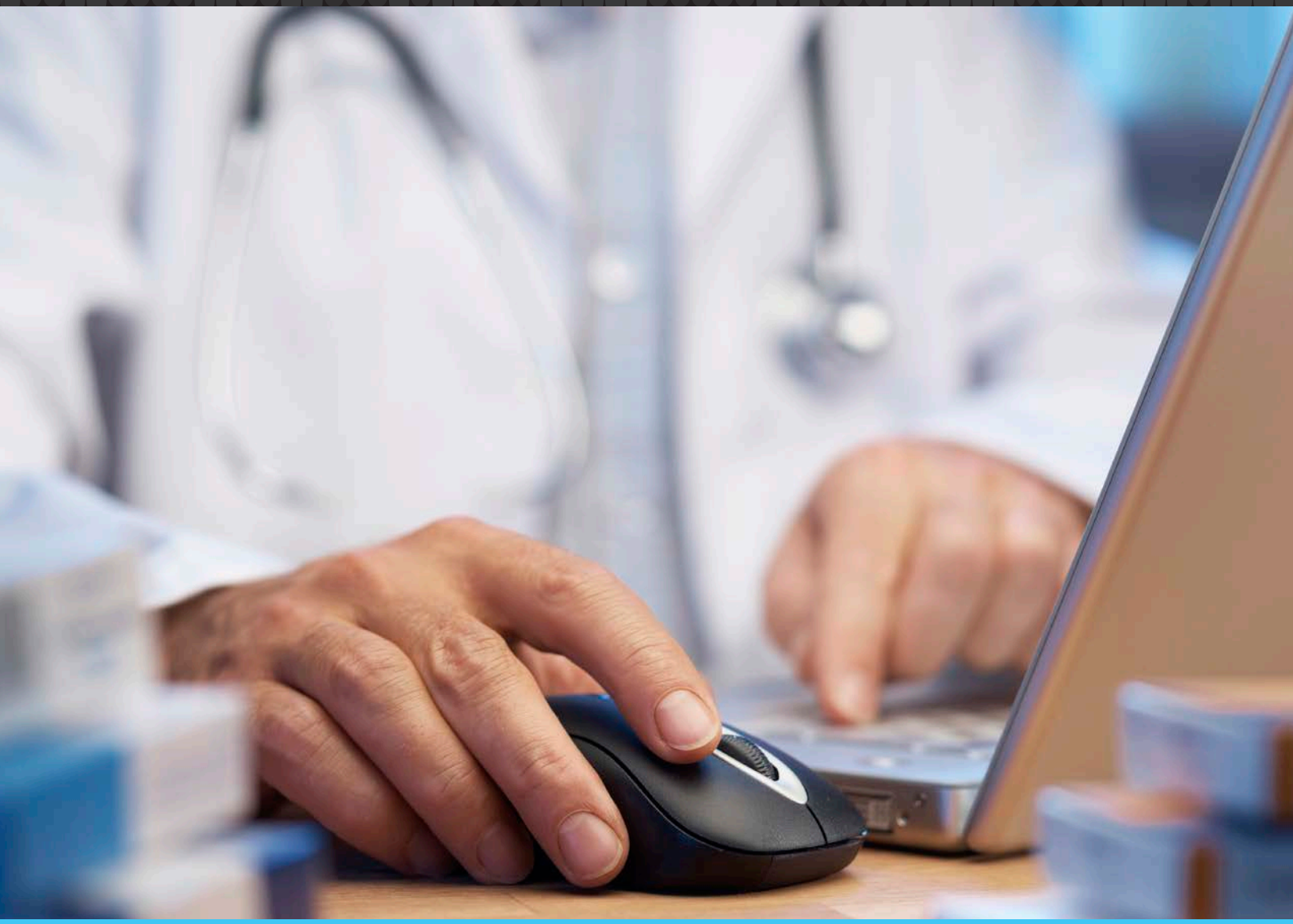
SUMMARY OF
Proactive Monitoring Procedures
for Secure Individual Identifiable Health Information

OCTOBER 2014



Minnesota E-Health Initiative & the Minnesota Department of Health, Office of Health Information Technology

P.O. Box 64882 85 East Seventh Place, Suite 220, St. Paul, MN. 55164-0882
www.health.state.mn.us/e-health/index.html | MN.eHealth@state.mn.us

Table of Contents

Acknowledgements

The Minnesota Department of Health thanks the many members of the Minnesota e-Health Initiative and the Minnesota e-Health Privacy and Security workgroup for their time, leadership and expertise in developing and endorsing this piece.

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

Special Advisor

Vicki Clevenger, Vice President of Compliance & Audit and Chief Compliance and Privacy Officer, Essentia Health

Other Advisors and Project Support

Stacie Christensen, Information Policy Analysis Division, Minnesota Department of Administration
Bob Johnson, Office of Health Information Technology, Minnesota Department of Health
Lisa Moon, Office of Health Information Technology, Minnesota Department of Health

Summary of Proactive Monitoring Procedures for secure individual identifiable health information

Feedback or questions?

