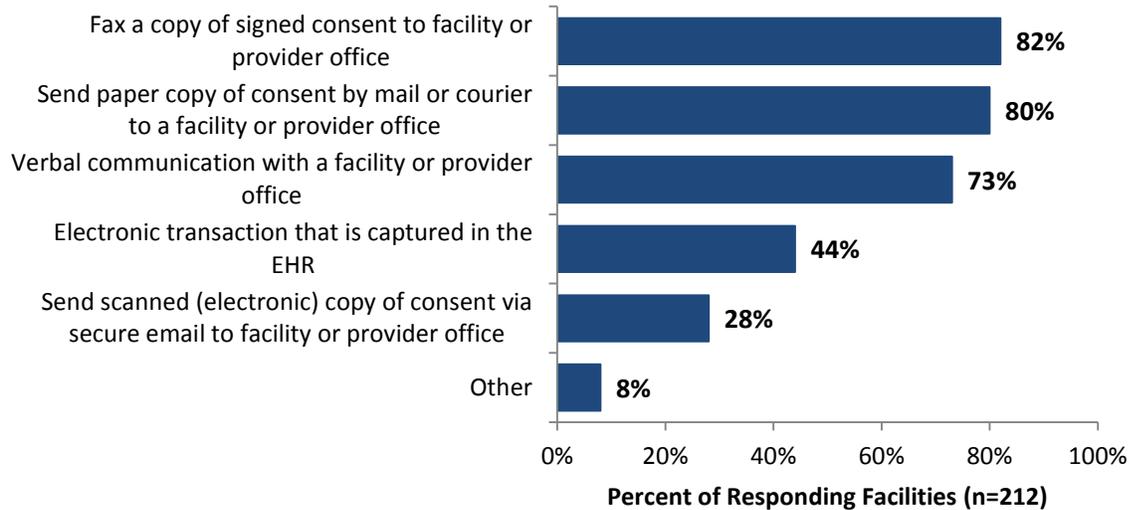
Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

There are several allowable methods for communicating patient consent, including verbal, fax, paper copy, scanned copy sent via secure email, and electronically through the EHR. It is not uncommon for providers to use more than one method, as the communication mode may depend on the preferences and/or capabilities of the receiving party.

Figure 4 shows that, among responding facilities, the most common mode of communicating patient consent is by faxing (82%) or sending by mail or courier (80%) a paper copy of the signed consent form. Verbal communication is also used by 73% of the survey population. Less than half (44%) of responding

facilities use electronic transmission of patient consent through the EHR, and just 28% use secure email to send a scanned copy of the consent.

Figure 4. Methods used at all for communicating to another provider with whom the facility has patient consent to share patient health data.

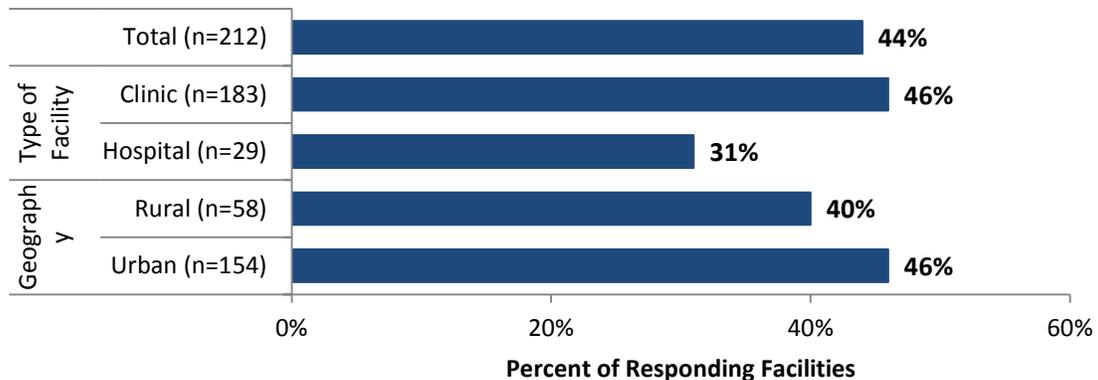


Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey. This information reflects communication with providers outside of their health system.

Figure 5 shows that significantly more clinics are able to transact patient consent *electronically within the EHR*, at 46% compared to 31% for hospitals. It should be noted that clinics and hospitals in larger health systems almost universally transact patient consent through the EHR when interacting with providers within their system.

Among responding facilities that do not capture patient consent within the patient records (n=113), almost half (49%) have plans to implement this in the future. Another 42% do not know the answer to this question.

Figure 5. Facilities Able to Capture Patient Consent Transaction in the EHR by Facility Type and Geography

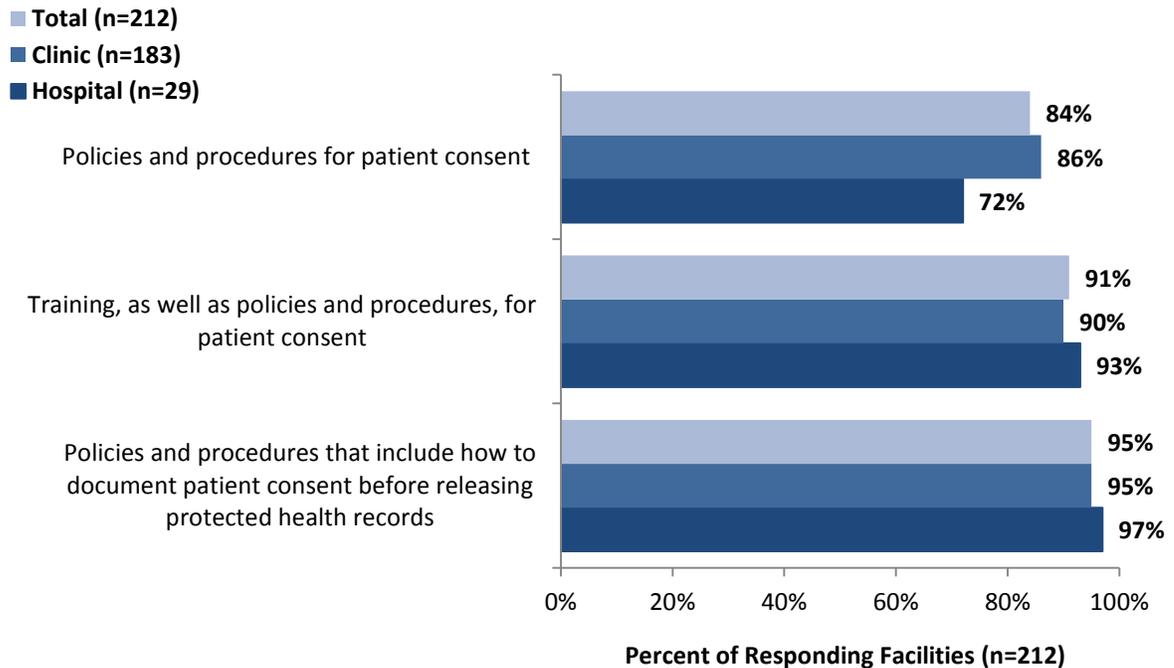


Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey. This information reflects communication with providers outside of their health system.

Implementation of Consent Policies and Procedures

Most of this survey population has established policies and procedures relating to patient consent. Figure 6 show that 91% of responding facilities have implemented training, as well as policies and procedures, for patient consent. Almost all (95%) have also implemented policies and procedures that include how to document patient consent before releasing protected health records.

Figure 6. Implemented Policies, Procedures and Training for Patient Consent

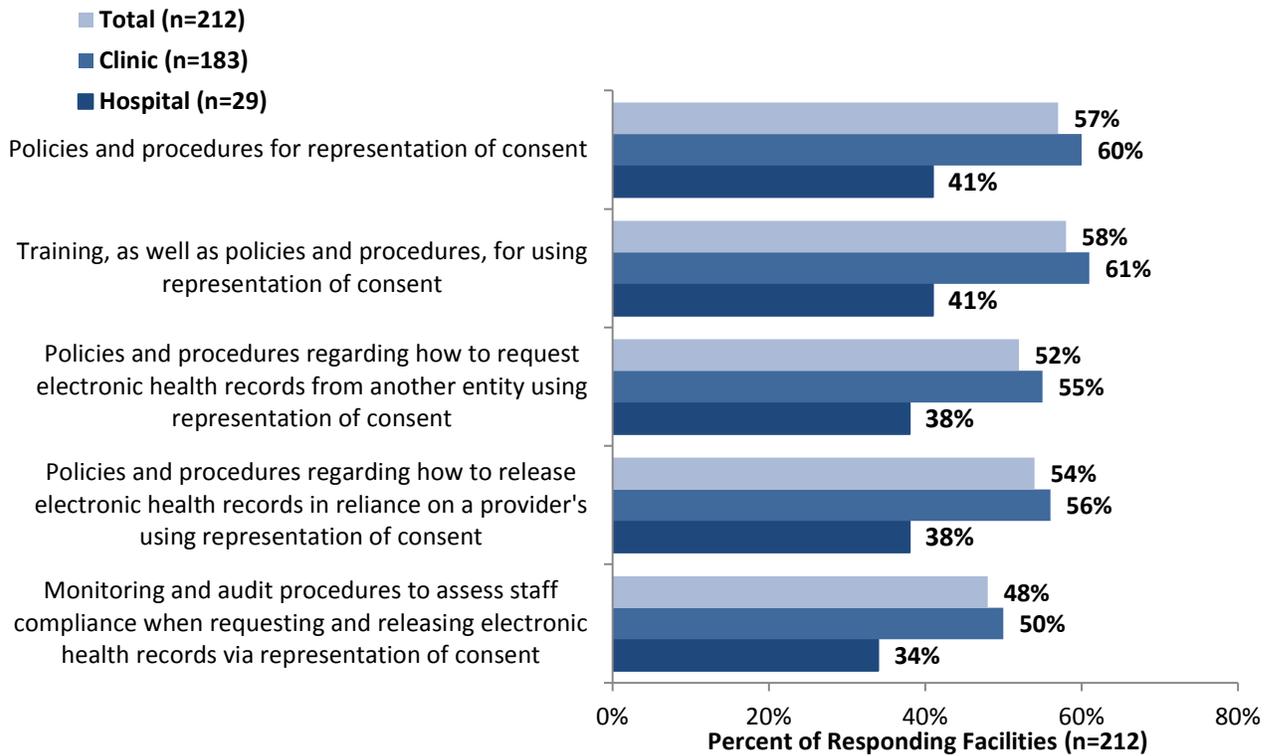


Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Figure 7 shows that fewer responding facilities have established policies and procedures relating to representation of consent, particularly among clinics and hospitals compared to clinics. More than half (58%) of all respondents have implemented training, as well as policies and procedures, for using representation of consent, yet 61% of clinics have implemented these compared to 41% of hospitals.

Almost as many have implemented policies and procedures on how to *request* electronic health records from another entity using representation of consent (52%) and how to *release* electronic health records in reliance on a provider's using representation of consent (54%). Again, a greater percent of clinics have implemented these policies and procedures compared to hospitals.

Figure 7. Implemented Policies, Procedures and Training for Representation of Consent



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Respondents from rural geographies have a lower prevalence on all three of these policy and procedure measures. Open-ended explanatory responses suggest that many of these are facilities do not use representation of consent, and in some cases are not familiar with the concept. Representative comments include:

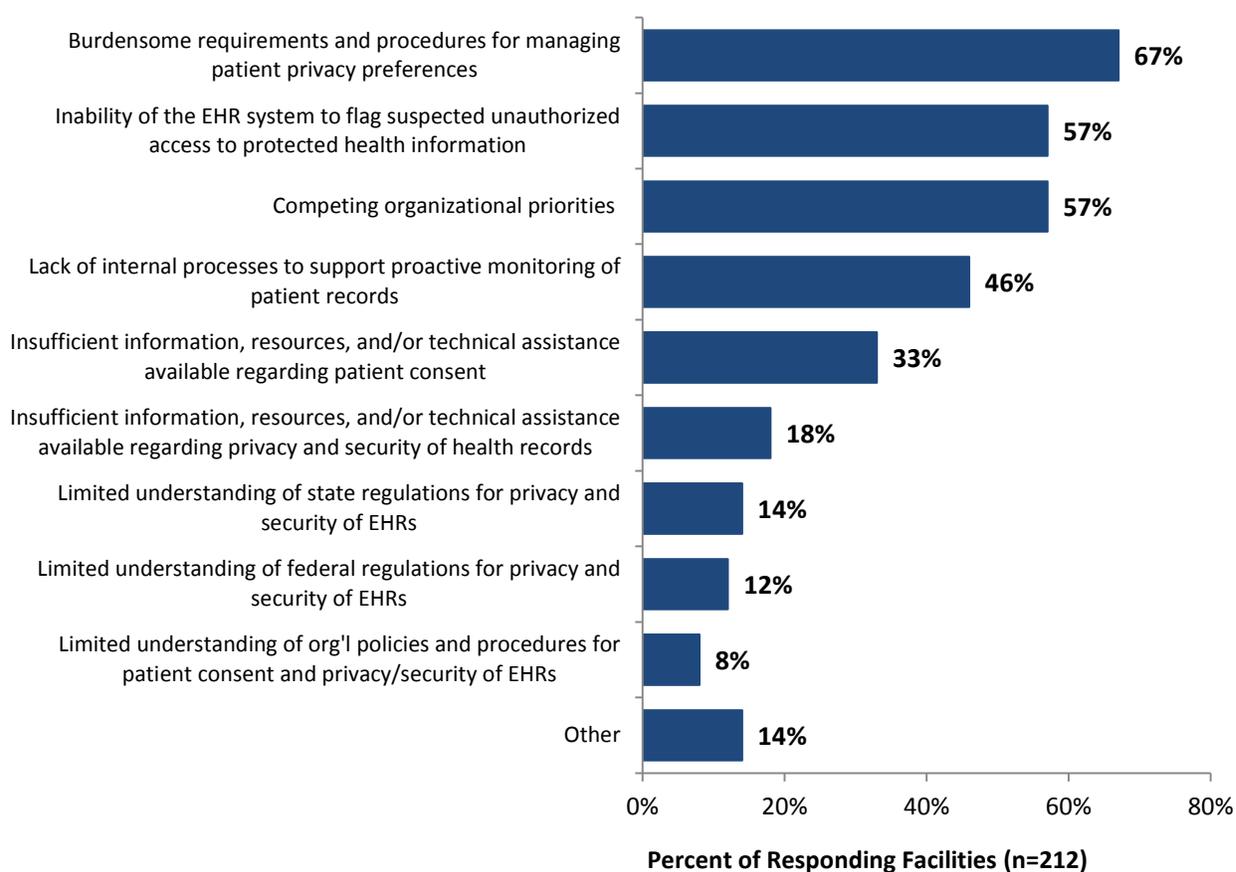
- “At this point we have no EHR connections with other provider clinics.”
- “Do not use Representation of Consent at this time.”
- “Since representation of consent is not utilized in our normal release of information process, policies and training are not implemented. The training, policies and procedures for standard release of information processes would be applicable.”
- “The representation of consent is not a term familiar to us. If a provider is holding a signed and dated consent from the patient, we would request that this consent be faxed to us. Most release of medical records is handled through the Correspondence Department of our Health Information Management Department.”

Challenges to Ensuring Privacy and Security of Electronic Health Information

Respondents were asked to indicate the significant challenges they have encountered or expect to encounter in ensuring privacy and security of electronic health information. The common challenges, presented in Figure 8, focused on both workflow issues and technical capacity of the EHR. Greatest challenges include burdensome requirements and procedures for managing patient privacy preferences (67%), competing organizational priorities (57%), inability of the electronic health record system to flag suspected unauthorized access to protected health information (57%), and lack of internal processes to support proactive monitoring of patient records (46%).

