Reassessing Your Security Practices in a Health IT Environment:

A Guide for Small Health Care Practices

Disclaimer: *This guide was prepared to help small health care practices learn about the information security considerations that they may need to take into account as they become more reliant on health information technology. Use of this guide is voluntary and while it includes many important concepts, it alone will not enable, nor was it designed to ensure, that a health care practice complies with all applicable Federal and State laws.*

TABLE OF CONTENTS

1 INTRODUCTION

This guide is intended to assist small health care practices[1] in reassessing their existing health information security policies[2] as they consider adopting and implementing emerging health information technology (health IT) capabilities such as electronic health records and electronic health information exchange. In addition, this guide identifies a basic approach to reassessing your health information security policies and poses questions that your practice can use to identify and secure electronic health information[3] as you adopt and implement new health IT. The questions posed by this guide are designed to draw your attention to the importance of conducting risk assessments. It does not, however, focus on or identify the legal obligations (e.g., State and Federal laws) that your practice may also have to take into consideration. This guide assumes your practice currently has some level of health IT in use (e.g., practice management software, electronic billing), and that you are already familiar with developing health information security policies such as those required by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Rule.[4,5] If you consider your experience with security policies to be less than what may be assumed by this document, you may want to contact a local or national association that can identify educational materials for you or consult a qualified professional.

Health information security is an iterative process driven by enhancements in technology as well as changes to the health care environment. As you adopt new health IT to enhance the quality and efficiency of care in your practice, it is also equally important to reassess your health information security policies. Identifying risks and protecting electronic health information can be challenging for small health care practices. This guide is designed to help your practice prepare for those challenges, effectively assess risks, and develop appropriate security policies to protect electronic health information.

Section 2 of this guide provides a general overview of health information security and the steps you can take to improve your awareness and understanding. Section 3 identifies questions that may help your practice determine the difference between your current information security policies and those you may need to develop to protect electronic health information as you adopt and implement electronic health records and participate in electronic health information exchange. Finally, Section 4 provides a collection of resources to support your decision-making processes.

---

[1] For the purposes of this document "small health care practices" are considered to be those practices made up of 10 or fewer health care providers.

[2] The term "security policy(ies)" is used throughout this document to refer to the high-level security guidelines and requirements your practice has established and follows in order to appropriately protect electronic health information.

[3] The term "electronic health information" is used throughout this document to generally refer to any type of individually identifiable health information that is in electronic form.

[4] http://www.cms.hhs.gov/SecurityStandard/02_Regulations.asp#TopOfPage

[5] *Security 101 for Covered Entities* developed by the Centers for Medicare & Medicaid Services can be used to familiarize your practice with basic health information security concepts. This document can be found at http://www.cms.hhs.gov/EducationMaterials/Downloads/Security101forCoveredEntities.pdf.

2 INFORMATION SECURITY IN HEALTH CARE

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and availability of information. In health care, and for the purposes of this guide, confidentiality, integrity, and availability mean the following:

- *Confidentiality* – the property that electronic health information is not made available or disclosed to unauthorized persons or processes.
- *Integrity* – the property that electronic health information have not been altered or destroyed in an unauthorized manner.
- *Availability* – the property that electronic health information is accessible and useable upon demand by an authorized person.

Figure 1, below, provides an illustrative example for implementing and monitoring information security in your practice. Assessing your electronic health information confidentiality, integrity, and availability needs requires you to first understand your practice's health IT environment. This may include the technologies your practice deploys for both clinical and administrative purposes, where those technologies are physically used and located, and how they are used within your practice. As you assess your health IT environment, think about those situations that may lead to unauthorized access, use, disclosure, disruption, modification or destruction of electronic health information.[6] These situations will likely be unique to your practice and may be in the form of technology issues (e.g., lack of securely configured computer equipment), procedural issues (e.g., lack of a security incident response plan), and personnel issues (e.g., lack of comprehensive information security training).