Email
mn.ehealth@state.mn.us

Purpose

This document provides a summary of proactive monitoring procedures identified through the Minnesota e-Health Privacy Security Workgroup. This document is meant to be a resource tool for providers and health care organizations and should be used to support compliance programing.

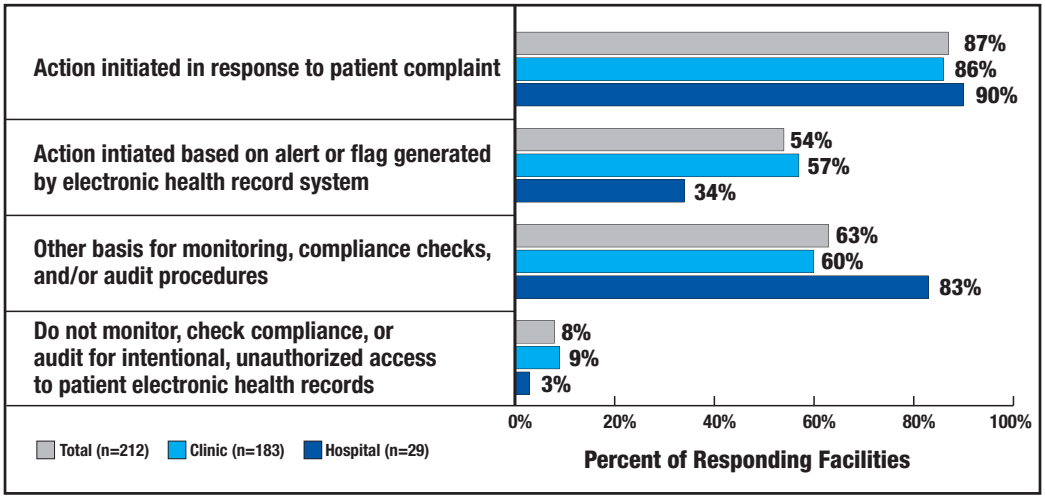
Background

Strong compliance programs are built on privacy, security and compliance functions. Based on both state and federal law, these functions and related activities are necessary so that the patient, who is at the center of the information exchange transaction, can have trust and confidence that their individually identifiable health information is safe within the electronic health record system and when shared with other health care providers.

Minnesota Health Records Access Study Data

The Minnesota Health Records Access Study (HRAS, 2013) conducted a survey of a random sample of 25% of Minnesota hospitals and ambulatory clinics that use electronic health record systems. Additionally, the study conducted three focus groups of Minnesota health information management and privacy experts. The HRAS found that monitoring unauthorized access to a patient's health record is completed through both proactive and reactive methods that are not standardized. Figure 1 shows the most common monitoring procedure was completed in response to a patient complaint.

FIGURE 1: 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

The survey data showed that 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. This may indicate a number of things, including that some EHRs are still not fully implemented or that some systems lack generated alerts in their EHR. It may also be an indication that tools, resources and processes are not in place to complete the needed monitoring process at these sites.

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.

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 that they have systematic auditing, monitoring and compliance policies and procedures in place for both internal and external unauthorized access to patient health records. These core procedures for securing health information appear to be more similar than different across organizations, though the processes for monitoring and auditing may differ from one health care entity to the other based on organizational policies. Most reported going above and beyond the regulations that govern monitoring of electronic health information.

Minnesota e-Health Privacy Security Workgroup

The HRAS report recommended that best practices and existing national standards be identified for proactive and reactive monitoring procedures. These procedures should be used as part of a larger compliance program in a health care organization or health care setting to detect unauthorized access to electronic protected health information. In response to this recommendation, the Minnesota e-Health Privacy Security Workgroup convened to discuss, identify and develop a summary of existing proactive monitoring procedures that can be shared with healthcare organizations statewide.

Proactive Monitoring Procedures

Proactive Monitoring Procedures are only one function within a larger and more robust compliance program. Proactive Monitoring Procedures should be used in conjunction with other administrative, technical, physical frameworks outlined in the Health Insurance Portability and Accountability Act (HIPAA)[1] to ensure the safe and secure use, disclosure and exchange of electronic health information. This federal regulation and the Minnesota Health Records Act[2] create the legal framework on which personally identifiable health information is protected in Minnesota.

Table 1 is a summary of proactive monitoring procedures that were identified through discussion of the Minnesota e-Health Privacy Security Workgroup using consensus methodologies. This is a resource tool for health care providers and organizations to use as part of larger compliance efforts. Some or all of these methods should be implemented in a healthcare setting to strengthen monitoring and audit activities used to detect unauthorized and impermissible access of patient electronic health information.