In their open-ended comments to this question many respondents noted that state and federal regulations do not align.

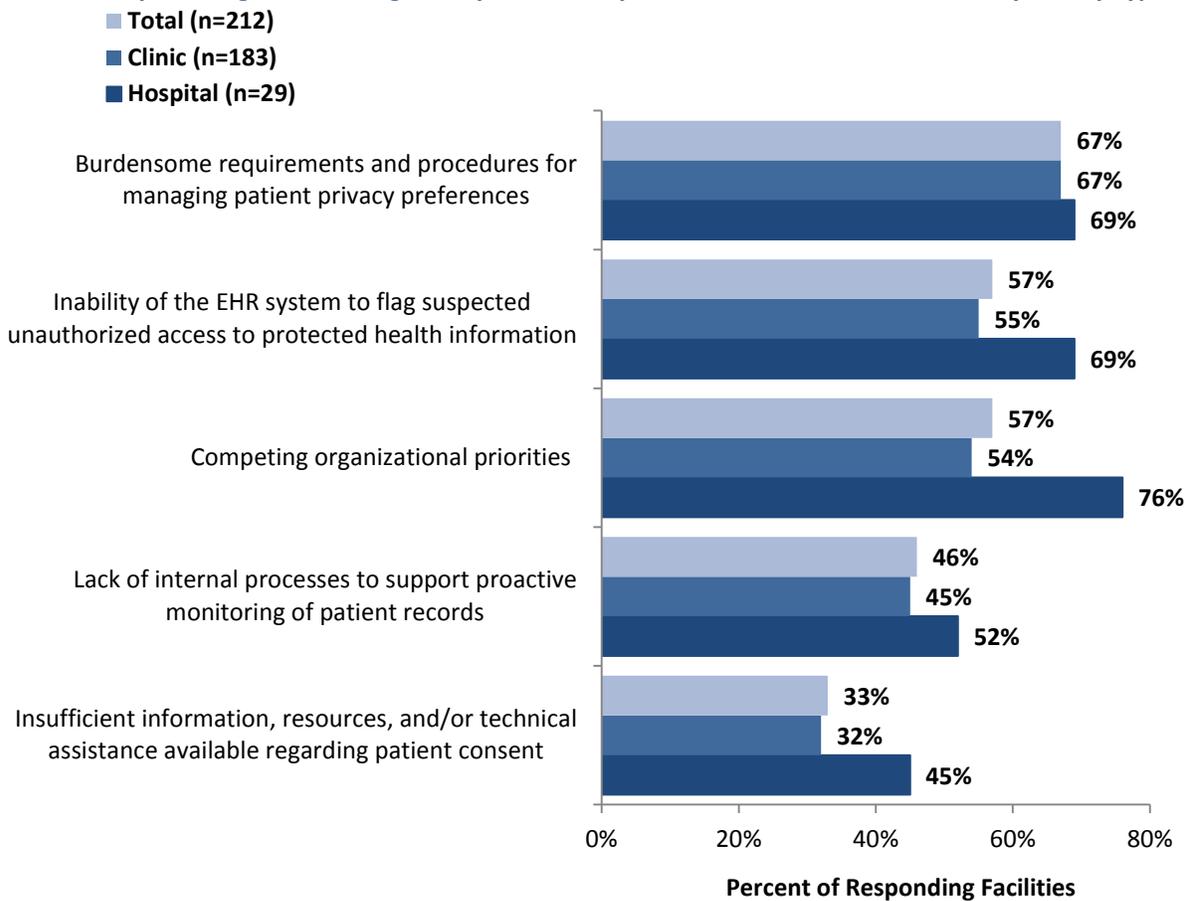
Figure 8. Challenges in Acting to Ensure Privacy and Security of Electronic Health Information



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Figure 9 shows key challenges by type of facility. More than two in three hospitals (69%) noted the inability of the EHR system to flag a suspected breach as a key challenge, compared to just 55% of clinics. Competing organizational priorities is also a greater challenge among hospitals (76%) compared to clinics (54%).

Figure 9. Key Challenges in Ensuring Privacy and Security of Electronic Health Information by Facility Type



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Monitoring for Appropriate Patient Consent

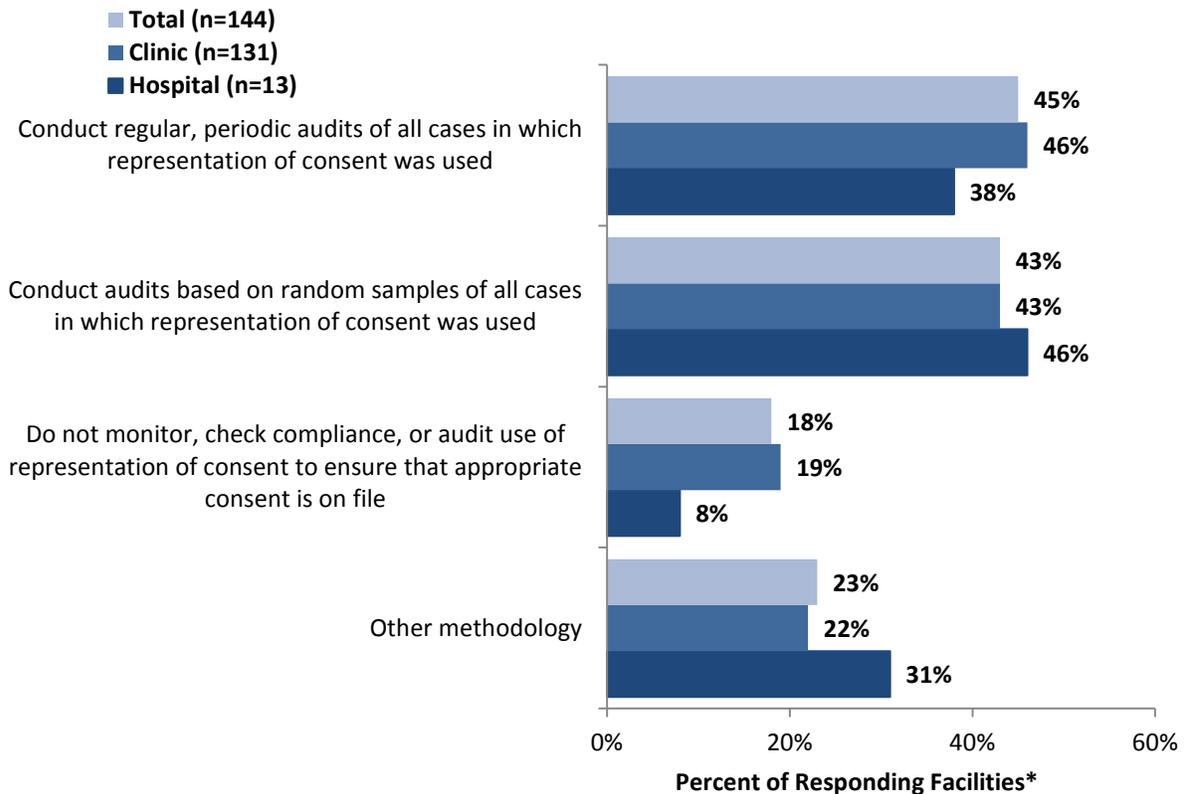
Among the 144 survey respondents that use representation of consent, Figure 10 shows that just 18% are NOT using some form of monitoring to check compliance or audit their use of representation of consent to ensure that appropriate consent is on file. Nine in ten (92%) of hospitals are monitoring, compared to 81% of clinics.

Among those who are monitoring, the common procedures are to conduct regular, periodic audits of all cases in which representation of consent was used (45%) and conduct audits based on random samples of all cases in which representation of consent was used (43%). Forty-six percent of clinics report using regular periodic audits, compared to 38% among hospitals, whereas hospitals more often rely on random audits (46%) and other methods (31%). Among respondents who indicated another methodology, they commonly noted that their procedures still include manual processes that ensure ROC is on file before any records are transferred. Representative comments include:

- “Before any records are sent out, we have the release in hand. Nothing is sent unless we have a signed document. So there is no point in conducting audits.”
- “If a patient requests the chart to be sent we verify there is a signed authorization on file.”

- “We check for consent before communicating with family, physicians, etc., 100% of the time.”

Figure 10. Methods Used for Monitoring, Compliance Checks, and Audit Procedures to Ensure that Appropriate Patient Consent is on File



*Respondents who indicated that they do not use representation of consent are not included in the base.
 Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

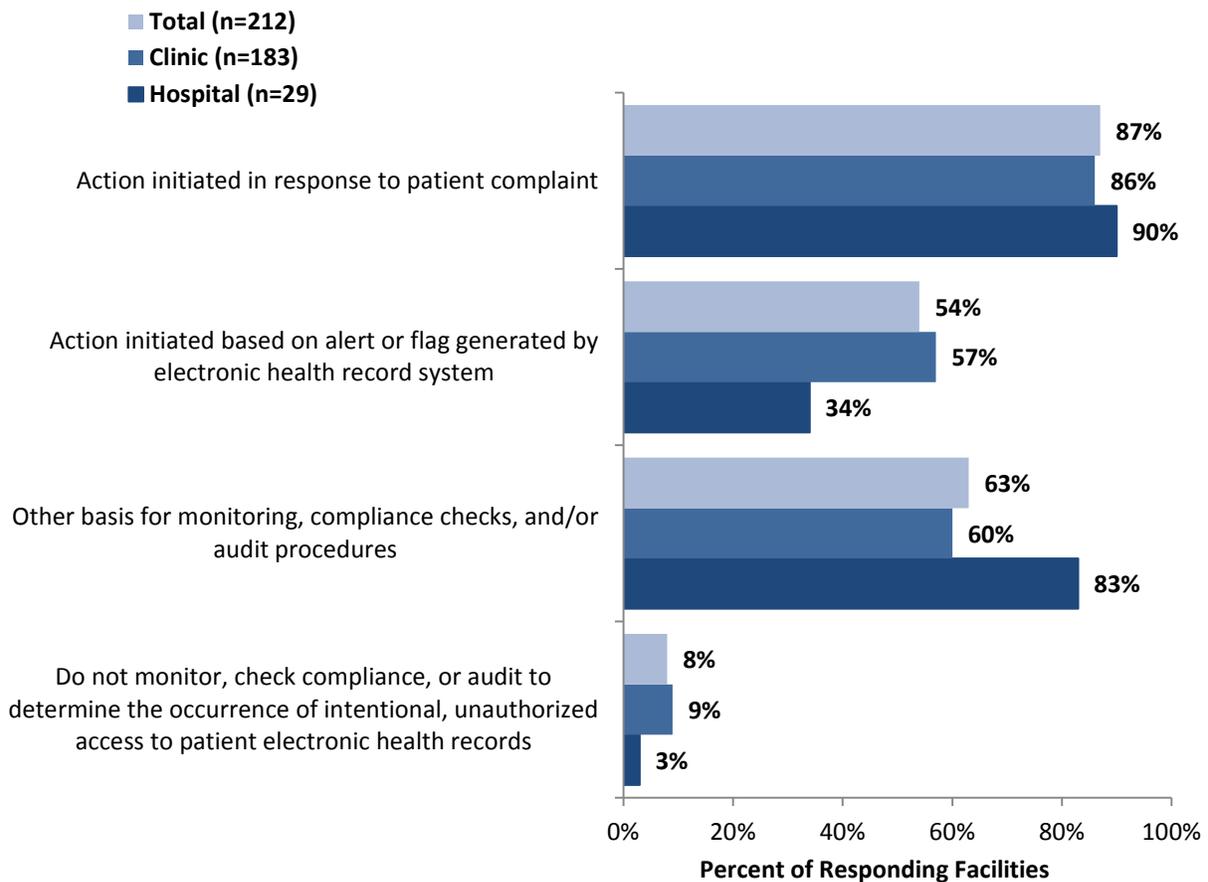
Figure 11 shows that just 8% of responding facilities do NOT monitor, check compliance, or audit to determine the occurrence of intentional, unauthorized access to patient electronic health records (commonly referred to as a “breach”), and all of the health systems report some form of monitoring. The most common procedure is an action initiated in response to patient complaint, with 87% of all respondents reporting this type of monitoring. In addition, more than half of all respondents (54%) rely on action initiated based on alert or flag generated by electronic health record system. Clinics are more likely to utilize the system alert (57%), compared to 34% of hospitals.

Almost two-thirds of respondents (63%) noted that they use other methods. Their open-ended comments include triggers such as an employee complaint and/or systematic random audits. Several respondents indicated that they prefer to rely on their random audits because automated tools within the EHR are not very efficient. In their open comments several respondents also noted that they specifically monitor their high-profile patients (such as public figures and celebrities) for unauthorized access. Representative comments include:

- “Audit can be initiated based on staff or patient request.”

- “Auditing tools within EHR system are not optimal.”
- “In addition to complaint driven monitoring, we have instituted random audit procedures where a specific number of employees are selected at random each month and all of their access is reviewed for a selected period of time. Random auditing has proven to be a very inefficient means of detecting inappropriate access. We have also implemented a specific separate audit that scans for employee access into their own or family member medical record, which takes up significant resources. Our electronic medical record does not have the capability on its own to flag suspected unauthorized access. Currently the only way to detect such access is through a manual review of access or by expending significant resources in purchasing third party auditing software, which is a fairly new and emerging technology.”
- “Monthly audit reports run target specific employee group. The goal is to audit everyone every 3-4 months to identify access of med rec or self, family or other employees.”
- “Random audits are performed on patient charts. VIP charts may be audited. We also have a mechanism for employees to submit suspected violations, which would prompt an audit.”
- “Same last name audits are conducted bi-weekly and high profile patient audits are conducted routinely.”
- “We can currently turn on the database audit but it does not monitor automatically. If an unauthorized intentional access was suspected we would inspect the record by client code.”