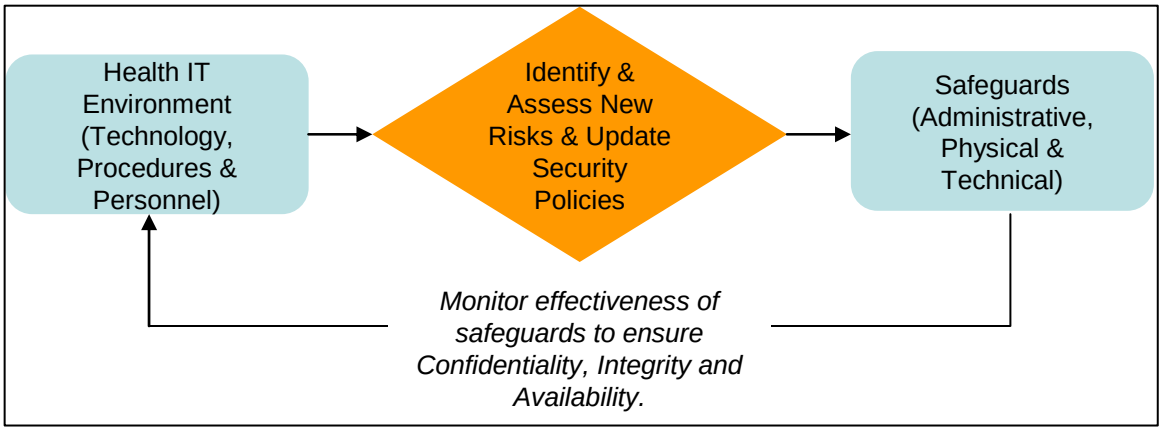

Figure 1: Health Information Security Requires Continual Assessment of Risks to Electronic Health Information

For each risk to electronic health information that your practice identifies, try to understand how likely it would be for an undesirable action or event to occur as a result of that risk, and evaluate

[6] Depending on the level of information security expertise within your practice, you may want to consider seeking outside security expertise to assist you in assessing your health IT environment and determining risks to electronic health information. This guide will help you to ask the right questions in obtaining such expert assistance. In concert with this type of assessment you may also want to consider whether to seek legal counsel familiar with the obligations your practice may need to take into account as you adopt and implement new health IT.

what kind of impact such an action or event would have on your practice and/or your patients. To mitigate each risk your practice can perform two important steps:

1. Review your existing health information security policies and develop new policy statements to address new risks to electronic health information. These new policy statements could require the use of certain technology (e.g., encryption of data on mobile computing equipment such as laptops), further refine who within your practice is authorized to view and administer electronic health information, or clarify and improve how and when electronic health information is provided to patients or other health care entities.
2. Institute your updated health information security policies into your practice to mitigate new risks to electronic health information. This step will help your practice keep security policies current, and decrease the likelihood and/or impact of electronic health information being accessed, used, disclosed, disrupted, modified or destroyed in an unauthorized manner.

Safeguards, the solutions and tools used to implement your security policies, can be administrative (e.g., implementation of new types of training for your workforce), physical (e.g., installation of new facility controls), or technical (e.g., implementation of new technology), examples of which are shown in the table below. It is important to note that the types of safeguards you choose may be limited or required by law, and once you have identified the scope of those safeguards applicable to your practice you may have some flexibility in determining which ones are appropriate for the risks you identified. Performing a trade-off analysis between the benefit received from implementing the safeguard versus the cost of implementing the safeguard is one way to make this determination. For example, your practice may not be able to justify purchasing an expensive technology to mitigate a risk to electronic health information. As an alternative, you may require your personnel to follow a new administrative safeguard that equally mitigates the risk. Conversely, your practice may not be able to accept the additional burden an administrative safeguard puts on your staff, and may opt to purchase a technology instead that automates the safeguard to mitigate the particular risk. Regardless of the type of safeguard your practice chooses to implement, it is important to monitor its effectiveness and regularly assess your health IT environment to determine if new risks are present.

Examples of Administrative Safeguards
• *Continual risk assessment of your health IT environment.*
• *Continual assessment of the effectiveness of safeguards for electronic health information.*
• *Detailed processes for viewing and administering electronic health information.*
• *Employee training on the use of health IT to appropriately protect electronic health information.*
• *Appropriately reporting security breaches (e.g., to those entities required by law or contract) and ensuring continued health IT operations.*
Examples of Physical Safeguards
• *Office alarm systems.*
• *Locked offices containing computing equipment that store electronic health information.*
• *Security guards.*
Examples of Technical Safeguards
• *Securely configured computing equipment (e.g., virus checking, firewalls).*