---

[1] Pub. L. No. 104-191, 110 Stat 1936 (codified in sections of 18, 26, 29, and 42 U.S.C.), 65 Fed. Reg. 82,474 (Dec. 28, 2000) and 45 C.F.R. 160 and 164 modifications made for the HIPAA final rule effective March 26, 2013

[2] Minn. Stat. 144.293-298

Table 1: Summary of Proactive Monitoring Procedures

Proactive Monitoring Procedures: Organized from less technical to more automated		
PROCEDURE	**HOW METHOD IS USED**	**EXAMPLES**
Staff Education to promote a culture of awareness	Conducting Planned and Scheduled Education, Training and Communication Target Audience: • Employee • Medical Staff • Contractor • Volunteer • Students	1. Use training events as a time to ask for staff feedback or questions related to health information safety 2. Results and feedback can be used as a way to monitor perceived risks to the organization 3. Sending compliance reminder emails routinely 4. Annual Staff Training on Privacy Security Topics
Conducting privacy rounds and physical monitoring of building and activities	Compliance staff are visible and accessible in health care setting or organization	1. Physical "Walk-Through" of facility to monitor staff 2. Use an official audit tool to complete a walkthrough of an area 3. Review physical safeguards including security of documents, verbal disclosures, proper disposal, white boards/bulletin boards, etc. 4. Review technical safeguards- unattended computer monitors, use of computer lock outs, etc. 5. Review staff knowledge and understanding of privacy-related matters (e.g. how do they manage PHI, how to report a privacy concern/ask questions, etc.) 6. Ask staff what help they need to protect PHI better within their area 7. Generate an official report with action plans to ensure accountability
Tracking and Trending	Baseline tracking and ongoing trending of incidents or unusual patterns of activity	1. Use results to build monitoring/auditing 2. Identification of educational needs 3. May lead to needed updates in policies, procedures, training, etc.
Monitoring Electronic Health Record access to records of "High Profile" Patients	Tracking access of EHR by staff and contractors when high profile patients or clients access medical care	1. Monitor Current Events: • Someone in news/missing persons • Using Google alerts • Vulnerable populations • VIP (e.g. public figures, celebrities, retired clergy, board members, highly visibility employees/ members of medical staff, etc.)
Performing Random Focused Audits of Electronic Health Record access	Manual random audits that are created based on case by case need	1. Medical emergency actions 2. Work unit audit logs: • Sorting by job titles • Use of data analytics tools

Proactive Monitoring Procedures: Organized from less technical to more automated, *CONTINUED*		
PROCEDURE	**HOW METHOD IS USED**	**EXAMPLES**
Conduct Systematic Audits of Electronic Health Record Access - Either random/periodic audits or continuous auditing	Using audit and business intelligence tools NOTE: the more specific the criteria used in predictive analytics, the less likely false positives or significant investigative work to rule in possible matches	1. Audit criteria can be selected based upon most common risk areas across health care providers or within a covered entity. Organizations with more complex tools are able to layer several pieces of criteria and databases to focus in on possible issues (e.g. medical record and employee database). Examples include: • Same last name • Spouse/child/ emergency contact match • Same address or address within certain radius (e.g. three blocks) • Guarantor match • Health insurance ID match • Department or location mismatch • Records accessed six months after last date of service/patient death
Monitoring Electronic Health Record use of "Break the Glass" type tools	Set-up to deter unauthorized access to record and flag access to records for any reason	1. Whenever going into a patient's chart who hasn't been seen by that facility 2. High Profile patients 3. Medical emergencies 4. Employee records 5. Place on accounts as a risk mitigation strategy for those who have had breaches or at patient's request
Trending Electronic Health Record Access Data followed by Focused Audits	Review data and assess for frequency of access and review users with higher utilization than their peer groups	1. Review date and time of access and compare to work schedules 2. Evaluate high utilization and access by staff and/or contractors 3. Look for trends that point to uncharacteristic access of patient records
Other related Monitoring Activities	Timely user ID / Access Administration	1. Most organizations have multiple applications that store, retrieve and access ePHI. Keeping appropriate user access up to date is critical for each ePHI application. This includes terminated employees/ contractors, people changing jobs/roles, etc.
	EHR audit logs	1. Keeping up to date audit logs secure 2. Controlling access to audit logs
	Monitoring Remote Network Access	1. Monitoring of firewalls, settings, access attempts, etc. is important

Strong Trust Fabric to Ensure Secure Electronic Health Information

Proactive Monitoring Procedures in health care settings are necessary and required. The ongoing work of the Minnesota e-Health Privacy Security Workgroup and the Minnesota eHealth Initiative supports sound privacy and security practices for the management of electronic health information that build patient trust and secure patient confidence.

Without patient trust and confidence, the sharing of health information is 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 be confident in the security measures that have been applied for the protection and exchange of their electronic protected health information.

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.

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.

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. To accomplish this, a health care system must support a framework of compliance that is built on preserving the integrity of the data, while facilitating the secure exchange of health information between providers to promote optimal health care. It is within this framework that the fabric of patient trust and confidence can grow, and meaningful exchange of health information can take place.