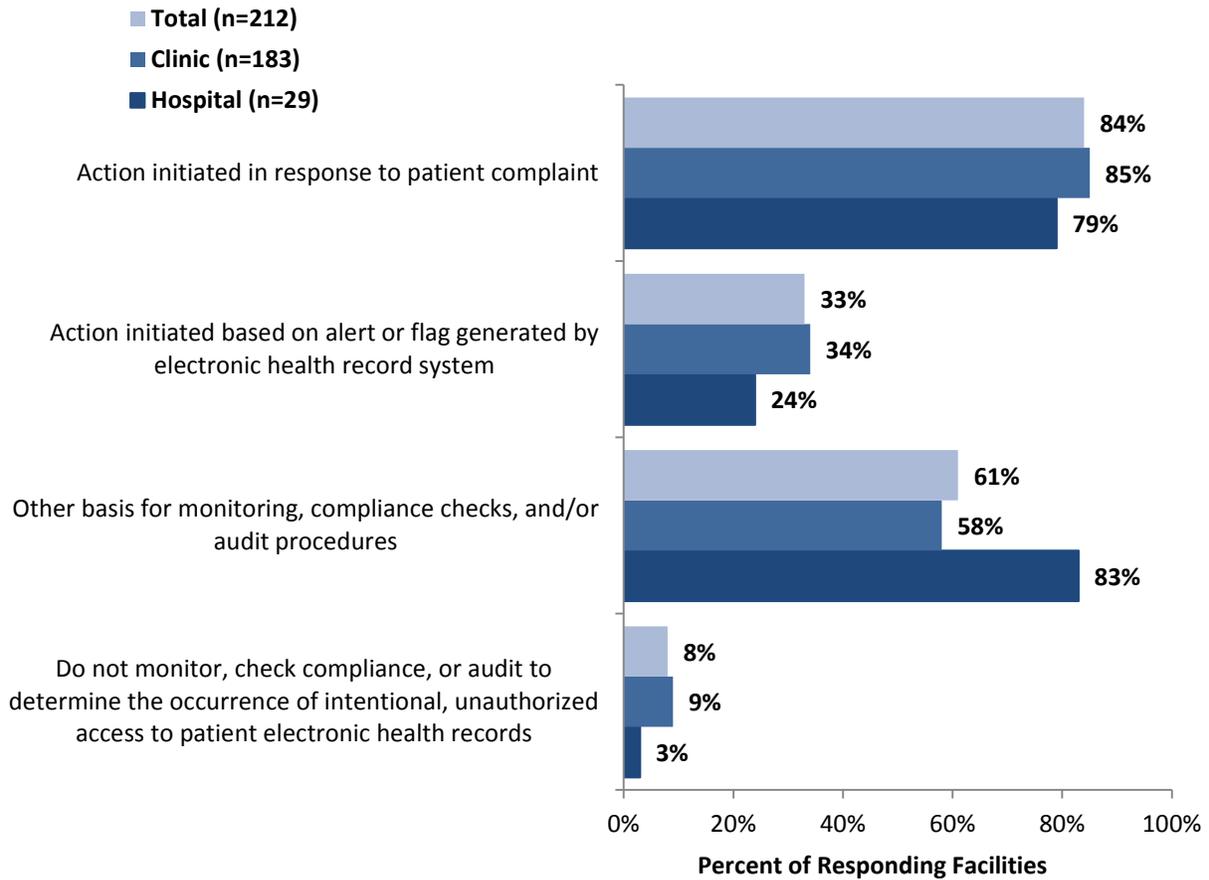
Figure 11. Methods for Monitoring, Compliance Checks, and Audit Procedures to Determine if there has been Suspected Intentional, Unauthorized Access to Patient Electronic Health Records



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Respondents were also asked about monitoring, compliance checks and auditing with respect to non-employees, such as contracted entities and workers. Their procedures are quite similar to those used for suspected breaches by employees. Figure 12 shows that almost all (92%) monitor in some way, with the most common method being in response to a patient complaint (84%). Just one in three (33%) rely on an on alert or flag generated by electronic health record system. Many respondents (61%) indicated other methods of monitoring for breaches; similar to their responses for internal breaches, they often rely on employee complaints and conduct random audits more frequently among non-employees.

Figure 12. Methods for Monitoring, Compliance Checks, and Audit Procedures For Non-Employees to Determine if there has been Suspected Intentional, Unauthorized Access to Patient Electronic Health Records



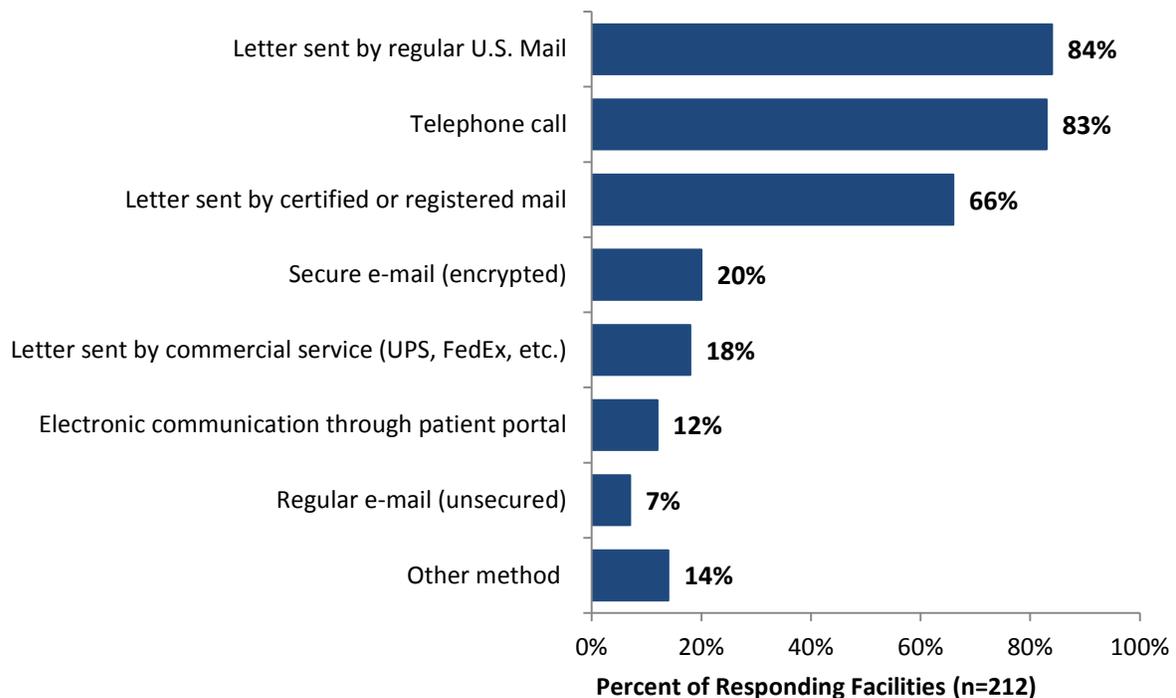
Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Notification of Intentional Unauthorized Access

In the event of intentional unauthorized access to a patient’s health records, the patient is required to be informed of the incident. The American Recovery and Reinvestment Act of 2009 requires that the patient be informed through written notice by first-class mail to the individual or next of kin at their last known address, or if specified as a preference by the individual, by electronic mail. Providers are also allowed to supplant that type of notice with other communication, such as a phone call.

Figure 13 shows that the most common methods for informing a patient of an intentional unauthorized access to their health record are through a letter sent through the mail (84%), and/or a telephone call (83%), and or a letter sent by certified or registered mail (66%). Just 20% of responding facilities use secure email and 12% use electronic communication through a patient portal.

Figure 13. Method of Communication Used to Inform a Patient of any Intentional, Unauthorized Access to their Health Record



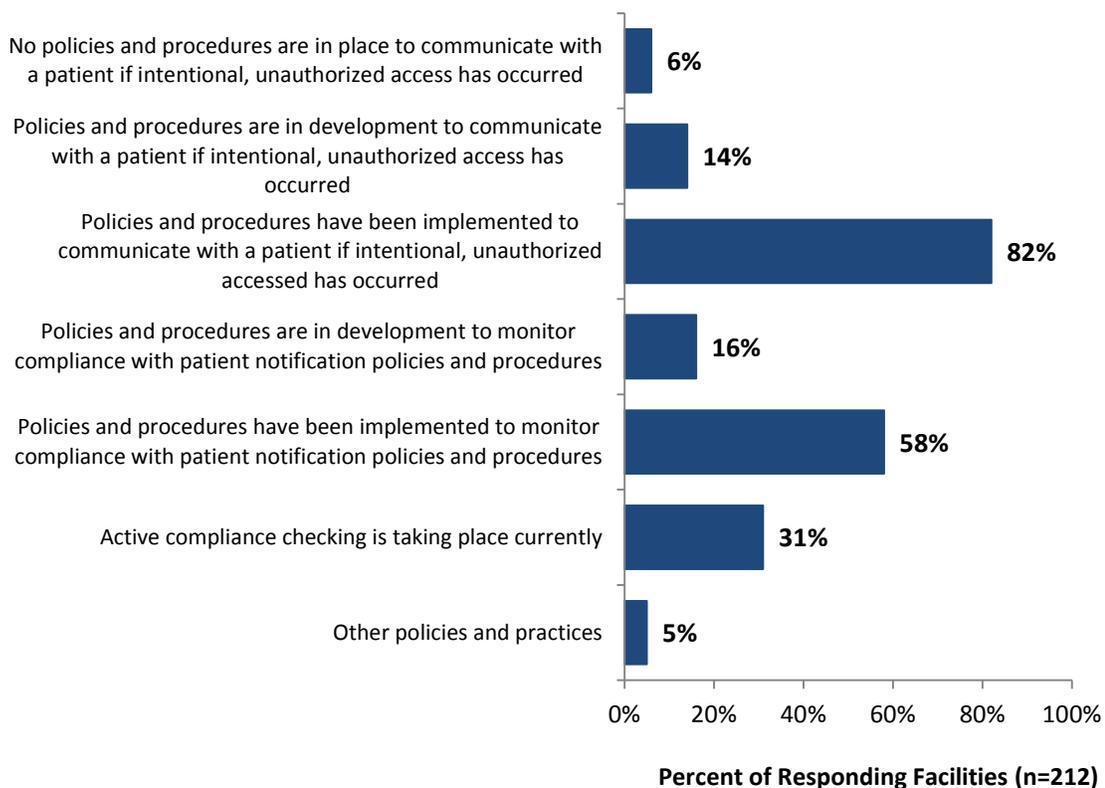
Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

As shown in Figure 14, almost all responding facilities (96%) indicated that have some level of policies and procedures in place to communicate with a patient if intentional, unauthorized access has occurred. More than four in five (82%) noted that policies and procedures have been implemented to communicate with a patient if intentional, unauthorized accessed has occurred, and another 8% are developing policies and procedures (another 6% are both developing and have implemented, for a total of 14% developing).

Responding facilities are also monitoring the compliance with these patient notification policies and procedures. As shown in Figure 14, almost one in three (31%) is actively checking compliance, while 58%

have implemented policies and procedures to monitor compliance with patient notification. Seven percent are developing policies and procedures to monitor compliance (another 9% are both developing and have implemented, for a total of 16% developing) which may be the result of ongoing EHR adoption and implementation.

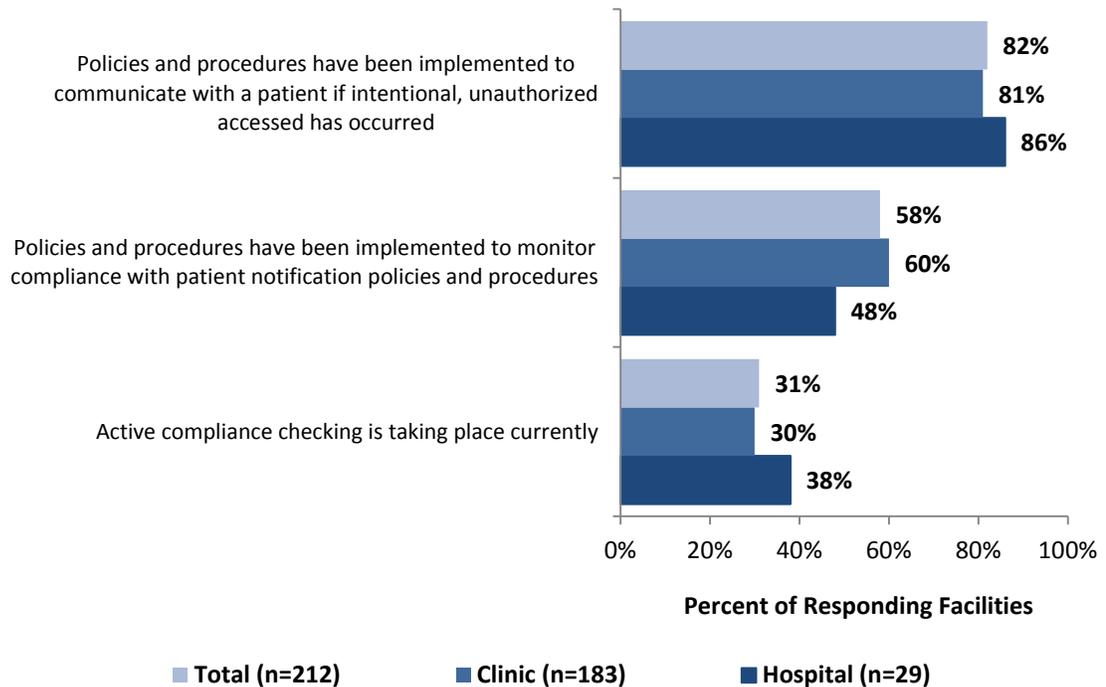
Figure 14. Policies and Practices Used to Inform Patients if Intentional, Unauthorized Access to their Health Records Occurs



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Figure 15 shows that a slightly higher percent of responding hospitals (86%) have implemented policies and procedures to *communicate* with patients in the event of a breach and monitor compliance with patient notification policies and procedures, compared to 81% of clinics. A higher percent of clinics (60%) have implemented policies and procedures to *monitor* compliance with patient notification policies and procedures, compared to 48% of hospitals. Hospitals also have higher rates of active compliance checking, at 38% compared to 30% among clinics.

Figure 15. Implemented Policies and Practices Used to Inform Patients if Intentional, Unauthorized Access to their Health Records Occurs by Facility Type



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Respondents were asked an open-ended question about challenges faced with informing patients of intentional unauthorized access. Responses included an array of comments ranging from staff resources to manage the situation, to communicating in a way that patients can understand, to problems tracking down patients, to EHR limitations in producing useful information about the breach, to concerns about the impact on the facility’s reputation and relationship with patients. These responses are not tabulated; some representative comments include:

- “A challenge we have encountered is regarding patient understanding of what a privacy breach means. There is also a challenge to notify patients about the breach that occurred but not to share more than necessary, such as HR corrective actions. There are times when patients have asked for this information.”
- “Angry or upset patients, loss of trust and/or business, potential legal action.”
- “Challenges in contacting a patient to inform them of an unauthorized, intentional access to their record would be associated with changes in their contact information. The client may have changed address or telephone number.”
- “Communicating to the patient in their language in a way that they are able to understand.”
- “Depending on size of breach...resources to implement plan. Clear direction about what needs to be done.”
- “Explaining our procedures to protect their information and how this could happen with these procedures in place.”
- “Full investigation must take place with worker and then follow up with patient. The biggest challenge would be to keep it all on a timely basis.”

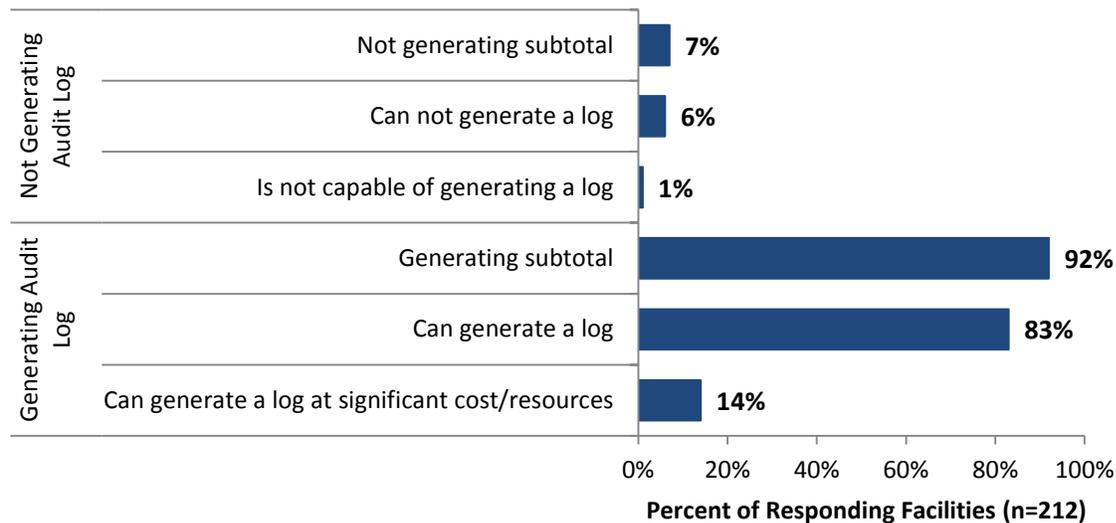
- “Getting in contact with the patient. Confirming the patient has received a letter or is aware of the breach.”
- “How much detail to include about the incident.”
- “Loss of patient trust; managing patient requests for information about outcomes for involved staff members.”
- “Patient legal Risks; Unhappy patients and risk of loss of patient to another organization; Potential word of mouth backlash.”
- “Patient wanting to know the employee name of who accessed their record – how do we protect our employees’ safety if providing that information? Over time, if every organization sent letters to patients, patients would become “immune” to the process (crying wolf analogy) – “just another letter and waste of healthcare dollars” Create anxiety or upset the patient.”
- “Patients would have a difficult time understanding work flow and business need access from an audit. Patients do not see the entire process or subsequent actions. Disciplinary actions taken with employees fall under HR guidelines and as such are confidential.”
- “Staff time to prepare letters, mailing costs, reliability of demographic data.”
- “The audit findings itself would be difficult for a lay person to interpret. Patients get upset when we cannot release the exact findings, but we do tell them we have taken appropriate action.”
- “When we are unable to notify patient due to disconnected phone numbers or change of addresses. We are not always informed of those changes.”

