O'CONNELL ARONOWITZ

ATTORNEYS AT LAW

SUMMARY OF HIPAA AND THE HITECH ACT

An Overview of the Security and Privacy Rules, Their Application and How to Comply

Kurt E. Bratten

Introduction and Background

The Health Insurance Portability and Accountability Act ("HIPAA") was enacted August 21, 1996. HIPAA consists of five Titles and covers many topics, including national identifiers for providers, health insurance plans, and employers, electronic health transactions, medical spending accounts and various insurance issues. Under Title II of HIPAA, known as the Administrative Simplification provisions, the Secretary of the U.S. Department of Health and Human Services ("HHS") was required to publish standards for the electronic exchange, privacy and security of health information.

The Secretary of HHS issued the Privacy Rule and Security Rule to implement this requirement. The Privacy Rule established a set of national standards for the protection of certain health information, the use and disclosure of that information and individuals' privacy rights in their health information. The Privacy Rule standards apply to what was defined as "protected health information" or "PHI" and those organizations subject to the Rule, defined as "covered entities". The primary aim of the Privacy Rule is to protect individuals' health information while allowing the flow of that information to promote high quality health care and to protect the public's health and well-being.

HIPAA's Administrative Simplification provisions also required the Secretary of HHS to publish national standards for the security of electronic protected health information ("e-PHI") and the electronic exchange and security of health information, which is referred to as the Security Rule. The Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities and business associates to use to assure the confidentiality, integrity, and availability of e-PHI. A major goal of the Security Rule is to protect the privacy of individuals' health information in a manner that allows flexibility for covered entities in developing and adopting new technologies to protect and use e-PHI. The Security Rule was designed to be flexible and scalable so that covered entities can implement the appropriate policies, procedures, and technologies based on the entity's size, organizational structure, risks and vulnerabilities.

Within HHS, the Office for Civil Rights ("OCR") has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities, investigations of complaints, audits and civil money penalties.

The HITECH Act

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") is part of the American Recovery and Reinvestment Act of 2009. The HITECH Act was created to facilitate the implementation of electronic health records (EHR) and supporting technology in the healthcare industry. The HITECH Act was passed in response to the rise in the use and exchange of e-PHI between medical providers, insurance plans and other entities as a means of delivering better quality of care to patients and cutting the cost of healthcare. The HITECH Act amended the Security and Privacy Rules by expanding and strengthening these privacy and security protections, providing for more stringent enforcement, imposing the same standards for protecting e-PHI on business associates as are applicable to covered entities, and modifying the standard for reporting breaches of unsecured PHI.

Disclaimer

This document is meant to provide a simplified and straightforward explanation of the most important and relevant aspects of the Privacy and Security Rules that were implemented under HIPAA and the HITECH Act. It does not address the Breach Notification Rule. This document is a summary; not a complete guide to compliance or the applicable regulatory requirements. Any organization that is obligated to comply with the Privacy and Security Rule requirements should consult the law and the applicable regulations. This document is not a comprehensive analysis on the Privacy and Security Rules and it should not be relied upon as a source of legal information or advice.

THE PRIVACY RULE

Who Does HIPAA Apply To

Generally, the Privacy and Security Rules apply to covered entities, business associates and the entities that they contract with. The term "**covered entity**" is defined to mean any of the following: (1) health plan; (2) health care clearinghouse; or (3) health care provider who engage in certain electronic transactions covered by the HIPAA Administrative Simplification transaction standards.[1] The definition of health plan includes individual and group plans and employer group plans with 50 or more participants or that are administered by a third party.

In reviewing the health care provider definition, entities are sometimes confused by the electronic transaction standard and its applicability. The Administrative Simplification Transaction Standards apply

to any electronic transaction between two parties to carry out financial or administrative activities related to health care. These requirements apply to all providers who conduct electronic transactions, not just those who accept Medicare or Medicaid. Below are some examples of the types of electronic transactions covered by this standard:

- Billing or claims submission
- Transmission of encounter data or requests for encounter data
- Receiving or requesting payment for healthcare services
- Seeking or receiving payment and remittance advice
- Checking claims status
- Checking or verifying eligibility
- Enrollment and disenrollment
- Requesting or receiving information about healthcare referrals and/or authorizations
- Coordination of benefits
- Health plan premium payment

Health care providers that conduct any of these transactions electronically are covered entities as these transactions are governed by the Administrative Simplification Transaction Standards.[2]

In general, a **business associate** is a person or organization, other than a member of a covered entity's workforce, that creates, receives, maintains or transmits PHI on behalf of a covered entity.[3] Business associates perform a function or service on behalf of a covered entity that involves the use or disclosure of individually identifiable health information. Some examples of business associate relationships include, but are not limited to, legal, data hosting, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. On the other hand, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of PHI, and where any access to PHI would be incidental or nonexistent.

