TOPIC:

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE: SAFEGUARDING ELECTRONIC PROTECTED HEALTH INFORMATION

INTRODUCTION:

Congress enacted the Health Insurance Portability and Accountability Act (“HIPAA”) in 1996 for, among other reasons, the purpose of improving the portability and continuity of health insurance coverage, simplifying the administration of health insurance, and addressing the privacy and security of health information held by HIPAA-covered entities – health plans, health care clearinghouses, and certain health care providers. While the primary mission of colleges and universities is educational, many institutions provide health care in the form of medical schools, health plans, or health clinics for use by students, staff, and the community. Thus, prior to using or disclosing health information, colleges and universities will need to assess whether and what aspects of their institution are covered by the HIPAA Security Rule.

This NOTE provides a summary of the HIPAA Security Rule, includes information to assist covered entities in complying with the Security Rule, and offers suggested steps for the development and implementation of health information security policies and procedures.

DISCUSSION:

I. What Does HIPAA Require?

HIPAA requires the establishment of “standards” for the electronic transmission of health information to achieve administrative simplification and to encourage the development of a uniform, electronic health information system.

Specifically, HIPAA requires the U.S. Department of Health and Human Services (“DHHS”) to establish standards in the following areas: (1) transactions; (2) unique health identifiers; (3) security of health information; and (4) privacy of health information.

II. To What Do the Standards Apply?

The DHHS-adopted standards apply to the following covered entities (“CE”): (1) a health plan; (2) a health care clearinghouse; (3) a health care provider that transmits any health information in electronic form in connection with a covered transaction; and (4) a prescription drug card sponsor. Many institutions will determine that specific departments or activities within their institution are CEs, and therefore, that the HIPAA standards are applicable to them.
III. The HIPAA Security Regulations

General Requirements

The purpose of the HIPAA Security Regulations [7] is to establish uniform, national standards for the security of electronic protected health information (“EPHI”). This is distinct from the Privacy Rule, which establishes privacy standards for protected health information in any form or medium [8]. EPHI is individually identifiable health information that is either: (i) transmitted by electronic media, or (ii) maintained in electronic media. EPHI does not include individually identifiable health information in: (i) education records covered by the Family Educational Rights and Privacy Act (“FERPA”) [9]; (ii) treatment records excluded from the definition of “education records” under FERPA; and (iii) employment records held by a CE in its role as employer [10]. Therefore, student treatment records are not protected by HIPAA, but would be protected by state medical records laws. If such records are disclosed for purposes other than treatment, then they would be considered educational records protected by FERPA.

The security regulations require covered entities to do the following:

- Ensure the confidentiality, integrity, and availability of all EPHI that the CE creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.
- Ensure compliance with the security regulations by its workforce [11].

A covered entity may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications as delineated in the regulations [12]. In deciding which security measures to use, the CE must take into account the following factors: (i) the size, complexity, and capabilities of the CE; (ii) the CE’s technical infrastructure, hardware, and software security capabilities; (iii) the costs of the security measures; and (iv) the likelihood and severity of potential risks to EPHI [13].

The cost of compliance alone is not a sufficient reason not to implement a specific procedure or measure [14]. All of the above factors must be considered in developing a compliance plan.

Organization of the Security Standards

The HIPAA Security Standards are organized into three main categories of administrative, physical, and technical safeguards. Each of the main categories contains a list of standards, which are to be put into practice according to implementation specifications identified for each standard.

Implementation specifications are labeled either “required” or “addressable.” If identified as “required,” the CE must implement the specification. If identified as “addressable,” the CE must:

- Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment when analyzed with reference to the likely contribution to protecting the entity’s EPHI; and
- As applicable to the entity –
  a. Implement the implementation specification if reasonable and appropriate; or
  b. If not reasonable and appropriate –
     i. Document why it would not be reasonable and appropriate to implement the implementation specification; and
     ii. Implement an equivalent alternative measure if reasonable and appropriate [15].
Administrative Safeguards [16]

The administrative safeguard requirements generally address the selection, development, implementation, and maintenance of security policies and procedures, including the assignment of responsibility for compliance and the training and oversight of the entity’s employees. There are nine administrative safeguard standards, most of which have specific implementation specifications (here noted in the footnotes).

- **Security Management Process.** Implement policies and procedures to prevent, detect, contain, and correct security violations [17].
- **Assigned Security Responsibility.** Identify the security official who will be responsible for the development and implementation of the required security policies and procedures.
- **Workforce Security.** Implement policies and procedures to ensure all members of the workforce have appropriate access to EPHI and prevent access by those workforce members who should not have access [18].
- **Information Access Management.** Implement policies and procedures for authorizing access to EPHI that are consistent with the Privacy Rule [19].
- **Security Awareness and Training.** Implement a security awareness and training program for all members of its workforce, including management [20].
- **Security Incident Procedures.** Implement policies and procedures to address security incidents [21].
- **Contingency Plan.** Establish and implement policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI [22].
- **Evaluation.** Perform a periodic technical and non-technical evaluation that establishes the extent to which a covered entity’s security policies and procedures meet the requirements of the Security Standards.
- **Business Associate Contracts and Other Arrangements.** Obtain satisfactory assurances that a business associate will appropriately safeguard EPHI.