Feasibility of Providing Patients with an Audit Log

An audit log is an electronic “trail” or record of access to a patient’s health information in the EHR. Figure 16 shows that most respondents (92%) indicated that their EHR currently generates audit logs that document every access to patient electronic health record, including all hospitals and 91% of clinics. Fourteen percent of respondents claim that the EHR system can generate audit logs, but significant additional costs and use of resources are required. Using open-ended comments, several respondents clarified that the nuances of the audit log are not always useful, for example:

- “As far as I know, we only generate a log when a potential breach is identified.”
- “Currently can review chart and see audit trail, but does not generate log.”
- “Many of the audit logs that are produced do NOT contain adequate, useful information. They may show who accessed and when it was accessed but not the why it was accessed or what was accessed.”
- “To some extent, but full out reports on full patient lists are not at this point developed. A record of chart access is automatically done in each individual record, but summary reports are not developed to my knowledge.”

Figure 16. Ability of Facility’s EHR System to Generate an Audit Log that Documents Every Access to the Patient EHR



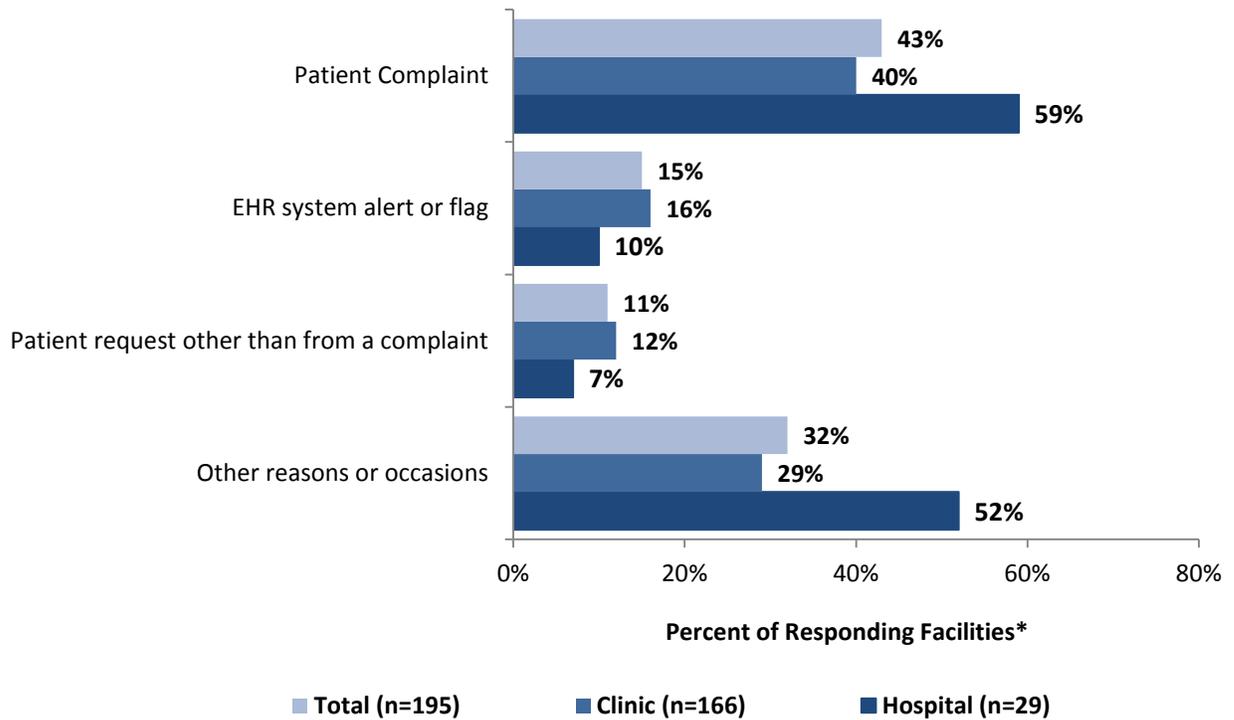
Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Respondents were asked how many times their facility’s EHR system has generated an audit log in response to a system flag or complaint. Figure 17 shows that, among facilities that can generate audit logs, the logs were most commonly generated in response to a patient complaint (43%). This incidence is 59% for hospitals, compared to 40% for clinics. Note that nearly one-third of respondents did not have this information, leaving the response blank.

Respondent open-ended comments to this question suggest that they logs are often generated based on a manual request, often as part of a random audit or suspected breach. Representative comments include:

- “Any time unauthorized access is suspected.”
- “Internal questions brought by staff members.”
- “Logs are not automated; amount of times varies based on type of audit report. Break the Glass alerts daily. Some audit reports are generated weekly, others generated with patient complaints or at the request of managers.”
- “Most audits are proactive.”
- “Twelve times a year as part of our monthly audit procedures.”
- “We generate logs when we need to. Mostly for our internal questions only.”

Figure 17. Reason for Generating an Audit Log at least Once in Past 12 Months by Type of Facility



**Respondents who indicated that they cannot generate an audit log are not included in the base.*

Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

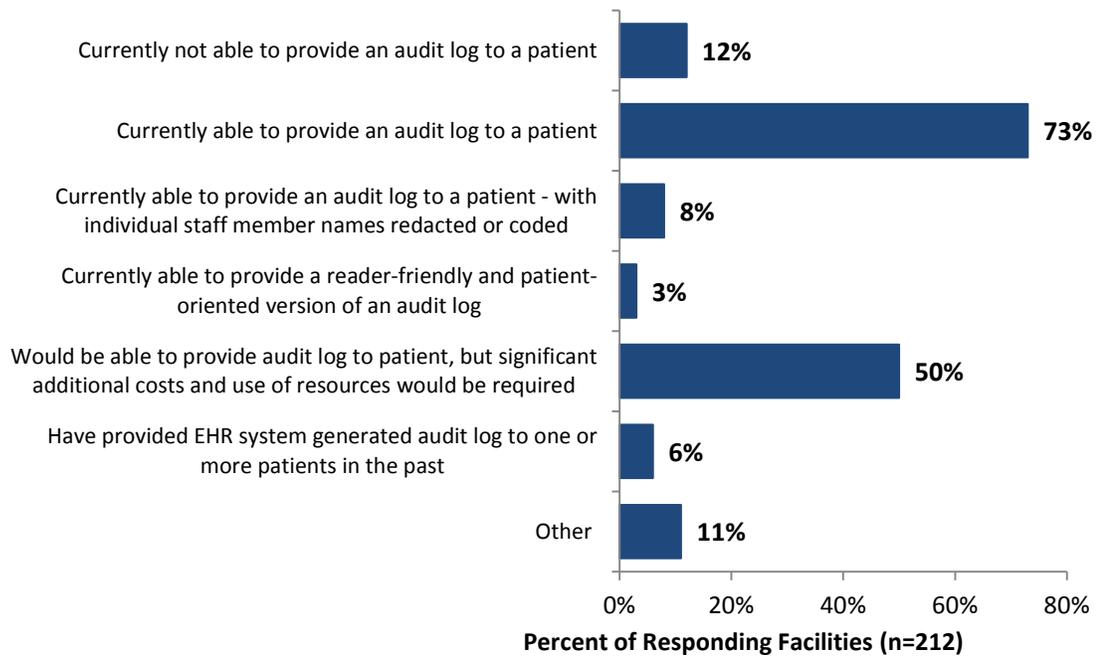
Figure 18 shows that three in four (73%) of responding facilities are able to provide an audit log to a patient; however, the nature providing the log is often cumbersome. While 73% say they can provide an audit log to a patient, 50% say they can do so, but significant additional costs and use of resources would be required. Just 8% can provide an audit log to a patient with individual staff member names redacted or coded (to ensure privacy for the employee), and only 3% can provide a reader-friendly and patient-oriented version of an audit log.

In their open-ended comments to this question, several respondents noted that the logs can be problematic due to their length and the need to redact employee information. Representative comments include:

- “Although such logs can be run, we would not provide them to patients. They contain sensitive employee and other security information, would be unhelpful to patients, would be extremely costly and time-consuming and would be an extremely inefficient way of providing patients with what they really want to know: whether someone has inappropriately accessed their EHR. We are able to provide patients with that information in a much more targeted and helpful way.”
- “An audit log could be provided, but would have to be manually redacted - it records numerous accesses within a minute’s time. Chances are it would not be understood by a patient so resources would have to be provided to be able to take time to educate and explain the report to patients. The type of media that would be necessary to provide a report would have to include paper, USBs, CDs, etc. and that would be an additional expense as well.”

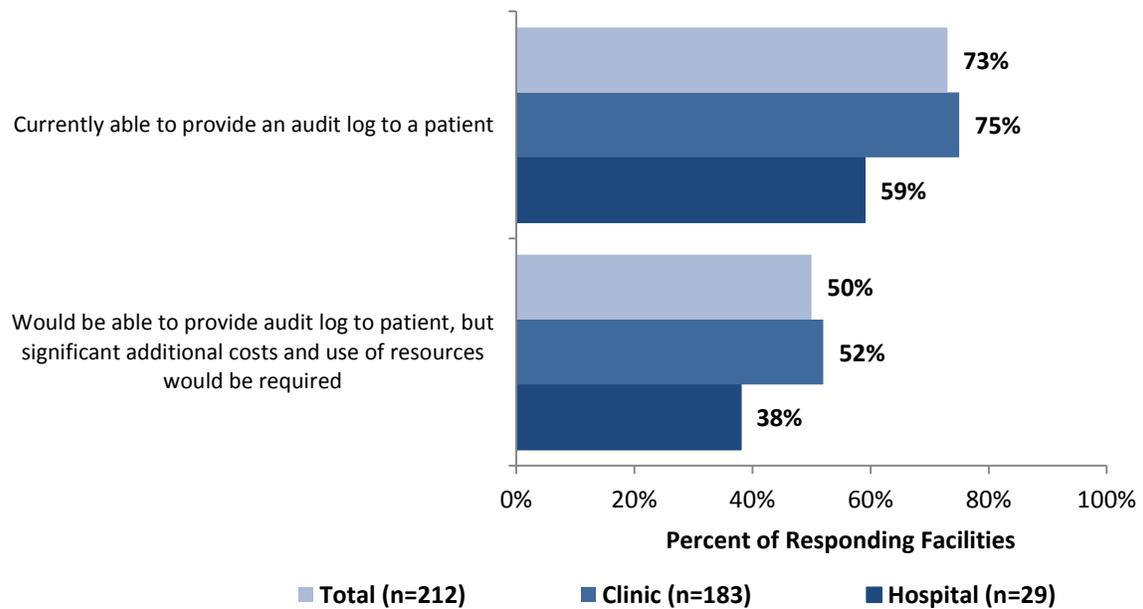
- “No way to redact staff names, the audit log is huge, extra staff time would be needed to explain to the patient what they are looking at.”
- “We could do one, but it would be very long and overwhelming for the patient to figure out.”

Figure 18. EHR Systems’ Capabilities to Provide a Patient with a Copy or Version of the Audit Log



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey. All responding health system facilities indicated that they are able to provide an audit log to a patient, but they also indicated that doing so involves significant additional costs and resources. Almost three in five hospitals (59%) can provide an audit log, but 38% indicated that this would involve significant resources. Three in four clinics (75%) can provide an audit log, but 52% indicated that this would involve significant resources.

Figure 19. EHR Systems' Capabilities to Provide a Patient with a Copy or Version of the Audit Log by Type of Facility



Source: Minnesota Department of Health, Office of Health Information Technology, 2012-2013 Health Record Access Survey.

Respondents were asked an open-ended question about challenges faced when providing patients with a copy of an audit log showing who has accessed their health records. Responses included an array of comments ranging from system limitations on viewing versus producing/printing a log, to difficulties in interpreting content, to legal concerns about employee information in the logs. Representative comments include:

- “Ability for patient to understand the audit log and distinguish appropriate access from inappropriate access.”
- “Audit logs are very technical and for the most part beyond the average patient’s ability to interpret correctly. Every EHR system is unique in terms of how it communicates access into an audit log, and the terminology used in those audit logs is often uniquely associated with the specifications of the EHR system. Codes and terminology are used to describe the various components of an electronic medical record that have no meaning to patients. Providing an audit from the EHR system to a patient would create more questions than it answers, requiring a significant expenditure of resources to provide interpretation, commentary, and answers to a patient receiving an audit trail. Various personnel other than a doctor and nurse access a medical record regularly, such as clinical informatics personnel, quality review staff, information technology staff, etc. and patients often do not understand their roles. Providing the names of those staff members to patients would unnecessarily expose those employees to questions from patients and additionally potential direct contact/conflict with patients outside of our healthcare setting.”
- “Can view audit trail in EHR, but does not print log. Would need to manually create.”
- “Concerns of retaliation or other safety concerns if identity of involved staff is not protected in some cases. Some access may be redacted as it protected under other operational needs (e.g.

Peer Review, Legal Work product). Audit logs are not readily understandable in current form and would require significant technical assistance for patient understanding.”

- “Having patient understand what the audit log stands for. Why certain people were in their chart. To be able to explain that to them face to face and not by a letter.”
- “Legal risks of doing so; Misinterpretation of the data being provided.”
- “Limitations of EHR system in regard to audit tools. Significant staff time and resources required for audits.”
- “Not currently able to provide an audit log.”
- “Patients don't understand that there are more people than just their provider and nurse who need to access the patient records in order to do their job. It is sometimes difficult to explain this to patients who think the only people who need to see their information is the provider and nurse.”
- “We cannot show any details regarding the access. We can only show who accessed on any given day.”
- “We need greater understanding and training on the functionality of our EHR and the newest upgrade version as it is significantly different from the version we are currently in. Money and time for the upgrades and learning the functionality and how to meet these constantly changing needs/provisions is a constant battle, as well as having enough staff to run all the checks and balances as well as the everyday operations with a FQHC budget.”

Appendix C:

FOCUS GROUP RESPONSES

Health Records Access Legislative Study

Focus Group Meetings of Hospitals, Clinics and Health Systems

January 2013

Introduction and Background

The Minnesota Legislature requested the Minnesota Department of Health (MDH) and the e-Health Advisory Committee to study the current landscape of patient consent practices as they relate to the access and sharing individually identifiable electronic health information. The request was submitted during the 2012 legislative session to explore three issues:

- 4) The extent to which health care providers have audit procedures in place to monitor use of representation of consent and unauthorized access to a patient's health records in violation of Minnesota Statutes, sections 144.291 to 144.297;
- 5) The feasibility of informing patients if an intentional, unauthorized access of their health records occurs; and
- 6) The feasibility of providing patients with a copy of a provider's audit log showing who has accessed their health records.