The final regulations implemented after the passage of the HITECH Act (referred to as the Final Omnibus Rule) expanded the business associate definition to include data storage companies, entities that provide data transmission services if they require routine access to PHI such as Health Information Organizations, and subcontractors of business associates.[4] Accordingly, an entity does not need to have actual access to PHI to be a business associate. It is also important to note that a covered entity can be the business associate of another covered entity.

O'CONNELL AARONOWITZ

ATTORNEYS AT LAW

Business Associate Agreements

Even though HIPAA now applies directly to business associates—with or without a business associate agreement—HIPAA requires covered entities and business associates to execute valid business associate agreements before disclosing PHI to the business associate.[5]

The first part of this process is to analyze whether business associate rules apply at all. Out of a desire to be cautious or overprotective, some covered entities ask other organizations to sign business associate agreements even though the "business associate" definition has not been met. Entities should avoid assuming business associate liabilities or entering business associate agreements if it is not required. These agreements create legal liabilities and obligations and can suggest an incorrect and misleading relationship or legal status. For instance, the following entities are not business associates: (i) entities that do not create, maintain, use or disclose PHI in performing services on behalf of the covered entity; (ii) other healthcare providers when providing treatment; (iii) members of an organized healthcare arrangement; (iv) members of the covered entity's workforce; (v) entities who do not use PHI on behalf of the covered entity; and (vi) entities that are mere conduits of the PHI.[6]

Business associate agreements must include certain provisions and issues, including but not limited to: (i) address permissible uses and/or disclosures of PHI; (ii) require that the business associate help the covered entity respond to the exercise of patient rights; and (iii) certain termination provisions.[7] In addition, business associates must: (i) comply with the Security Rule[8]; (ii) execute downstream business associate agreements with their subcontractors[9]; (iii) if the business associate carries out a duty of a covered entity, comply with any HIPAA rule applicable to such duty[10]; and (iv) report breaches of unsecured PHI to the covered entity.[11]

Breaches of business associate agreements potentially expose the business associate to contract liability and HIPAA penalties. Noncompliance by a business associate can also result in liability to the covered entity, although covered entities are generally not liable for the actions of their business associates unless the entity knows of a pattern of conduct or practice that materially violates the business associate's obligation and there is a failure to cure such violation[12], or the business associate is acting as the agent of the covered entity.[13] To avoid liability, covered entities should ensure that business associates are acting as independent contractors, not agents of the covered entity.

Business associates must also execute valid subcontractor agreements if the business associate uses subcontractors or other entities to provide any services for the covered entity involving PHI. These business associate agreements with subcontractors must contain the same terms outlined above[14] as the subcontractor has become a business associate subject to HIPAA.[15] The subcontractor agreement must be at least as stringent as the primary business associate agreement between the covered entity and the business associate and it cannot grant the subcontractor the right to act in ways that are inconsistent with that original business associate agreement.[16]

Business associates should be aware of the Privacy Rule requirements for several reasons. First, covered entities may want to pass down some of their obligations onto the business associate through the parties' agreement, which requires adherence to the Privacy Rule standards. Second, there are components of the Privacy Rule that are applicable to business associates such as complying with the minimum necessary standard and general rules regarding the use and disclosure of PHI.[17] While most of the Privacy Rule provisions do not apply directly to business associates, they should implement many of the same policies and safeguards that the Privacy Rule requires for covered entities and may be asked to do so by contract.

What Information is Protected

The Privacy Rule protects "**individually identifiable health information**" held or transmitted by a covered entity or its business associate, in any form or media. The Privacy Rule defines this information as **protected health information** or **PHI**.[18] Individually identifiable health information is information, including demographic data, that relates to: (i) the individual's past, present or future physical or mental health or condition; (ii) the provision of health care to the individual, or (iii) the past, present, or future payment for the provision of health care to the individual; and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[19] Examples are many of the common identifiers used in our everyday lives, such as name, address, birth date and Social Security Number. In short, the definition of PHI is extremely broad and will be met if both components are present: demographic information and health information, as defined above.