Physical Safeguards [23]

The physical safeguard requirements relate to the practices, policies, and procedures aimed at protecting the covered entity’s EPHI, and the systems, equipment and facilities that house EPHI, from natural and environmental threats, and unauthorized access. There are four physical safeguard standards, two with implementation specifications.

- **Facility Access Controls.** Implement policies and procedures to limit physical access to systems and facilities in which they are housed [24].
- **Workstation Use.** Implement policies and procedures that specify the functions to be performed, the manner in which to perform them and the physical surroundings of one or more workstations that can access EPHI.
- **Workstation Security.** Implement physical safeguards to prevent unauthorized use of workstations that can access EPHI.
- **Device and Media Controls.** Implement policies and procedures regarding the receipt, removal, movement, and disposal of hardware and electronic media that contain EPHI [25].

Technical Safeguards [26]

The technical safeguard requirements are the technology and the policies and practices regarding its use, and are intended to protect EPHI and prevent unauthorized access to it. There are five technical safeguard standards, three with implementation specifications.

- **Access Control.** Implement policies and procedures to allow access to systems containing EPHI only to authorized users [27].
- **Audit Controls.** Implement hardware, software, and/or procedural mechanisms that record and
examine activity in information systems that contain or use EPHI.

- **Integrity.** Implement policies and procedures to protect EPHI from improper alteration or destruction [28].
- **Person or Entity Authentication.** Implement policies and procedures to ensure that a person or entity seeking access to EPHI is the one claimed.
- **Transmission Security.** Implement security measures to ensure that electronically transmitted EPHI is not improperly accessed or modified without detection during transmission and until disposal [29].

In addition to the main categories of safeguards noted above, the regulations also require organizational and documentation standards.

**Organizational Requirements** [30]

The organizational requirements relate to business associate relationships and specific requirements placed upon covered health plans.

- **Business Associate Contracts (“BAC”) or Other Arrangements.** Contracts or other arrangements between covered entities and their business associates must incorporate specific provisions. Existing BACs may need to be amended or new agreements created [31].
- **Requirements for Group Health Plans.** Group health plans must limit the EPHI disclosed to the plan sponsor or ensure the plan documents require the plan sponsor to safeguard EPHI [32].

**Policy and Documentation Requirements** [33]

Security policies and procedures and all required actions and assessments must be documented in writing (which may be in electronic form); must be retained for six years from the date of creation or date when it was last in effect, whichever is later; must be available to those responsible for implementation; and must be reviewed and updated periodically.

- **Policies and Procedures.** Implement reasonable and appropriate policies and procedures to comply with standards.
- **Documentation.** Document in writing all policies, procedures and required actions and assessments [34].

**IV. Implementation of the Security Rule**

The list of security standards and specifications appears daunting, especially to hybrid covered entities [35], such as colleges and universities, whose primary mission is education, not health care. Fortunately, the security regulations allow covered entities flexibility in their approach to compliance. CEs may adopt security measures that are proportional to their size and complexity. No specific technology is required, although campus IT personnel should play a critical part in compliance planning and implementation of the Security Rule. A small college with a covered health plan or health center will not be expected to implement the same measures adopted by a large university with a medical school, teaching hospital, and affiliated medical practices. The words to keep in mind are “reasonable” and “appropriate.” A CE may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications as indicated in the regulations [36].

No particular approach to risk analysis or risk management is required. A CE must “[c]onduct an accurate and thorough assessment of potential risks and vulnerabilities [37]” of EPHI and “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level [38].”

Although each institution should tailor its compliance efforts to its specific operations and needs, the following sections are intended to guide institutions in the development and implementation of health information security policies and procedures [39].
Risk Assessment

Before a covered entity can develop and implement security policies and procedures, it will need to engage in information gathering and assessment. Surveys, inventories, interviews, observations, audit reports, and previous assessment documentation can all provide information necessary to do an accurate assessment. The following are examples of the type of questions that an institution should consider answering during this process:

1. Inventory of institutional EPHI. What types of EPHI does the institution have, where is it maintained, how much of it is there, and who has or needs access to it?
2. What are the vulnerabilities, weaknesses and security gaps of the current information technology system, hardware, software, facilities, work force, policies, and practices?
3. What are the existing and potential threats to the confidentiality, accessibility, and integrity of EPHI: internal, external, human, natural, and environmental?
4. What administrative, physical, and technological security measures are currently in place?
5. What is the likelihood of a security breach? What would be the impact of a specific security breach?

The information generated in response to the above questions may be used to evaluate the current level of risk to an institution’s EPHI. It may be helpful to conceptualize the interrelation of vulnerabilities, threats, impact, and risk by using the following equations:

\[ \text{Vulnerability} + \text{Threat That Can Exploit Vulnerability} = \text{Likelihood of Breach} \]
\[ \text{Likelihood of Breach} \times \text{Potential Impact} = \text{Level of Risk} \]

Existing security measures may decrease the likelihood of a security breach and lower the level of risk, and therefore should be taken into consideration when evaluating the level of risk presented by each vulnerability and its corresponding threat [40]. The documentation coming out of the risk assessment process should identify the information systems involved and the vulnerabilities, threats, risks, and existing security measures associated with them [41].