(Minnesota Laws 2012, Regular Session, Chapter 247, Article 1, Section 10)

To explore these issues the MDH Office of Health Information Technology (OHIT) developed a project plan to analyze comprehensive information on the three legislative questions and provide commentary on current patient electronic health record consent practices in Minnesota. This study utilized mixed research methods, including a literature review and environmental scan, qualitative focus groups, a quantitative survey, and a public meeting to solicit comment from the community. This report presents the findings of the qualitative focus groups of healthcare facilities in Minnesota, conducted in November of 2012, which were intended to add context and details to the quantitative data gathered through the hospital and clinic survey.

Methodology

OHIT secured an interagency contract with the Management Analysis Division (MAD), of the Minnesota Management and Budget (MMB) Department, to assist with development of the focus group questions and to facilitate information gathering during the focus group meetings.

Three, three hour focus group meetings were conducted in November 2012. The meetings were held in Bloomington, Willmar, and Duluth to provide an opportunity for regional representation.

Twin Cities: Health Systems November 8, 2012 HealthPartners	Willmar: Hospitals and Clinics November 13, 2012 Rice Memorial Hospital	Duluth: Hospitals and Clinics November 16, 2012 St. Luke's Hospital
---	---	---

Attendance was by MDH invitation and sought to provide a cross-section of health systems as well as large and small, urban and rural health care facilities. Two meetings included representatives from health systems, hospitals, and clinics; the metro area meeting included health systems and hospitals. A total of 21 of persons participated, and the number of participants ranged from six to nine for each of the three sessions. The list of attendees and the organizations they represented is included at the end of this report.

Process

For each focus group meeting, MDH-OHIT staff provided key materials one week in advance to provide context, background, and to answer initial questions. Documents included the meeting agenda, focus group questions, and a copy of the survey questions.

The sessions were co-facilitated by an outside subject matter expert in health privacy and security issues and a consultant from the Management Analysis & Development Division of Minnesota Management & Budget. Notes for the sessions were taken by a Management Analysis consultant and by MDH staff. The notes were consolidated into a summary beginning with the information from the he Management Analysis consultant lead and additional information was added from staff notes to add detail, provide clarity, and assure as complete and comprehensive documentation as possible.

The focus group notes are intended to capture key themes and ideas expressed in the meeting. No attribution of specific comments were recorded that associate specific comments to individual participants or their organizations. The notes below include findings from the sessions and a summary of key themes is presented at the end, based on the focus group findings. The structure of topics follows the legislative directive for the study.

Findings and Observations from Focus Groups

PART 1 THE EXTENT TO WHICH PROVIDERS HAVE AUDIT PROCEDURES IN PLACE TO MONITOR UNAUTHORIZED ACCESS TO PATIENT HEALTH RECORDS.

Question 1 *How does your organization know when there has been unauthorized access of a patient's electronic health records?*

- 1- ***Determination of unauthorized access may be complex and resource-intensive.*** Participants reported that they are “very protective of health information.” Organizations generally utilize proactive methods (e.g. regular audits, random audits, and other reports of employee access to patient records) and reactive methods (such as responding to complaints). There may be daily monitoring of certain individuals if warranted. In some cases, managers review EHR system generated reports of access to assess whether there were instances of potential inappropriate access. Smaller organizations, including many clinics, are usually more limited in the tools and resources available to detect unauthorized access but may utilize a “roaming management style” and would “conduct an audit if it appeared there was an issue.” Each organization needs to determine what types of audits work best for its circumstances. The larger entities generally have more resources overall, including automated tools to assist in detection and better capabilities to conduct broader and more in-depth follow-up activities. Because the available automated tools and organizational practices are in place to detect *suspicious* about unauthorized access that may need further inquiries or investigations, there is considerable effort and cost expended where the results are “false positives.”
- 2- ***EHR tools available; variability among vendor products and entities' access/implementation.*** The electronic health record systems document access to health records. One example is the EPIC EHR, which is a health information system used by several of the focus group participants' organizations, especially those that are part of larger health systems. There are many other EHR options (one of the participants represented a group of 50 affiliated entities with 18 different information systems) and there is great variability among EHR systems with respect to capturing relevant information for the detection of suspicious access. Some EHR systems also support more focused monitoring. An example is the EPIC EHR's *Break the Glass*¹³ feature. This feature is only in the EPIC EHR and is not deployed by all users.

¹³ The EPIC EHR *Break the Glass* feature requires that a person who attempts to access a patient's record at a specific security level must go through an initial procedure before the information is revealed. The person must be signed in, which creates an audit trail. Additionally, the

Additionally, not all EPIC users have the same audit procedures. A participant noted that some entities may not yet have fully implemented or utilized EHR features for monitoring access to records. Nearly all participants noted or implied that the monitoring function relies heavily on the privacy and security staff of the entities; the tools provide only part of the needed intelligence. Another issue is the major concern about inclusiveness of capture of all types of access, which is subject to ongoing development in these systems. Issues here included external access, mobile technologies, and others. The software technologies, provider networks, levels and types of access internally and externally, and sophistication of the privacy staffs' monitoring are in states of development, change, and adaptation.

- 3- **Monitoring/auditing practices – proactive and responsive; variability.** Practices vary considerably among health care entities, depending on available resources and the organizations' perceptions of needs. Among the practices are: (1) random monthly audits, the results of which may be provided to managers and supervisors for review; (2) quarterly audits for smaller entities; (3) listings of "name matches" between employees and family member patients, for example; (4) internal reports of suspicious activity or an employee's overlooking a prescribed privacy practice; (5) complaints from patients, family members, or others about suspicious circumstances such as someone knowing about something they shouldn't have known; (6) checks to ensure that employee access is consistent with the roles defined in the EHR; (7) checks on "high utilizers" – those who access records much more often than usual; (8) monitoring where a "VIP" – someone about whom there may be considerable curiosity – is a patient; (9) and responses to reports generated by the EHR. There are more examples. Practices are tailored to the circumstances of the facility or health system, within the limits of available resources.

Question 2 *What are the challenges associated with monitoring for unauthorized access of a patient health record?*

- 1- **Resource limitations, costs, and evolving needs and requirements, including consideration of different state and federal requirements.** The organizations are experiencing a "push-pull" where health information sharing is being heavily promoted at the federal and state levels while at the same time concerns about privacy and security are more prominent than before. Some of the organizations noted their compliance with HIPAA requirements and the potential that state requirements may not be consistent with their practices that comply with federal laws. Processes are generally not as sophisticated in small clinics as in hospitals. In small clinics there may be much more sharing of information because staff have multiple roles, and auditing is more likely to be based exclusively on complaints. It was also noted that in rural clinics the capabilities to audit can be very limited and there may be not enough IT staff to try to keep compliant. Overall, a major use of time is "digging through false positives" – that is, the cases in which the initial indication of potential unauthorized access did not result in finding actual unauthorized access.
- 2- **Re-establishing and reinforcing organizational culture; management actions; education.** Employees' understanding and adoption of privacy and security requirements, policies, and practices for electronic health records requires continuous training and sometimes action to enforce compliance. For example, a health system that acquired several clinics provided initial training, annual training, and one-to-one support. Employees were reeducated to understand the connection between their defined roles and access to specific information. Employees are encouraged to ask for clarification. In some instances, employees take training and must take and pass a quiz on their learning. An example was provided where the culture in one organization was slow to change – some people would not curtail their curiosity to look at records. In that case, after appropriate steps were taken including discipline, some employees were terminated. In another case, the entity publishes an internal newsletter that includes privacy and security reminders in relation to employees' jobs, including excerpts from an audit log showing access documentation. There was also concern expressed that overbroad monitoring of access to records could

person must provide an explanation of the need to access the medical record. At that time, a security reminder is presented to the employee. When the procedure is used, additional auditing reports are generated and alerts may be sent, for example to a privacy officer or analyst.

potentially have a detrimental effect on patient care. For example, when an employee may not want to conduct an unusual but useful access for fear that she will be called to explain it months later to the satisfaction of an auditor – when she may not recall it. In smaller clinics, following training, staff may be “scared to perform their jobs” and have many questions about proper access.

3- *Imprecise tools potentially generating many false positives, requiring judgment and some resource-intensive reviews.* The diversity of EHR systems in use and different monitoring practices are an ongoing challenge, within large organizations and among organizations. In rural health systems and facilities, employees “wear so many hats” and their various roles require broader access to information. With respect to EHRs, some participants noted that “standard reports [for monitoring access] may not be valuable.” Therefore, organizations may try to customize reports, download the information to another database, or make the report contents “more granular.” This increases the manual work in monitoring access. One participant noted that they need a “standardized set of tools” to use for monitoring access and detecting possible unauthorized access. Another participant noted that add-on software can add detection functionality, but it is expensive and has other potential drawbacks. Several participants noted they are always seeking “creative ways to get prompted” to identify potential problems.

4- *Additional challenges for monitoring external access; scope of audit including related internal systems.* The discussions by participants principally concerned internal access to records. However, monitoring external access to records (between the entity and other providers, facilities, or health systems) is also a major concern. EHR software provides the infrastructure for that purpose. As an example, *EPIC Care Everywhere*¹⁴ is a portal that provides an audit trail to determine what records are retrieved by another facility. A participant noted that they would not necessarily know whether the access was appropriate or not, or whether the other facility is monitoring the appropriateness of access. However, there is a high level of security that is built in to these portals, including a requirement that someone accessing information has a registered active account and several other layers of security. There is also a question about which EHR systems are included in the audit or monitoring scope. “A lot of the access is happening in a different system when a patient is there (another location), plus there are pharmacy and lab systems. Where do I stop auditing?” Every vendor’s report is different and may not give you the information needed. “It’s like peeling back an onion.” Some EHR systems do not have strong audit trails and reporting tools. As noted earlier, reports from these systems can increase the level of “false positives.” In some instances, what appear to be instances of accessing records is not technically an access.

5- *Overall limitations and trade-offs – examples.* Some participants noted their usual procedures in place and the need to be alert to new circumstances that require additional effort or focus. They also noted that resources must be used effectively for both routine and unusual monitoring. Some features of EHRs currently do not fully support effective monitoring. An example of difficulties in identifying potential unauthorized access is a system that does not document when part of a record is printed. A printed copy could be utilized inappropriately. Additionally, participants noted that EHR vendors are not necessarily focused on the issues of detecting unauthorized access as part of the evolving functionality of their information systems. It is “not an area where we have had success” or where the “vendors are putting much energy.”

Question 3 *Comparing paper-based and electronic methods for detecting unauthorized access – Which is more reliable? Which is more vulnerable to breaches or fraud?*

1- *Paper health records – considerations.* A participant noted that some organizations were “naïve and trusting in a paper environment.” The policies and processes may have been good, but in general there was “no or limited monitoring.” If someone walked out with the chart, no one would necessarily know because there is no audit trail. With a paper chart, one person sees it at a time.

¹⁴ *EPIC Care Everywhere* is described as providing a framework for interoperability between providers, facilities, and healthcare systems. Health records can be exchanged in the same vicinity or across state or national borders.

- 2- **Electronic health records – considerations.** The electronic records systems can provide multi-layered security that looks for intrusion. The systems provide documentation of “when records are accessed and it ‘kind of knows’ what has been accessed.” More than one participant noted they are very concerned about avoiding vulnerabilities such as from hacking and appearing on the federal Office for Civil Rights’ “wall of shame” website as a result of inappropriate or unauthorized disclosures (breaches). We “can’t measure unauthorized access frequency.” “We have to proceed with electronic medical records and put in as many controls as we can.”
- 3- **Comparison of reliability and vulnerability; other tradeoffs.** Participants noted that: with paper records, it is easier to control external access; with electronic records, it is easier to monitor internal access. With electronic records, “it can go spectacularly wrong, but you know where it went wrong.” In other words, unauthorized access or breach could be on a much larger scale but can be more easily and thoroughly tracked.

PART 2 THE FEASIBILITY OF PROVIDING FOR PATIENT REVIEW OF AUDIT LOGS TO DETECT UNAUTHORIZED ACCESS OF THEIR HEALTH RECORDS.

Question 1 What is (describe) your system’s ability to generate an audit log for a patient to identify possible unauthorized access to their own records?

- 1- **Variety of EHR systems – different capabilities to generate functional reports and audit logs.** Generally, EHR-generated audit logs are produced for internal purposes upon our request or on a schedule for reviews. Standard reports can be of limited use to identify potential unauthorized access. They are often very lengthy and not easy to interpret. Information contained in the reports is generally very limited (name or ID, date, brief description of records accessed; may also include department). The extent and types of variation in contents among reports produced by various EHRs was not discussed in these focus groups. In some organizations reports are handed off to managers for periodic reviews within their departments.
- 2- **Not often requested or provided to patients.** Because of the variation in what can be produced and what fields are feasible to include, this “could be a nightmare” for patients. It is unlikely that patients would be able to interpret the limited data. Additionally, audit logs are often voluminous, even for short patient experiences. Among the participants, it was rare that patients would seek audit logs – although it happened occasionally. An example of when an audit log was provided was in connection with a legal matter. One larger facility noted about ten people per year request a report of access of their records, and those reports were hundreds of lines long. Follow-up questions from the requesters are numerous and response can take considerable time and resources. Other participants stated they never have provided patients with an audit log.
- 3- **What patients might want versus what can be provided; feasibility.** Audit logs could be provided to patients but would be of very limited use in their present form and may not meet the needs of the requestor. According to one participant, patients probably want to know what kinds of people have been in my records – perhaps even the names of those people – and how the information was used and why. This would be sought for every access. Patients might become more concerned or frustrated upon reviewing the audit log because, for example, it would likely be quite lengthy and would not have the specific information and explanations they seek. EHR systems vary in capabilities, and improvements may be coming from some vendors. But it is not clear now what those improvements would be or what the benefits would be for patients. Some changes by EHR vendors to respond to patient preferences for a more understandable and useful report may be in the future.

Question 2 *What are the overall benefits and risks associated with providing an audit log?*

- 1- *So far benefits from providing available audit log reports to patients (not often done) have been limited, at best.*** In the limited instances where such reports were provided, there were, according to a few participants, considerable follow-up activities and resources required to satisfy the requester's information needs. The reports generate too much information that require clarification. An example was given of five different reports of patient episodes that were from one to five days of care, and the reports were from 90 to 545 pages. A participant noted that "we would be providing a report that is not understandable, and sometimes patients don't want this level of detail." Additionally, some of the information in reports is difficult to understand or recall even for the people most directly involved and the privacy officer or analyst. The reports may even "cause distrust between patients and providers" as long as the system is imperfect and cannot always show the reason or in what capacity an individual accessed a record. Some information may have to be redacted, or changed to codes, before being provided to a patient. For some participants, a better approach has been to meet with the patient/requester to narrow or focus the request and concerns. Follow-up resulting from such discussions may lead to quicker and more satisfying results for the patient. Another approach is to let the patient know that an internal investigation will be conducted and they will be sent the results. Another participant noted that providing general, advance educational information to patients about privacy practices and the roles of persons who access patient records could reduce the need for more specific information such as in audit logs. Other participants were not convinced that requesters would be satisfied with this more general information about the roles of people who need to access patient records. Additionally, none of the participants' EHRs would generate an audit log that identified only roles rather than more specific identifiers.
- 2- *Important concerns about employee privacy and safety.*** Some audit logs and reports list names of persons who access records. Other reports use codes. Participants noted that a patient who wants to know who accessed their records would probably not be satisfied with a coded name. For reasons of compliance with data privacy laws and internal policies, and for employee and institutional safety and security, the content of audit logs that identifies people directly or indirectly must be seriously reviewed before releasing the information. Participants noted experiences or reports of stalkers and persons whose good or bad experiences in a facility inspired them to seek to engage with employees, and other reasons for concern from providing too much information. In another scenario, a staff member may not want to participate in an activity that would leave their name on the record because it could raise questions later – for example, a nurse (nurses may work in multiple settings) involved in QI auditing when that is not her usual access of records. The record of her access might be asked to recall why her name appeared in the audit log. It was noted by more than one participant that there have been circumstances where an inquiry was initiated that turned out to involve authorized access but no one initially remembered why the record showed the name of a particular person. Organizational policies often require employees to have "minimum necessary" access to records.
- 3- *Scope and coverage of the audit log are important considerations.*** An important question is how access outside of the facility expected or required to be covered in audit logs or reports. A participant asked if access by business associates is required to be listed. One person noted that, as a covered entity, they might be required to contact hundreds of associates. The discussion in focus groups was almost entirely centered on internal access of patient records and not access by others who may be authorized access but not directly involved with patient care – for example, access for billing, coding, and access by external parties and associates. Finally, a primary EHR such as EPIC may provide audit log contents, but "all of the other ancillary systems" may not be so accessible.