- *Certified applications and technologies that store or exchange electronic health information.*
- *Access controls to health IT and electronic health information (e.g., authorized computer accounts).*
- *Encryption of electronic health information.*
- *Auditing of health IT operations.*
- *Health IT backup capabilities (e.g., regular backups of electronic health information to another computer file server).*

3 SECURING ELECTRONIC HEALTH INFORMATION IN YOUR HEALTH IT ENVIRONMENT

Using the information and considerations discussed in Section 2, this guide further examines a health IT capability many small health care practices are considering to implement: the electronic health record (EHR). An EHR is "an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization," as defined by the National Alliance for Health Information Technology (NAHIT).[7]

We focus on the EHR because it fundamentally changes your practice's health IT environment, and introduces risks to health information, specifically electronic health information, that you might not have considered before. The EHR is not a subtle enhancement to your existing health IT processes. Rather, it is intended to introduce significant efficiencies in the delivery of health care to your patients. In effect, it can become the cornerstone to your health IT environment. While you may first use EHRs within your practice to maintain medical records in electronic form, you may have also purchased your system to exchange electronic health information through a variety of mechanisms with other health care entities and your patients.

For example, you may decide to participate in a health information organization (HIO), defined by the NAHIT as, "an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards" or engage in health information exchange (HIE), which is also defined by the NAHIT as, "the electronic movement of health-related information among organizations according to nationally recognized standards."[8,9] Or you may decide to implement an extension within your EHR that allows your patients to access and view their electronic health information (e.g., via a portal). Additionally, you may also leverage a capability within your EHR to establish some form of on-line communications with your patients (e.g., secure messaging).

EHRs can have a wide-ranging impact, and ensuring the confidentiality, integrity, and availability of EHRs (and electronic health information contained within EHRs) can be challenging. The sections below were developed to assist you think about the types of security policies your practice may need to define as your reassess your ability to appropriately protect EHRs. The first set of questions, categorized by confidentiality, integrity, and availability, is designed to help you assess a health IT environment that now includes EHRs, and any new risks

[7] http://www.hhs.gov/healthit/documents/m20080603/10_2_hit_terms.pdf
[8] http://www.hhs.gov/healthit/documents/m20080603/10_2_hit_terms.pdf
[9] http://www.hhs.gov/healthit/documents/m20080603/10_2_hit_terms.pdf

to electronic health information you may find from analyzing that environment. The second set of questions, categorized by administrative, physical, and technical safeguards, is targeted to helping you define appropriate information security safeguards to protect electronic health information.

Both sets of questions focus primarily on EHRs and electronic health information exchange. By thinking about and addressing these questions, you will help prepare yourself to securely implement your EHR, as well as properly position your practice to understand and address the security challenges you may face if you plan to participate in a HIO or offer your patients electronic access to your EHRs.

Assessing Risks Regarding EHRs and Other Health IT Within Your Health Care Practice

Questions to Ask Yourself When Assessing Confidentiality Risks
• What new electronic health information has been introduced into my practice because of EHRs? Where will that electronic health information reside?
• Who in my office (employees, other providers, etc.) will have access to EHRs, and the electronic health information contained within them?
• Should all employees with access to EHRs have the same level of access?
• Will I permit my employees to have electronic health information on mobile computing/storage equipment? If so, do they know how, and do they have the resources necessary, to keep electronic health information secure on these devices?
• How will I know if electronic health information has been accidentally or maliciously disclosed to an unauthorized person?
• When I upgrade my computer storage equipment (e.g., hard drives), will electronic health information be properly erased from the old storage equipment before I dispose of it?
• Are my backup facilities secured (computers, tapes, offices, etc., used to backup EHRs and other health IT)?
• Will I be sharing EHRs, or electronic health information contained in EHRs with other health care entities through a HIO? If so, what security policies do I need to be aware of?
• If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet (e.g., through a portal), am I familiar with the security requirements that will protect my patients electronic health information before I implement that feature?
• Will I communicate with my patients electronically (e.g., through a portal or email)? Are those communications secured?
• If I offer my patients a method of communicating with me electronically, how will I know that I am communicating with the right patient?