Develop and Implement a Security Plan

When the specific risks to EPHI and the levels of risk have been determined, the covered entity will need to look at the security measures, policies, and practices currently in place and decide whether and where additional and/or different security measures are needed to meet the requirements of the Security Rule and to reduce the risks to EPHI to a reasonable and appropriate level. The CE must meet all of the security standards and all of the required implementation specifications. It also must assess whether each addressable implementation specification is reasonable and appropriate, considering the specific circumstances of the CE, and document that assessment. If the addressable specification is reasonable and appropriate, then the CE must implement it. Conducting a gap analysis between existing security measures and the requirements of the Security Rule will help the CE to define and prioritize its compliance efforts.

The security regulations allow covered entities flexibility in their approach to compliance. The regulations require no specific technologies, software, or hardware. CEs may adopt security measures that are proportional to their size and complexity; for example, a small health center will not be expected to implement the same measures adopted by a large hospital. The plan should include, but not necessarily be limited to, the following information: (i) vulnerabilities, threats, risks, current security measures, and risk levels; (ii) recommended security measures; (iii) prioritized actions; (iv) selected security measures; (v) resources required for implementing the selected security measures; (vi) responsible staff; (vii) starting date for implementation; (viii) target completion date; (ix) maintenance requirements [42]; (x) required training of staff; and (xi) periodic evaluation.
All of the relevant constituencies within the covered entity, from senior management to end users, should have input into the development of the security compliance plan. This will ensure that the plan is feasible. The most detailed plan in the world will not succeed without buy-in from those who will have to fund, implement, and work with it. Having a comprehensive but workable security compliance plan will make implementation and compliance more effective and efficient [43].

Continuing Compliance

The covered entity’s obligations under the Security Rule do not end with implementation of the security plan. The CE must periodically evaluate, reassess and adjust its security measures, including its policies and procedures. The evaluations should be done at regular intervals and at any time there are changes in the Security Rule, technology, software, hardware, staff members, functions, facilities, or threats, or any other changes that affect the security of EPHI.

HIPAA provides for civil or criminal penalties [44] for noncompliance. In general, the civil penalty will be not more than $100 for each violation, except that the total amount imposed on a person for all violations of an identical requirement during a calendar year may not exceed $25,000. There are limitations on this penalty when the failure to comply is due to reasonable cause and is cured within 30 days, when the noncompliance was not known and could not have reasonably been known by the person, and when other penalties apply. Also, no civil penalty will apply when the criminal penalty is applicable [45].

DHHS enforces civil monetary penalties, while the U.S. Department of Justice enforces criminal penalties [46].

And, although DHHS enforcement regulations provide for a formal complaint process, compliance reviews, and the imposition of penalties, the primary methods for achieving compliance are through voluntary, cooperative, informal processes and technical assistance from DHHS [47].

CONCLUSION:

At first blush, the requirements of the HIPAA Security Rule may appear insurmountable, especially to colleges and universities whose primary mission is not health care, but education. However, the security regulations, unlike the HIPAA Privacy Rule, allow covered entities flexibility in their approach to compliance. CEs may adopt security measures that are proportional to their size, complexity, technical infrastructure, hardware and software security capabilities, and resources, and the likelihood and extent of potential risks to EPHI. The words to keep in mind throughout the security compliance process and continuing review are “reasonable” and “appropriate.”

FOOTNOTES

AUTHOR:
Nina Lavoie

RESOURCES FOR COUNSEL:

NACUA Resources:

• HIPAA Resources and Links
Statutes and Regulations:

- **Health Insurance Portability and Accountability Act** (42 U.S.C. §§1320d-1320d-8)
- **DHHS – Security Standards for the Protection of EPHI** (45 C.F.R. §§164.302-164.318)
- **DHHS – HIPAA Administrative Simplification** (45 C.F.R. Parts 160, 162 and 164)
- **DHHS – Privacy of Individually Identifiable Health Information** (45 C.F.R. § 164.500(a))
- **Family Educational Rights and Privacy Act (“FERPA”)** (20 U.S.C. 1232g)
- **Medicaid (42 U.S.C. § 1396 et seq.)**
- Medicare Prescription Drug Discount Card (42 U.S.C. § 1395w-141(h) (6) (A))

Agency Guidance:

- **Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services, HIPAA Security Series**
- **National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 800 Series of Special Publications**

Other Resources:

- **Nina Lavoie Security Standards and Specifications Chart**
- **Health Information and Management Systems Society, CPRI Toolkit: Managing Information Privacy & Security in Healthcare**
- **American College Health Association HIPAA Resource Page**
- **EDUCAUSE/Cornell Institute for Computer Policy and Law**

---

Permitted Uses of NACUANOTES Copyright and Disclaimer Notice