Question 3 *What are some additional or desired ways to successfully detect unauthorized access?*

- 1- *Identify best practices/approaches and add focus to inquiries.*** Participants noted a variety of practices that were attuned to their facilities or systems. They included enhanced monitoring when needed;

focusing on “for cause” inquires; identifying more specific patient concern early in process, and others. One participant noted using Google inquiries and alerts to keep informed of developments that may involve the facility’s patients. Several participants noted interest in the practices and activities described by other participants concerning their facilities and systems. There may be some potential for a summary report of access, but it is not clear if patients would be satisfied, and none of the EHRs currently could produce such a report that would be useful to patients. Many of these organizations have “laid out a process” and regularly assess risks to identify potential unauthorized access. One group generally agreed that implementation of these changing requirements requires more time; meanwhile there should be a higher level of trust that they are doing what is appropriate and required as well as working to accommodate patient needs for information.

- 2- **Continuing to enhance uses of available tools.** The types of reports or logs that patients would find most useful “would require that the EMR be reconfigured.” Vendors may become more attentive to these patient concerns for usable information and devote more resources to adapting or enhancing their information systems, including to meet current and emerging requirements in federal and state laws/regulations. At least one participant noted that there may be more usable features in their current system that they will need time to become familiar with and obtain resources to implement.

PART 3 THE FEASIBILITY OF NOTIFYING PATIENTS WHEN UNAUTHORIZED ACCESS IS DETECTED.

Question 1 What are examples of current practices used in your organization for notifying a patient when an unauthorized access of their health record is detected?

- 1- **Adherence to federal notification requirements; standards; interpretations and adaptation.** Minnesota law does not have a notification requirement.¹⁵ A participant noted that if there was a state notification standard, that would make it more difficult to determine whether federal or state requirements should be followed if they were inconsistent. Federal law¹⁶ requires certain actions to protect health records and specifies requirements for notification of individuals affected. Participants stated that they interpret and apply federal law and regulations to their organization and the circumstances of individual cases. They noted that judgment needs to be applied for individual determinations. Some of the participants did not know whether notification was done in all cases, and indications of the extent of notifications varied among the participants. Some said if there is inappropriate access, then there is notification. Others noted “I don’t notify everybody every time – except of course if there is a substantial risk of harm.” Another participant noted that even if federal law would not require it, there is notification because of “company policy.” They noted that, if notification is not required, they do not notify everybody every time; there may be risk of more harm if the patient knows. “We look at the circumstances in every case individually.” One participant noted in summary that “we would want to be held to the federal requirement, with some judgment [we would apply] to go beyond [the minimum required notice] if desired.”
- 2- **Notification processes and practices in specific circumstances; variations.** The process often begins with an assessment of risk of significant harm to the individual and determination of whether notification is necessary under the laws and regulations – and also whether notification will be made even if not strictly required. “Everyone has created their own spectrum or matrix of *significant harm* – so it will be good when this [federal] rule is clarified.” One participant noted their organization may consider whether there was “inappropriate access” or a mistaken access. Another participant said they would call a patient by phone in addition to a mailing and allow the patient to ask questions about what happened. If records are faxed to the wrong place and the recipient is another provider, typically that provider would inform us

¹⁵ Minn. Stat. §72A.502, subd. 12, requires that “Whenever an insurer, insurance agent, or insurance-support organization discloses personal or privileged information about a person that requires the written authorization of that person under this section, the insurer, insurance agent, or insurance-support organization shall notify that person in writing within ten days of the date the information was disclosed. The notification must specify the identity of the person to whom information was disclosed and the nature and substance of the information that was disclosed.” The section pertains to health plans that fall within this definition.

¹⁶ See the Endnote following this section for a summary of federal notification requirements.

and we would instruct them to shred the records. In that case, it is often concluded that there is not the potential for significant risk of harm. If a patient receives another patient's information, that is more difficult. We call the unintended recipient and in most cases the record is returned. It is also important that we let the patient whose records were misdirected know what happened. One participant noted that "usually it is a family member who violates another family member's privacy" but we may hear back that "it was not right" that the errant family member was "punished" for his actions.

- 3- **Delivery methods for notification.** For most participants who noted methods, used a letter is the usual or standard method of notification, and may be preceded by or followed up with a phone call or other personal contacts. None of the participants noted that their organizations would use email to communicate notifications because it is not a secure communication. Participants generally were not inclined to use patient portals to communicate notification information because first, others besides the patient may have access, and second, it requires that the patient access the portal before she would know that there is a notification message. "With mail, we know we have made a best faith effort." One participant noted that certified mail, when used, gets the patient's attention.

Question 2 *Are there any notification practices that your organization uses that go beyond what is currently required by law or regulation?*

- 1- **General ideas and discussion.** Overall, participants did not describe specific notification practices that go beyond what is currently required by law or regulation. Many participants described the complexities of working with federal and state laws. Participants noted that colleague groups have met to discuss practices and to help resolve specific issues related to notification. Some of these discussions have been in the nature of case studies and examples of how to approach various situations. The meetings had an educational function and may have promoted dissemination of good practices.
- 2- **Reliance on the "soft skills."** Currently and for the future, there will be important reasons to use discretion and good judgment, and to manage each unique situation with the necessary "soft skills" which can be important to keep the situation from escalating. When there are legal implications, certain actions are required, but the soft skills are still necessary.
- 3- **Discussion of additional guidance; how.** A participant noted that "sub-regulatory guidance would not be helpful because we don't know what the obligation is." Another stated that in some ways, additional guidance other than federal guidance could be worse than current law. Additional federal guidance would be helpful. Another noted "we are happy with HIPAA [requirements]."

Question 3 *What other processes do you see emerging in the industry for notifying patients of unauthorized access of their health records?*

- 1- **Federal health law developments.** HIPAA and HITECH related regulations are in continual development and different stages of adoption. "Meaningful use" requirements are being discussed and the major health systems have provided information to the federal agency.
- 2- **Technology developments.** The further development of EHRs may include additional capabilities to help detect unauthorized access. Notification practices could benefit as well. On the other side, evolving technologies like cloud computing and ubiquitous mobile devices make the work of detection and tracking more challenging.

PART 4 **THE EXTENT TO WHICH PROVIDERS HAVE AUDIT PROCEDURES IN PLACE TO MONITOR REPRESENTATION OF CONSENT.**

Question 1 *How do you currently use representation of consent in your requests for or release of protected health information?*

1- Varied practices; some use ROC, some do not; contrast to comprehensive consent practice.

Organizational use of representation of consent covered a wide range of practices. One participant noted they typically do not use ROC. Their solution was to have a “comprehensive consent practice” in which they first reference what consents they have on file then, as needed, “have the other provider send us a copy of the consent form.” Another participant noted that they have been looking at using ROC but haven’t adopted it yet. Another participant stated that they do not have a standard process for ROC and therefore required signed consents. A participant noted that they do not have a standard process for accepting representation of consent by phone. Another noted that they allow staff to accept a verbal authorization.

2- Representation of consent in relation to paper records and electronic records. To obtain consent in a paper records environment, the fax is most relied upon. For electronic records, this does not pertain and representation of consent is more necessary and useful – “there is not another way to show consent.” It is built in to the electronic exchange.

3- Specific EHR: EPIC and Care Everywhere. The EPIC EHR feature called Care Everywhere allows a signed-in user to click a box that represents that the person has consent to request electronic records within the EPIC system. The participant noted that “this is representation of consent for EPIC users only.” Each EPIC user facility can get a printout of the “releasing” language and the “requesting” language consent forms. So a physical, signed paper copy is available. Electronic signatures are not allowed. When a person has the paper in hand, she can click the box in the system that confirms she has the patient consent. The form is then scanned into the system and maintained for reference. In summary, if both the requester and responder have EPIC, this form of ROC makes the exchange easier. Each facility would have its own form and language of consent – both facilities need to have their own forms signed. An exchange can be made between states, so long as it is EPIC to EPIC. It was noted that, with respect to the many EHR systems used in the state, “vendor requirements need to change to better match our needs.”

Question 2 How do you monitor or audit the use of representation of consent?

1- Practices and ability to audit vary; electronic systems easier to audit. One participant noted that “we don’t have audits in place.” Another person noted that “we do for Care Everywhere” when they check, prior to obtaining records, that the forms are in place.

2- Time and resources limited for audits of representation of consent. EPIC users sign usage forms that cover uses such as those noted above. A participant noted that providers would not want to break those “rules of the road.” Further, this organization “did not have time or resources to audit what is downloaded through this system.” Another participant noted that “we would audit our partners when we receive representation of consent, to insure we have consent on file.”

Question 3 What are the challenges associated with representation of consent?

1- Out of state providers present additional challenges. EPIC works across state borders, and Minnesota has the most stringent requirements. Even when both the requester and responders are EPIC Care Everywhere users, the out-of-state provider must print out “our form” and have the patient sign it. Then the checkbox in Care Everywhere can be checked to represent that consent has been obtained. The transaction would be more complicated for a provider not in Minnesota. It would be “more costly to build individual exchanges if they were not EPIC to EPIC transactions. Another participant noted they were not allowed to do such transactions outside of the EPIC environment. Another said that if the documentation for representation of consent is not available, “then we will request a separate release of information authorization form.”

- 2- **Liability for misrepresentation is different in interstate transactions.** Under Minnesota law, the liability for misrepresentation of consent is on the provider of the record. But the statute defines the liability only for a Minnesota provider. This participant concluded that there would be a shift of liability, because an out-of-state provider would not be held liable under this law.
- 3- **Entities need their own forms; lack of standardized forms.** Organizations want their own consent to release forms signed. “They wouldn’t be comfortable if it was a standardized language.” MDH has created a standard consent form, but organizations continue to use their own. Participants had mixed opinions about mandating use of a standardized consent form, whether this one or another, but most did not indicate a preference for a standard form.
- 4- **Use of representation of consent when in a “crisis situation.”** A participant noted that records would be provided to an emergency department in a crisis situation on the basis of a verbal request, which would be a use of representation of consent.
- 5- **Reverting to federal health privacy laws.** Some of the participants concluded that “reverting” to the use of federal privacy laws would help with many current problems. One person noted that we “will not make it into the electronic world if Minnesota stays at the status quo.” “State laws were good, but that was before we had the federal rules.” Another participant added that “HIPAA establishes standards that are manageable and facilitate patient care. Privacy laws should allow flexibility. This would also increase the interoperability across state lines and within the state.” “HIPAA is what most follow and providers don’t understand all of the implications of the state’s laws.”

Summary of Key Themes from Focus Group Findings

1. **EMR vendor software.** Vendors create software features for the national market based on federal mandates and to meet certification requirements. Minnesota specific features, such as for representation of consent, do not get enough attention in the market. This complicates health information exchange and monitoring for privacy and security, and may impact the cost of health care. Additionally, software systems within and among facilities (for example, between a principal EHR and labs/pharmacy systems, or between a facility and its business associates and related entities, make comprehensive views and analysis very difficult.
2. **Public and workforce education on privacy practices and requirements.** Patients and those in the healthcare workforce need to better information and education on privacy and security of ePHI to promote a culture of trust and awareness.
3. **Revert to federal laws for privacy.** Compliance with privacy requirements would be more efficient if based only on federal laws and regulations. HIPAA and HITECH laws provide national standards. The conclusion does not mean that Minnesota laws should be changed unnecessarily, just that the national standards are utilized in Minnesota and in other states. If consistencies in definitions between Minnesota laws and federal regulations can be improved, it will lessen confusion.
4. **Representation of consent.** Many providers do not use representation of consent, relying on a “comprehensive consent practice” instead.
5. **Audit logs available to patients.** As currently generated by EHR systems, the audit logs are burdensome to use for the detection of unauthorized access, are rarely requested and when requested are not useful to patients.
6. **Improving detection capabilities for unauthorized access to records.** Most detection is based on heavy use of human resources. EPIC EHR Break the Glass (mentioned above) is an example of a software feature that

allows an organization to put additional focus on areas of potential risk. More and improved software tools could add to the ability of organizations to monitor and detect unauthorized access of health records. The extent of vendor development in this area may be improved based on new federal regulations.

Focus Group Participants (alphabetical order by participant name)¹⁷

<u>Name</u>	<u>Organization</u>	<u>Title</u>
Beverly Annis	Sibley Hospital – Arlington	Director Quality and Risk Mgt
Sue Belford	First Light Health System	HIM Mgr/Privacy Officer
Teri Beyer	Rice Memorial Hospital	Privacy Officer
Leah Buermann	Park Nicollet	Privacy Officer/HIPAA
Pat Carter	HealthPartners	Senior Counsel Privacy-Security
Vicki Clevenger	Essentia	Chief Compliance Officer
Corla Enevoldsen	Madison Hospital/Lutheran Home	HIM - Quality
Bill Jagow	Affiliated Community Medical Centers	Chief Information Officer
Suzy Johnson	St. Luke’s Duluth	HIS Specialist
Leigh Kreemer	Northland Ear Nose and Throat Assoc	Clinic Manager
Diane Larson	St. Luke’s Duluth	HIM/Privacy Officer
Trina Lower	Mercy Hospital – Moose Lake	Director of Quality and HIS
Stephanie Luthi-Terry	Allina	HIT Compliance
Michele McLoughlin	St. Luke’s Duluth	Manager Medical Record Dept
Kari Myrold	Hennepin County Medical Center	Privacy HIM
Rachael Nyenhuis	Integrity Health Network	Chief Operations Officer
Nicole Olson	CentraCare	Privacy Officer
Tobi Tanzer	HealthPartners	Privacy JD
John Thomas	Ortonville Area Health Services	HIM Manager
Morgan Vanderburg	Mayo Clinic	Privacy Analyst
LaVonne Wieland	HealthEast	Privacy Officer

¹⁷ Most organizations provided one person to participate, although the host facilities added one or two more.

Endnote: Summary of Federal Laws Concerning Notification

Excerpted from: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>.

The Health Insurance Portability and Accountability Act (**HIPAA**) and related rules require group health plans to protect the privacy of health information. The notification interim final rule requires **covered entities** to provide the Secretary of HHS with notice of breaches of unsecured protected health information (45 CFR 164.408).

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. Covered entities must **notify affected individuals** following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach. In addition, **business associates** must notify covered entities that a breach has occurred.