Questions to Ask Yourself When Assessing Integrity Risks
• Who in my office will be permitted to create or modify an EHR, or electronic health information contained in the EHR?
• How will I know if an EHR, or the electronic health information in the EHR, has been altered or deleted?
• If I participate in a HIO, how will I know if the health information I exchange is altered in an unauthorized manner?
• If my EHR system is capable of providing my patients with a way to access their health record/information via the

Internet (e.g., through a portal) and I implement that feature, will my patients be permitted to modify any of the health information within their record? If so, what information?

Questions to Ask Yourself When Assessing Availability Risks

- How will I ensure that electronic health information, regardless of where it resides, is readily available to me and my employees for authorized purposes, including after normal office hours?
- Do I have a backup strategy for my EHRs in the event of an emergency, or to ensure I have access to patient information if the power goes out or my computer crashes?
- If I participate in a HIO, does it have performance standards regarding network availability?
- If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet (e.g., through a portal) and I implement that feature, will I allow 24/7 access?

Identifying Safeguards for EHRs and Other Health IT Within Your Health Care Practice

Questions to Ask Yourself When Identifying Administrative Safeguards

- Have I updated my internal information security processes to include the use of EHRs, connectivity to HIOs, offering portal access to patients, and the handling and management of electronic health information in general?
- Have I trained my employees on the use of EHRs? Other electronic health information related technologies that I plan to implement? Do they understand the importance of keeping electronic health information protected?
- Have I identified how I will periodically assess my use of health IT to ensure my safeguards are effective?
- As employees enter and leave my practice, have I defined processes to ensure electronic health information access controls are updated accordingly?
- Have I developed a security incident response plan so that my employees know how to respond to a potential security incident involving electronic health information (e.g., unauthorized access to an EHR, corrupted electronic health information)?
- Have I developed processes that outline how electronic health information will be backed-up or stored outside of my practice when it is no longer needed (e.g., when a patient moves and no longer receives care at the practice)?
- Have I developed contingency plans so that my employees know what to do if access to EHRs and other electronic health information is not available for an extended period of time?
- Have I developed processes for securely exchanging electronic health information with other health care entities?
- Have I developed processes that my patients can use to securely connect to a portal? Have I developed processes for proofing the identity of my patients before granting them access to the portal?
- Do I have a process to periodically test my health IT backup capabilities, so that I am prepared to execute them?
- If equipment is stolen or lost, have I defined processes to respond to the theft or loss?

Questions to Ask Yourself When Identifying Physical Safeguards

- Do I have basic office security in place, such as locked doors and windows, and an alarm system? Are they being used properly during working and non-working hours?
- Are my desktop computing systems in areas that can be secured during non-working hours?
- Are my desktop computers out of the reach of patients and other personnel not employed by my practice during normal working hours?
- Is mobile equipment (e.g., laptops), used within and outside my office, secured to prevent theft or loss?

- Do I have a documented inventory of approved and known health IT computing equipment within my practice? Will I know if one of my employees is using a computer or media device not approved for my practice?
- Do my employees implement basic computer security principles, such as logging out of a computer before leaving it unattended?

Questions to Ask Yourself When Identifying Technical Safeguards

- Have I configured my computing environment where electronic health information resides using best-practice security settings (e.g., enabling a firewall, virus detection, and encryption where appropriate)? Am I maintaining that environment to stay up to date with the latest computer security updates?
- Are their other types of software on my electronic health information computing equipment that are not needed to sustain my health IT environment (e.g., a music file sharing program), which could put my health IT environment at risk?
- Is my EHR certified[10] to address industry recognized/best-practice security requirements?
- Are my health IT applications installed properly, and are the vendor recommended security controls enabled (e.g., computer inactivity timeouts)?
- Is my health IT computing environment up to date with the most recent security updates and patches?
- Have I configured my EHR application to require my employees to be authenticated (e.g., username/password) before gaining access to the EHR? And have I set their access privileges to electronic health information correctly?
- If I have or plan to establish a patient portal, do I have the proper security controls in place to authenticate the patient (e.g., username/password) before granting access to the portal and the patient's electronic health information? Does the portal's security reflect industry best-practices?
- If I have or plan to set up a wireless network, do I have the proper security controls defined and enabled (e.g., known access points, data encryption)?
- Have I enabled the appropriate audit controls within my health IT environment to be alerted of a potential security incident, or to examine security incidents that have occurred?

