The Journal of the Michigan Dental Association

Volume 105 | Number 8 Article 5

8-1-2023

HIPAA Update: Conducting a Security Risk Analysis

Jennifer Cosey
Eagle Associates, jennifer@eagleassociates.net

Recommended Citation
Cosey, Jennifer (2023) "HIPAA Update: Conducting a Security Risk Analysis," *The Journal of the Michigan Dental Association*: Vol. 105: No. 8, Article 5.
Available at: https://commons.ada.org/journalmichigandentalassociation/vol105/iss8/5

HIPAA Update: Conducting a Security Risk Analysis

Cover Page Footnote

Eagle Associates is endorsed by the MDA to provide HIPAA, OSHA, and Office of the Inspector General compliance assistance to member dental offices

HIPAA Update: Conducting a Security Risk Analysis

By Jennifer Cosey
President, Eagle Associates

The Security Rule of the Health Insurance Portability and Accountability Act, at paragraph 45 CFR 164.308(a)(1)(ii)(A), requires documentation of periodic security risk analyses. A Security Risk Analysis assesses compliance with standards within the HIPAA Security Rule.

This Rule requires covered entities to implement written policies and procedures to prevent, detect, contain, and correct security risks to the electronic protected health information, or EPHI, that they have created, collected, and maintain.

An effective SRA assesses threats and vulnerabilities, and considers all devices, media, software, hardware, etc., that access, store, or transmit EPHI, or connect to a network. Thus, a comprehensive asset listing is an important starting point to ensure that the SRA evaluates all items that

Good information to know in the never-ending quest to make sure your office systems are safe and secure, and that you are in full compliance with federally required HIPAA regulations.

are impacted by security measures. In addition to traditional workstations, servers, hard drives, and other devices, the listing should include devices such as diagnostic equipment, Voice Over Internet Protocol phone systems, scanners, etc., if they connect to your network.

The Security Rule is flexible and scalable, meaning that no one software program or specific technology is required by the Rule, and the size and complexity of your organization may be considered in this analysis. However, it does not mean that small organizations may ignore security rule standards. But the good news is that your dental practice may consider a wide range of solutions that fit your needs.

IT vendors and staff

Your IT vendor or staff is a valuable resource for finding and implementing HIPAA safeguards. Be sure that you have contracted with or hired an experienced IT vendor that is aware that you store and transit EPHI. Unfortunately, hackers and other bad actors are well-aware that dental care entities utilize EPHI, and target dental practices for malware and other attacks. Note: Gone are the days of having a friend or family member who "likes computers" come in and set up and manage your network. The use of a qualified IT professional is necessary to ensure the security and integrity of your EPHI.

There is no specified format for conducting an SRA. The federal government has a tool at the following link that may be used: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. Many companies have developed their own templates as well.

Threats and vulnerabilities

Identifying reasonably anticipated threats to EPHI is part of the risk assessment process. A *threat* is a person or event that has the potential to impact EPHI in a negative manner. Threats are generally grouped into categories, such as human, environmental, physical, and technical.

A *vulnerability* is a weakness that can be exploited or triggered by a threat, resulting in a risk to EPHI. Vulnerabilities may also be categorized, first into technical and non-technical types, and then further into categories, such as human, environmental, and physical.

Identifying threats and vulnerabilities allows appropriate safeguards to be selected to mitigate risks to the confidentiality, availability, and integrity of EPHI. Mitigation, also referred to as corrective action, is any effort to prevent a threat from having a negative impact on EPHI; to limit the impact if total prevention is not possible; and to improve the speed or effectiveness of a recovery effort.

For More Help — Eagle Associates Is Endorsed by the MDA

Eagle Associates, endorsed by the MDA for member regulatory compliance assistance, can assist your practice in complying with HIPAA's Security Rule, including completion of a Security Risk Analysis. Contact Eagle Associates by phone at 800-777-2337 or email info@eagleassociates.net for more information. Identify yourself as an MDA member to access exclusive bundles and discounts.

Types of safeguards

Administrative safeguards are intended to provide the practice with actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures for EPHI, and to manage the conduct of the practice's workforce (staff and external persons

(Continued on Page 46)

or entities involved with EPHI). Examples of administrative safeguards include managing access to information (creating privilege sets/roles within systems), training, contingency planning, managing business associates and agreements, and so on.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, as well as from unauthorized intrusion. Examples of physical safeguards would include: facility access controls such as locks, keys, keypads, alarm systems, security cameras; workstation security such as side shields or blur screens; or physical cables and locking mechanisms, etc.