The **number of individuals affected** by the breach determines when the notification must be submitted to the Secretary of HHS. If a breach affects 500 or more individuals, a covered entity must provide the Secretary with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically. For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary with notice annually. Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (**HITECH**) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

A **breach** is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the **use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual**. There are three **exceptions** to the definition of “breach.” The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Appendix D:

PUBLIC PARTICIPATION AND COMMENTS

**Minnesota Health Records Access Study
January 2013**

Background

As a result of the 2012 legislative session, the Minnesota Department of Health (MDH) was charged by the Minnesota Legislature to conduct a study, in consultation with the Minnesota e-Health Advisory Committee, regarding access to patients' records. The Minnesota Health Records Access Study will collect information from hospitals, clinics, and health systems through a survey and a series of focus groups/facilitated discussions to help understand:

- 1) The extent to which providers have audit procedures in place to monitor use of representation of consent and unauthorized access to a patient's health records in violation of Minnesota Statutes, sections 144.291 to 144.297;
- 2) The feasibility of informing patients if an intentional, unauthorized access of their health records occurs; and
- 3) The feasibility of providing patients with a copy of a provider's audit log showing who has accessed their health records.

(Minnesota Laws 2012, Regular Session, Chapter 247, Article 1, Section 10)

Public involvement in the process of conducting the study has been a priority and a consideration throughout. In addition to asking hospitals and providers to comment on the legislative questions, MDH held a special meeting to gather input from the public and held a comment period for submitting written comments.

Below is a list of meetings that were open to the public, in which the study methods were formulated and public comment solicited:

Minnesota e-Health Advisory Committee Planning	July 2012
Informal planning gathering of the Minnesota e-Health Advisory Committee. Included consumer representatives from the Advisory Committee as well as the HIE Oversight Review Panel.	
Minnesota e-Health Privacy and Security Workgroup	August 2012
Special meeting of the Workgroup was called to review and comment on proposed study methods. This meeting was broadly publicized to multiple lists, including the Minnesota e-Health Update which has over 4200 subscribers, inviting all interested parties to attend.	

Minnesota e-Health Advisory Committee Quarterly Meeting	September 2012
Regular quarterly meeting of the Advisory Committee. The Minnesota Health Records Access Study was specifically publicized as a discussion topic, with members of the public and interested parties invited to attend the meeting. Consumer representatives from the e-Health Advisory Committee and the HIE Review Panel were in attendance to provide comments and feedback on the study approach and methodology.	
Public Meeting	December 6, 2012
A special meeting was convened to gather public input on the legislative questions. This meeting was scheduled for December 6, 2012 and advertised starting on October 29, 2012. An eight day public comment period was opened following the meeting, which was extended to 15 days to allow adequate time for public comment. It was advertised through multiple public MDH email updates and newsletters, as well as on the public MDH Facebook and Twitter pages.	
Minnesota e-Health Advisory Committee Quarterly Meeting	December 6, 2012
Regular quarterly meeting of the Advisory Committee. The MN Health Records Access Study was specifically publicized as a discussion topic, with members of the public and interested parties invited to attend the meeting.	

Public Meeting and Comments

MDH convened a public meeting on December 6, 2012 to give a status update on the progress of the study, including methods for capturing information to respond to the legislative study questions, to share preliminary data from the Hospital and Clinic surveys (which were still in progress on that date) and to share some preliminary observations from the survey data and the three Hospital/Clinic/Health Systems focus group discussions that had taken place and were still being analyzed.

Over 20 people attended the December 6 MDH public meeting, including members of the public, representatives from hospitals and clinics, government agencies, and news media. KSTP 5 Eyewitness News aired a “live” piece informing the public about the Health Records Access Study during their 5:00 pm broadcast.

One hour and fifteen minutes were scheduled for persons in attendance to share their perspectives on the legislative study questions. One person offered comment at the meeting: Twila Brase, representing the Citizen’s Council for Health Freedom, suggested that the public did not understand the legislative questions being studied and requested a fact sheet from MDH describing the questions being studied.

MDH provided a fact sheet within 3 business days, which was published on the MDH website and shared via the Minnesota e-Health Update email list (which has over 4,200 followers) and promoted on the MDH Twitter (4,223 followers) and Facebook (1,272 followers) public pages. To allow adequate time for individuals to review the factsheet and respond to the legislative questions, the original nine day public comment period, scheduled to close on December 14, was extended to fifteen days, closing on December 20, 2012.

During the fifteen-day comment period following the public meeting, MDH received 91 communications from members of the public, a few of which were multiple messages from a given individual. 88 responses were emails, two were letters and one was a holiday card send via the United States Postal Service.

Summary of Comments Received

MDH received 57 form letters which included important comments on the following topics:

1. Terms and assumptions of the legislative questions: asks why there are no questions on how the public feels about such terms and assumptions.
2. The concept of Representation of Consent: providers should have a copy of consent on file before health information is shared.
3. Data belongs to the patient.

A single response on behalf of the Citizen's Council for Health Freedom was received with the following comments:

1. The public does not know about or understand "Representation of Consent".
2. Audit logs will not change perceived lack of accountability.
3. Audit logs require extensive administrative effort to determine unauthorized access.
4. "Wiggle room" in law allows health care executives to define terms of "intentional", and "authorized" access, meanwhile the public may unknowingly have data shared and used in ways it may deem as unauthorized.
5. Patients should have access to information in audit logs regarding their own information and who accessed it.
6. Health care institutions should support defined written and limited consent that gives legal assurance that data is shared in a way that is acceptable to the patient.
7. Data belongs to the patient.

8. Requirement that patient privacy recommendations from the study are reported, including privacy concerns of individual patients.

Other Themes Highlighted in Public Comments:

1. Patient privacy is important.
2. Do not want anyone looking “my” data without “me” knowing it.
3. Consent should only be for those treating “me” directly.
4. Patient should feel secure that communications with physicians is confidential.
5. Written consent should always be required.
6. Audit logs should be easy to generate and provide to a patient.
7. Need for accountability in auditing, including ability to decipher what data was accessed by whom and when.
8. Providers need to insure appropriate safeguards to protect information.
9. Health care providers should take reasonable precautions to prevent unauthorized access and inform the patient if an intentional, unauthorized access occurs.
10. Representation of Consent is a fuzzy term used to disguise questionable practices.
11. People may be discriminated against if medical records are too open.

Addressing Public Comments in the Minnesota Health Records Access Study

Many of the comments received during the public comment period were not germane to the narrow of scope of this particular study as determined by the Legislature, but expressed a general and important concern for patient privacy, security of their health information and patient ownership of their own data, which should be noted to the extent that the Legislature and health care organizations consider policies and future action that might impact patient privacy. Prominent themes relating to the legislative study questions that emerged from the responses received during the public comment period were 1) a desire for patients to be informed if unauthorized access of their health information occurs and 2) to be able to access a patient-friendly audit log listing the individual and the roles of those who accessed their records and for what purpose.

Copies of all public comments received by MDH are available upon request.

Appendix E:

OVERVIEW OF MINNESOTA HEALTH RECORDS ACT AND FEDERAL LAW

It has come to be widely recognized by diverse stakeholders in Minnesota and across the country – patients, legislators, health care providers, policy makers – that health information exchange (HIE),¹⁸ facilitated by the use of electronic health record (EHR) and other technology, can provide many benefits towards improved health and health care in the community, particularly as it relates to quality of care, patient safety, and population health.¹⁹ It is widely understood, also, that to realize these benefits while also fostering the trust critical to effective care, HIE must occur within the important framework of state and federal privacy protections.

To effectively analyze the findings and evaluate the recommendations of the Health Records Access (HRA) Study, it is necessary not only to understand the federal and Minnesota approaches to health information privacy protection but also to identify how the approaches differ and how the sometimes-divergent federal and state requirements interact to impact patient interests.

The Federal Approach to Privacy Protections

In 1996, the Health Information Insurance Portability and Accountability Act (HIPAA)²⁰ was enacted to improve the efficiency and effectiveness of the American health care system through, among other strategies, implementing national standards to facilitate electronic data exchange. The HIPAA provisions establishing national standards are in a section of the Act called “Administrative Simplification.”²¹ Because of concerns that as the electronic exchange of health information increases, so can the likelihood of inappropriate access of that health information, Congress in 2000 added privacy and security requirements in the Administrative Simplification provisions.²²

In 2009, as part of the Stimulus Bill, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) was enacted, calling for the nationwide expansion of electronic health care information exchange and establishing economic incentives to encourage health care providers to invest in health care information exchange technology.²³ Mirroring the approach in the original HIPAA legislation, the HITECH Act contains provisions that both encourage the expansion of electronic health care information exchange and also require the establishment of enhanced privacy and security requirements. As required by both the Administrative Simplification provisions and HITECH Act, the Department of Health and Human Services (HHS) issued regulations both to implement standards for

¹⁸ *Health Information Exchange (HIE)* means the electronic transmission of health-related information between organizations according to nationally recognized standards.

¹⁹ See *MINNESOTA STRATEGIC PLAN FOR HEALTH INFORMATION EXCHANGE: A Prescription for Meeting Minnesota's 2015 Interoperable Electronic Health Record Mandate* (July 2010) (Minnesota Department of Health); available at: <http://www.health.state.mn.us/e-health/hitech/ht070810hiesplan.pdf>.

²⁰ Pub. L. No. 104-191, 110 Stat 1936 (codified in sections of 18, 26, 29, and 42 U.S.C.).

²¹ Pub. L. No. 104-191, Title II, Subpt. F.

²² 65 Fed. Reg. 82,474 (Dec. 28, 2000).

²³ Pub. L. No. 111-005.

the electronic transmission of health information (*Transaction Standards*) and to establish privacy and security protections (*Privacy Rule* and *Security Rule*).²⁴ Of the many privacy and security safeguards HIPAA and HITECH establish related to protected health information (PHI)²⁵ - whether it is in electronic, paper, or oral form - two are particularly relevant to the issues addressed in the HRA Study: (1) permissions required to access, use, or disclose PHI; and (2) notification requirements in the case of a privacy breach (unauthorized use or disclosure).

Federal law addresses permissions required to use, access, or disclose health information

Under HIPAA, PHI can be used²⁶ within or disclosed²⁷ outside the covered entity that maintains it only as permitted by the Privacy Rule. Broadly speaking, any health care provider that transmits or receives information electronically in connection with one of a set of common health care transactions is a covered entity.²⁸ A key feature of the federal Privacy Rule is that it permits a patient's PHI to be used or disclosed by a covered entity without the patient's express permission, but **only if** the PHI will be used or disclosed for **treatment, payment or health care operation** purposes exclusively.²⁹ Subject to some very narrow exceptions (for example, to avert a serious threat to health or safety or if ordered by a court), a covered entity must secure the patient's express permission (called an *authorization*) for all other uses or disclosures (for example, disclosures to employers or attorneys, or for fundraising or marketing).³⁰

In January 2013 the Final HIPAA Rule was announced that strengthens and expands patient rights as well as enforcement including;

- Limitations on the use and disclosure of PHI for marketing and fundraising;
- Prohibition on the sale of PHI without authorization;
- Expand rights to receive electronic copies of health information and to restrict disclosures to a health plan concerning treatment paid out of pocket in full;
- Requirement to modify and redistribute notice of privacy practices;
- Modify the individual authorization and other requirements to facilitate research, disclosure of child immunization proof to schools and access to decedent information by family members/others.

²⁴ 45 C.F.R. Parts 160, 162, and 164.

²⁵ *Protected Health Information (PHI)* includes, among other information, individually identifiable information that is created by a covered entity that relates to (1) the physical or mental health or condition of an individual; (2) the provision of health care to an individual; or (3) the payment for such health care. *See*, 45 C.F.R. 160.103.

²⁶ *Use* includes the accessing, sharing, employment, application, utilization, examination, or analysis of PHI within the covered entity that maintains it. 45 C.F.R. 160.103.

²⁷ *Disclosure* means any release, transfer, provision of access to, or divulging of PHI outside the covered entity maintaining it. 45 C.F.R. 160.103.

²⁸ 45 C.F.R. 160.103.

²⁹ 45 C.F.R. 164.506(c).

³⁰ 45 C.F.R. 164.508.

The final HIPAA rule also increases privacy protection for genetic information, includes changes to HIPAA enforcement incorporating higher penalties, and includes the adoption a new Breach Notification Rule that replaces the previous rule's "harm" threshold with a more objective standard.³¹

Federal law notification requirements for the breach of health information privacy and security

Under the Privacy Rule as originally issued, a covered entity has certain obligations in the event of an unauthorized use or disclosure (breach) of an individual's PHI. These include duties to mitigate harm caused by the breach; sanction workforce members who acted in violation of the Privacy Rule or organizational policy; provide an accounting of certain breaches to HHS; and, if requested, provide an accounting of disclosures (including breaches) to a patient.³² The original Privacy Rule did not, however, require a covered entity to proactively notify affected individuals in the event of a privacy or security breach involving their PHI.

The HITECH Act addresses this notification gap. In August 2009, to implement the HITECH Act's breach notification mandate, HHS issued interim final breach notification regulations (*Breach Notification Rule*). The Breach Notification Rule requires a covered entity, after it discovers a breach of unsecured PHI to provide notification to affected individuals, HHS, and in some cases, the media. The notification provisions are effective for breaches occurring on or after September 23, 2009.³³

Breach defined

Under the Breach Notification Rule, not every instance of unauthorized access of an individual's PHI is considered a breach requiring notice to the affected individual. The Breach Notification Rule defines a breach as the acquisition, access, use, or disclosure of unsecured PHI³⁴ that (1) is not permitted by the Privacy Rule, and (2) compromises the security or privacy of the PHI. To determine whether a breach has occurred, the Breach Notification Rule requires a covered entity to perform a risk assessment to establish whether the unauthorized use or disclosure of unsecured PHI creates a significant risk of financial, reputational, or other harm to the affected individual(s). If so, breach notification is required³⁵ (unless a specific limited exception applies³⁶).

³¹ 45 C.F.R. 160 and 164 modifications made for the HIPAA final rule effective March 26, 2013

³² 45 C.F.R. 164.530 (e) and (f) and 45 C.F.R. 164.528

³³ During the 60-day public comment period on the Interim Final Rule, HHS received approximately 120 comments. HHS reviewed the public comment and developed a final rule, which it submitted to the Office of Management and Budget (OMB) for review on May 14, 2010. Later that summer, however, HHS withdrew the final rule from OMB review to allow for further consideration. HHS states that it intends to publish a final rule "in the coming months" and that until such time as a new final rule is issued, the Interim Final Rule that became effective on September 23, 2009, remains in effect. *See*, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/>.

³⁴ *Unsecured PHI* means any patient health information that is not secured through a technology or methodology, specified by HHS that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals found in 45 C.F.R. 164.402.

³⁵ 45 C.F.R. 164.402

³⁶ The law identifies that breach notification is not required in the following circumstances:

1. An **unintentional** acquisition, access, or use of the PHI by a workforce member or an individual, acting upon the authority of the covered entity, who acquired, accessed, or used the PHI in good faith and within the normal scope of the person's authority, if that PHI is not further used or disclosed;

Notice requirement

When a covered entity has a reasonable belief that an individual's PHI has been involved in a breach, the covered entity has an obligation to notify each affected individual personally.³⁷ Notice of a breach must be made to the affected individual(s) "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."³⁸ The notice must be provided by first class mail to the individual's last known address unless the individual agreed to receive it electronically.³⁹ If the breach of unsecured PHI involves more than 500 residents of a state, the covered entity must notify media outlets within that state.⁴⁰ The covered entity must also notify the HHS of all breaches, and "immediately" of any breach involving 500 or more people.⁴¹

Minnesota's Privacy Protection Framework Differs from the Federal Approach

Minnesota's framework for health information privacy protection differs from the federal approach described above, particularly regarding (1) the permissions required to access, use, or disclose PHI; and (2) breach notification requirements.