4 RESOURCES

We hope your practice has found this guide useful in understanding and addressing health care information security challenges. To supplement and complement the information provided within this guide, a list of some publicly available Federal resources is compiled below. The first set of resources represents guidance from the Centers for Medicare and Medicaid Services (CMS) – the agency within the Department of Health and Human Services responsible for implementing and enforcing the HIPAA Security Rule – that can be referred to if your practice has questions about complying with HIPAA Security Rule. The second set of resources is a limited set of National Institute of Standards and Technology (NIST) Special Publications that may be of interest to your practice. While NIST specifically establishes standards for Federal agencies, their Special Publications are generally considered industry best-practices, and as a result may offer additional insights for your practice as it relates to electronic health information security.

[10] One organization that certifies EHRs is the Certification Commission for Healthcare Information Technology (CCHIT) (www.cchit.org).

Resources Developed at the U.S. Federal Level

Centers for Medicare and Medicaid Services (CMS) Security Information Series:

- Security 101 for Covered Entities – *This document provides a general overview of the HIPAA Security Rule, and clarifies important Security Rule concepts that will help covered entities as they plan for implementation.*
- Security Standards: Administrative Safeguards – *This document addresses standards for Administrative Safeguards and their implementation specifications, and assumes the reader has a basic understanding of the Security Rule.*
- Security Standards: Physical Safeguards – *This document addresses standards for Physical Safeguards and their implementation specifications, and assumes the reader has a basic understanding of the Security Rule.*
- Security Standards: Technical Safeguards – *This document addresses standards for Technical Safeguards and their implementation specifications, and assumes the reader has a basic understanding of the Security Rule.*
- Security Standards: Organizational Policies – *This document addresses standards for Organizational Requirements, Policies, Procedures and Documentation Requirements, and their implementation specifications, and assumes the reader has a basic understanding of the Security Rule.*
- Basics of Risk Analysis and Risk Management – *This document addresses the required risk analysis and risk management implementation specifications, and assumes the reader has a basic understanding of the Security Rule.*
- Security Standards: Implementation for the Small Provider – *This document is devoted to implementation of the Security Rule standards, implementation specifications and requirements as they relate to covered entities that are sole practitioners or otherwise considered small providers. It assumes the reader has a basic understanding of the Security Rule.*
- HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information (EPHI) – *This document reinforces some of the ways a covered entity may protect EPHI when it is accessed or used outside of the organization's physical purview. In so doing, it sets forth strategies that may be reasonable and appropriate for organizations that conduct some of their business activities through (1) the use of portable media/devices (such as USB flash drives) that store EPHI and (2) offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers or other non corporate equipment.*

National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), and their Special Publications (SPs).

- SP 800-12: An Introduction to Computer Security: The NIST Handbook – *SP 800-12 is written primarily for those who have computer security responsibilities and need assistance understanding basic concepts and techniques. This publication can be used as educational material for those employees in your practice that have information security responsibilities.*
- SP 800-30: Risk Management Guide for Information Technology Systems – *SP 800-30 provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. This publication can be used by your practice to support risk assessment and management functions in support of your health IT environment.*
- SP 800-39: DRAFT Managing Risk from Information Systems: An Organizational Perspective – *SP 800-39 provides guidelines for managing risk to organizational operations, organizational assets, individuals, and other organizations resulting from the operation and use of information systems. This publication can assist your practice in assessing and managing overall information risk within your practice.*
- SP 800-66 Rev1 : An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule: *SP 800-66 helps educate readers about the security standards included in the HIPAA Security Rule. This publication can help your practice better understand the HIPAA Security Rule and how to use other NIST standards and publications to implement safeguards*

Resources Developed at the U.S. Federal Level

consistent with the Security Rule.

- SP 800-70 Rev 1: DRAFT National Checklist Program for IT Products – Guidelines for Checklist Users and Developers: *SP 800-70 describes security configuration checklists and their benefits. This publication can assist your practice in developing a security checklist to help maintain your health IT environment, and specifically addresses the small business environment applicable to a small health care practice.*
- SP 800-100: Information Security Handbook: A Guide for Managers: *SP 800-100 informs information security managers about various aspects of information security that they will be expected to implement and oversee in their respective organizations. This publication can assist your practice in defining, organizing and operating an information security management program to monitor and maintain your information security policies and safeguards for protecting* electronic health information.