Technical safeguards are intended to provide the technology, policies, and procedures for the use and protection of EPHI in a practice's information system. There are many technical security tools, products, and solutions from which a practice may select. Determination of specific security measures is up to each individual practice, based upon what is reasonable and appropriate for the organization. Technical safeguards can range from auditing controls and reporting, to multi-factor authentication methods, transmission security such as encryption or secure file sharing, data integrity mechanisms, and so on.

Each set of safeguards contains specifications, which are instructions for meeting the requirements. Some specifications are required, while others are addressable. Required specifications must be implemented without exception, but there is always flexibility for how the specification is met (the software, methodology, etc.). Addressable specifications should be implemented if they are reasonable and appropriate for your practice's environment.

Three options exist for addressable specifications:

- If an addressable implementation specification is determined to be reasonable and appropriate, your practice must implement it.
- If an addressable implementation specification is determined to be an inappropriate or unreasonable security measure for your practice, but a reasonable and appropriate alternative exists, your practice may implement an equivalent alternative method that accomplishes the same end.
- If you have determined that a specification is not applicable, or you decide not to implement the specification or a reasonable alternative, your practice must document the decision, along with the rationale behind it. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

Technical review

A Technical Network Assessment, or TNA, is a documented snapshot of your practice's IT infrastructure with regard to specific Security Rule requirements. The purpose of a TNA is to provide objective documentation concerning the security protections that have been implemented. A key aspect is that a TNA produces factual reports from your network demonstrating that protections are in place, rather than relying on a strictly anecdotal response.

Reports from a TNA will enable your organization to determine whether any corrective actions need to be implemented to mitigate or reduce risks to EPHI on the network. A repeat or periodic TNA should be performed to address environmental, technical, or operational changes affecting the security of EPHI.

A TNA should be conducted by qualified IT vendor/personnel. Some vendors will provide them at no charge as part of your existing maintenance contract, especially if you pay a monthly/regular management fee. You could have your existing IT vendor or staff perform a TNA, or contract with an outside entity. Using an outside entity will provide your practice with an independent confirmation that key technical security requirements have been met, and will help determine whether your IT vendor is performing capably.

Elements of a TNA

A TNA should evaluate technological risks and vulnerabilities including, but not limited to:

- Open port security.
- Internal and external user IDs.
- User IDs that have been inactive for a period of time (i.e., 30 days or more).
- Network devices and implementation of current security updates or patches.
- Current network protocol for complexity and frequency of password changes by users.

About the Author

Jennifer Cosey is president of Eagle Associates, which is endorsed by the MDA to provide HIPAA, OSHA, and Office of the Inspector General compliance assistance to member dental offices. Cosey has also been featured as a speaker at various MDA continuing education events. To learn more about Eagle Associates, visit mdaprograms.com and look under MDA Services and regulatory compliance.

Cosey

- Installation of antivirus/malware protection and a firewall.
- Automatic logoff and the period of inactivity to activate logoff.
- Activation of lockout protections (a predetermined number of allowable unsuccessful login attempts).
- A vulnerability scan.

Documentation of TNA results should be available in network-generated reports as outlined below — note that the names and types of reports will vary depending on the tools used to generate the TNA.

Computer identification report: A list of the active and inactive computers found in the active directory. It should show the machine name, its enabled status, operating system, last login date, and should include columns to indicate whether the machine contains any EPHI.

User identification report: A list of the active and inactive user accounts found in the active directory. It should show the user name, display name, last login date, last password reset date, password expiration date, and last login time. It would be helpful if the report included columns to manage the users and note their access to EPHI.

Endpoint security status: A listing of all the computers and servers found on the network and including their status on antivirus, antispyware, firewall, and backup software installed.

External vulnerability scan detail report: Detailed information on all the external vulnerabilities found during the external IP address scan performed on the IP addresses used by the network.

Security policy assessment: The results of a security scan performed internally on the network. This document will highlight your office's password policies, account lockout policies, audit policies, event log policies, and group policies.

Patch status: This report will contain a list of each computer and its corresponding patch status.

Corrective actions to take

After the data has been gathered and reports generated, your practice should evaluate the results for possible corrective actions, if any, to mitigate your risks and vulnerabilities. The combined documentation of the SRA, TNA, and implemented corrective actions will enhance your practice's ability to demonstrate its efforts to protect EPHI.

Although a practice security officer often holds primary responsibility for making corrective actions, various practice processes may be affected. Be sure to communicate any changes down to applicable staff, or provide training on new procedures and protocols as appropriate. ●

Journal
THE DENTIST'S ROLE IN RECOGNIZING SLEEP-DISORDERED BREATHING IN CHILDREN
Journal
Oral Health Consideration for Cancer Therapy Patients