Minnesota has not enacted a health care information breach notification law

Minnesota law is silent regarding providing notice to affected individuals in the event of a breach of their personal health information.⁴² In the absence of Minnesota requirements, health care organizations must comply with the federal Breach Notification Rule provisions. As explained, the practice regarding breach notification varies across Minnesota's health care organizations. Some organizations provide notice only in the circumstances and by the means dictated by the federal Breach Notification Rule. Others provide notice of unauthorized access, use, or disclosure in instances where the Breach Notification Rule would not require them to do so.

-
2. Any **inadvertent** disclosure by a person who is authorized to access PHI at a covered entity to another person authorized to access PHI at the same covered entity if the PHI is not further used or disclosed in violation of the Privacy Regulations; or
 3. A disclosure of PHI where a covered entity has a **good faith belief** that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

45 C.F.R. 164.402(2).

In addition, if law enforcement determines that notification would impede a criminal investigation or cause damage to national security, covered entities are allowed to delay notification. 45 C.F.R. 164.412.

³⁷ 45 C.F.R. 164.404(a).

³⁸ 45 C.F.R. 164.404(b).

³⁹ Although the Breach Notification Rule does not specify, permission to provide notice electronically would presumably be provided prior to the breach, possibly as part of a request by the patient to receive all correspondence electronically.

⁴⁰ 45 C.F.R. 164.406(a).

⁴¹ 45 C.F.R. 164.408(b).

⁴² Minnesota's breach notification provisions establish requirements related to the breach of personal information **other than** personal health information (for example, personal financial information). Minn. Stat. 325E.61.

Minnesota law addresses the permission needed to disclose, *but not to use or access*, health information

As described above, the federal Privacy Rule addresses the permissions required for a health care organization not only to **disclose** health information outside the organization, but also the permissions required for a health care organization itself to **use** or **access the** health information it maintains. In contrast, the Minnesota Health Records Act (MN HRA)⁴³ addresses only what permissions a health care organization must secure before it **discloses** health information outside the organization. Minnesota law is silent regarding the permission required for a health care entity itself to **use** or **access** the health information it maintains.

To the extent, therefore, that the issues addressed in the HRA Study concern the **use** or **access** of health information by a health care organization itself, federal law alone applies. In contrast, in instances where the issues concern the **disclosure** of health information by the health care entity to a third party, federal and Minnesota law both establish requirements. As described above in section ***, under the federal Privacy Rule, a health care organization must secure a patient's permission (*authorization*) to disclose his or her health care information **except** in situations where the information will be used for **treatment, payment, or health care operations**. In contrast, Minnesota law provides that permission (*consent*) is required for the disclosure (*release*) any health record for **any** purpose, **including treatment, payment, and health care operations**.⁴⁴

Divergent Federal and Minnesota Approaches to Permissions Impact HIE and Patient Privacy

The exchange of health information is promoted in large part to enhance the quality, safety, and cost effectiveness of treatment. As discussed above, HIPAA's Privacy Rule and the MN HRA establish different requirements regarding what permissions a health organization must secure before it discloses (releases) health information to a third party for treatment purposes: HIPAA allows an individual's health information to be exchanged among providers treating an individual without the patient's express permission. The MN HRA prohibits exchange for treatment purposes unless the patient has provided a signed, written permission (consent).

Minnesota is nearly unique among states in requiring patient permission to disclose any type of health information for treatment purposes.⁴⁵ Almost all states instead align their requirements with

⁴³ Minn. Stat. 144.291 – 144.298.

⁴⁴ Unless an exception applies, a provider, or a person who receives health records from a provider, may not release a patient's health records without: (1) a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release; (2) specific authorization in law; or (3) a representation from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. 144.293, subd. 2.

⁴⁵ "Only two states (Minnesota and New York) appear to generally require patient permission to disclose all types of health information." *Privacy and Security Solutions for Interoperable Health Information Exchange Report on State Law Requirements for Patient Permission to Disclose Health Information*, prepared for RTI, International; Section 4-3 (August 2009); available at: <http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf>.

HIPAA and permit the disclosure of most types of health information⁴⁶ without patient permission if the information will be used for treatment purposes. Because most states have standardized their approach to patient permission for release of health information for treatment purposes on the HIPAA model, EHR technology and HIE structures and systems are typically designed and built to meet the HIPAA requirements.

Because Minnesota law is an outlier on this issue, health care organizations must customize standard technological systems (for example, EHRs), administrative procedures, and care workflows to accommodate Minnesota consent requirements before they can release information for treatment purposes. As reported in section *** below, the time and other costs required for such customization can hinder the development of robust health information exchange across the state.

Mitigating the Impact of Minnesota’s Consent Requirements on HIE: *Representation of Consent*

In 2007, the MN HRA was amended to include what has come to be known as the *Representation of Consent* provision.⁴⁷ This provision expands the conditions under which a provider can release a patient’s health information to mitigate (at least partially), the barrier to exchange erected by Minnesota’s “consent to release for treatment” requirement. Prior to enactment of the *Representation of Consent* provision, unless otherwise authorized by law, a provider could release a patient’s health records **only if** the provider was itself in possession of a signed and dated consent to release form from the patient. Under the *Representation of Consent* provision, now a provider who is not itself in possession of a valid consent to release can still release information required for treatment **if** the provider reasonably believes that the Minnesota provider who is requesting the information has secured the appropriate consent from the patient.⁴⁸ In other words, the provider that is being asked to

⁴⁶ “More common is for the state to permit disclosure of general health information for treatment without patient permission, but to require patient permission to disclose information related to certain types of medical conditions, generally considered sensitive.” *Id.*

⁴⁷ The *Representation of Consent* provision language (in bold below) was added to the MN HRA to modify the “consent to release” requirements:

Unless an exception applies, a provider, or a person who receives health records from a provider, may not release a patient’s health records without:… (1) a signed and dated consent from the patient or the patient’s legally authorized representative authorizing the release; (2) specific authorization in law; or (3) **a representation from a provider that holds a signed and dated consent from the patient authorizing the release.**

Minn. Stat. 144.293, subd. 2

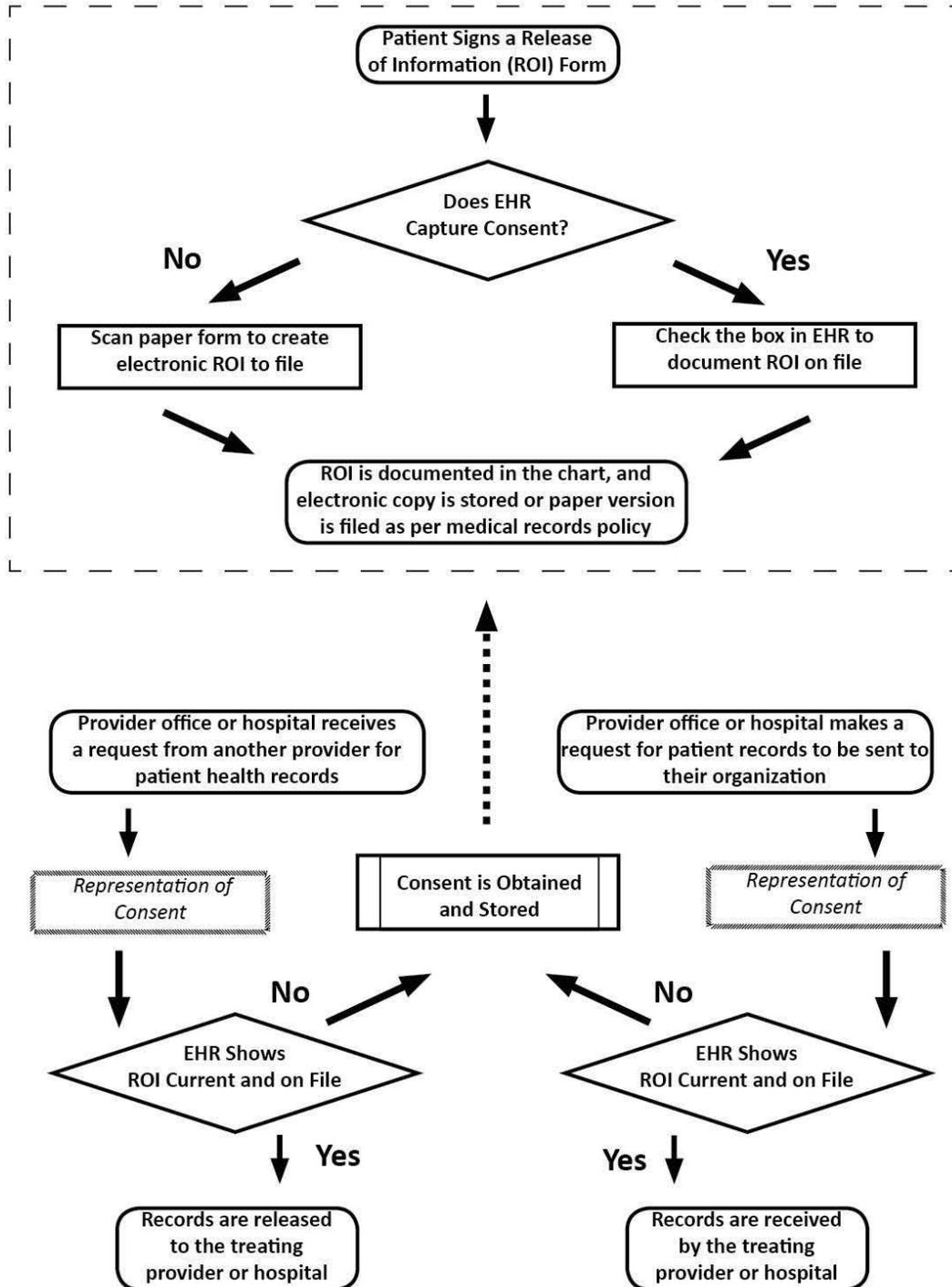
A provider who **releases** health records in reliance upon a requesting provider’s *representation of consent*, must document: (1) the provider requesting the health records; (2) the identity of the patient; (3) the health records requested; and (4) the date the health records were requested. Minn. Stat. 144.293, subd. 9.

⁴⁸ Providers who **request** health records by making a *representation of consent* warrant that the consent (1) contains no information known to be false; and (2) accurately states a patient’s desire to have the health records disclosed or that the release is otherwise authorized by law. Minn. Stat. 144.293, subd. 10.

release the information that the treating provider needs can rely on the treating provider's statement (*representation*) that it has, in fact, secured the patient's written, signed consent to the release.

Although the *Representation of Consent* provision creates the potential for some small efficiency gains in the waning world of manual requests for health information and the exchange of health information in static format (for example, the release via fax of a prescription history from one clinic to another based on a phone request) (*See Attachment A*), its real value is realized in the evolving HIE environment, where requests for, and releases of, health information are effectuated through automated, full-electronic transactions.

Appendix F: Example Workflow: Representation of Consent



Appendix G:

Minnesota e-Health Advisory Committee Members (2012-2013)

<p>Bobbie McAdam Advisory Committee Co-Chair Senior Director, Business Integration Medica Representing: Health Plans</p>	<p>Marty Witrak, PhD, RN Advisory Committee Co-Chair Professor, Dean School of Nursing, College of St. Scholastica Representing: Academics and Research</p>
<p>Alan Abramson, PhD Senior Vice President, IS&T and Chief Information Officer HealthPartners Representing: Health Plans</p>	<p>Thomas A. Baden, Jr. Director, Office of Enterprise Architecture Minnesota Department of Human Services Representing: Minnesota Department of Human Services</p>
<p>Laurie Beyer-Kropuenske, JD Director Community Services Divisions Representing: Minnesota Department of Admin.</p>	<p>John Fraser CEO ApeniMED, Inc. Representing: Health IT Vendors</p>
<p>Raymond Gensinger, Jr., MD Chief Medical Information Officer Fairview Health Services Representing: Professional with Expert Knowledge of Health Information Technology</p>	<p>Sue Hedlund, MA Deputy Director Washington County Public Health Representing: Local Public Health Departments</p>
<p>Maureen Ideker, MBA, RN Director of Telehealth Essentia Health Representing: Small and Critical Access Hospitals</p>	<p>Mark Jurkovich, DDS, MBA Dentist Gateway North Family Dental Representing: Dentists</p>
<p>Paul Kleeberg, MD Clinical Director Regional Extension Assistance Center for HIT Representing: Physicians</p>	<p>Marty LaVenture, PhD, MPH Director, Office of Health IT and e-Health Minnesota Department of Health Representing: Minnesota Department of Health</p>
<p>Jennifer Lundblad, PhD President and Chief Executive Officer Stratis Health Representing: Quality Improvement Organization</p>	<p>Charlie Montreuil Vice President, Enterprise Rewards and Corporate Human Resources Best Buy Co., Inc. Representing: Health Care Purchasers</p>
<p>Kevin Peterson, MD Family Physician Phalen Village Clinic Representing: Community Clinics and FQHCs</p>	<p>Peter Schuna Director of Strategic Initiatives Pathway Health Services Representing: Long Term Care</p>
<p>Peter Pytlak, MBA Chief Patient Experience Officer Mayo Clinic Health System SW MN Region Representing: Health Care Systems</p>	<p>Stuart Speedie, PhD, FACMI Professor of Health Informatics University of Minnesota Representing: Academics and Clinical Research</p>

<p>Steve Simenson, BPharm, FAPhA President and Managing Partner Goodrich Pharmacy Representing: Pharmacists</p>	<p>Joanne Sunquist SVP and CIO HealthEast Care System Representing: Large Hospitals</p>
<p>Cally Vinz, RN Vice President, Health Care Improvement Institute For Clinical Systems Improvement Representing: Clinical Guideline Development</p>	<p>Donna Watz, JD Deputy General Counsel Minnesota Department of Commerce Representing: Minnesota Department of Commerce</p>
<p>Bonnie Westra, PhD, RN, FAAN, FACMIjo Associate Professor University of Minnesota, School of Nursing Representing: Nurses</p>	<p>Ken Zaiken Consumer Advocate Representing: Consumers</p>
<p>Kathy Zwiieg Associate Publisher & Editor-in-Chief Inside Dental Assisting Magazine Representing: Clinic Managers</p>	<p>Cheryl M. Stephens, MBA, PhD Executive Director Community Health Information Collaborative Ex-Officio Exchange Liaison</p>

Minnesota e-Health Advisory Committee Designated Alternates (2012-2013)

<p>Geoffrey Archibald, DDS Dentist North Branch Dental Alternate Representing: Dentists</p>	<p>Wendy Bauman, MS Deputy Director Dakota County Public Health Alternate Representing: Local Public Health</p>
<p>Melinda Machones, MBA Health IT Consultant Alternate Representing: Professional with Expert Knowledge of Health Information Technology</p>	<p>David Osborne Director of Health Information Technology/ Privacy Officer Alternate Representing: Long Term Care</p>
<p>Linda Ridlehuber, RN, MBA Quality Improvement Specialist MN Association of Community Health Centers Alternate Representing: Community Clinics and Federally Qualified Health Centers</p>	<p>Rebecca Schierman, MPH Manager, Quality Improvement Minnesota Medical Association Alternate Representing: Physicians</p>
<p>Susan Severson Director, Health IT Services Stratis Health Alternate Representing: Quality Improvement</p>	<p>Mark Sonneborn Vice President, Information Services Minnesota Hospital Association Alternate Representing: Hospitals</p>

For More Informa. on:



Minnesota Department of Health
Minnesota e-Health Initiative/
Office of Health Information Technology
P.O. Box 64882
85 East Seventh Place, Suite 220
St. Paul, MN 55164-0882
651-201-3662
www.health.state.mn.us/e-health