Significantly, PHI does not include employment records that a covered entity maintains in its role as an employer and also excludes education and certain other records that are subject to, or defined by, other laws such as the Family Educational Rights and Privacy Act.[20]

The concept of de-identified health information is a frequent topic of debate among covered entities because there are no restrictions on its use or disclosure.[21] The legal standard for **de-identification** is a challenging one to meet. De-identified health information neither identifies nor provides a reasonable basis to identify an individual and there are only two accepted ways to de-identify health information. De-identification can be done either (1) through a formal determination by a qualified statistician; or (2) by removing specified identifiers of the individual and their relatives, household members, and employers, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

In order to meet the "safe harbor" method of de-identification, the regulation requires that the following personal identifiers of the individual and the individual's relatives, employers, and household members be removed:

A. Names;

B. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
C. All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
D. Telephone numbers;
E. Fax numbers;
F. Electronic mail addresses;
G. Social security numbers;
H. Medical record numbers;
I. Health plan beneficiary numbers;
J. Account numbers;
K. Certificate/license numbers;
L. Vehicle identifiers and serial numbers, including license plate numbers;
M. Device identifiers and serial numbers;
N. Web Universal Resource Locators (URLs);
O. Internet Protocol (IP) address numbers;
P. Biometric identifiers, including finger and voice prints;
Q. Full face photographic images and any comparable images; and
R. Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met.[22]

In addition to the removal of the identifiers described above, the covered entity may "not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[23] As should be clear from the terms of the standard itself, this method of de-identification of PHI is challenging for most organizations to meet.

Permitted Uses and Disclosures of PHI

The general rule is that a covered entity cannot use or disclose PHI except: (1) as the Privacy Rule permits or requires; or (2) as the person who is the subject of the PHI (or the individual's personal representative) authorizes in writing.[24] Required disclosures of PHI arise in only two situations: (a) when individuals (or their personal representatives) specifically request access to, or an accounting of disclosures of, their PHI; and (b) to HHS in connection with a compliance investigation, review or enforcement action.[25]

Covered entities are permitted, but not required, to use and disclose protected health information, without an individual's authorization, for a number of specific purposes or situations, which are defined as exceptions to the general rule stated above. These exceptions and acceptable disclosures and uses of PHI, which do not require patient authorization, include the following[26]:

A. To the Individual (unless required for access or accounting of disclosures);
B. For Treatment, Payment, and Health Care Operations;
C. When the Individual has an Opportunity to Agree or Object;
D. Incident to an Otherwise Permitted Use and Disclosure;
E. Public Interest and Benefit Activities; and
F. Use of a Limited Data Set for the Purposes of Research, Public Health or Health Care Operations.

The Treatment, Payment, and Health Care Operations[27] exception is one of the more commonly used bases for disclosure or use of PHI without patient authorization. A covered entity may use and disclose PHI for its own treatment, payment, and health care operations activities[28]. A covered entity also may disclose PHI for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

Another important means for covered entities to use or disclose PHI without consent is when the individual is given the opportunity to agree or object[29]. This exception is applicable where covered entities seek informal permission from the individual or if circumstances clearly give the individual the opportunity to agree, acquiesce, or object. In emergency situations, or when the individual is incapacitated or not available, covered entities may use and disclosure PHI if, in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual. This exception often plays out when a covered entity relies on an individual's informal permission or extenuating circumstances to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, PHI that is directly relevant to the individual's care and the relative's involvement.

The Privacy Rule also allows covered entities to make certain incidental uses or disclosures[30] of PHI. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is allowed as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule. This exception is based on the Privacy Rule's intention to protect privacy without obstructing normal and essential communications and practices among covered entities and their workforce members.

HIPAA contains numerous exceptions that allow disclosures of PHI to the extent another law requires disclosures or for certain public safety and government functions, including reporting of abuse and neglect, responding to government investigations and making disclosures to avoid a serious and imminent threat to the individual.[31] This includes the use and disclosure of PHI without individual authorization when required by law, and includes disclosures mandated by statute, regulation, and valid court orders, subpoenas and legal process.[32]

When these uses and disclosures occur, covered entities and business associates must take reasonable steps to verify the identity of the person to whom a disclosure is being made[33] and they must take care to disclose or use only the information that is minimally necessary to carry out the intended purpose.[34]

Authorized Uses and Disclosures of PHI

The use of a written authorization that is signed by the individual or patient is required for all uses and disclosures of PHI that do not fit an exception or permitted use under HIPAA.[35] An authorization must be written in plain language and contain specific terms and information about the information to be disclosed and used, including the person(s) disclosing and receiving the information, expiration date, the right to revoke in writing, and other language. State law and the nature of the PHI that is being disclosed or used will often dictate additional requirements in authorization forms. Treatment, payment, enrollment, or benefits eligibility may not be conditioned on an individual's authorization.[36]

Covered entities must obtain written authorization before using an individual's PHI for marketing purposes, including most non-face-to-face communications for treatment purposes if the covered entity receives financial remuneration for the communication.[37] Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[38] While no authorization is needed to make a communication that meets one of the exceptions to the marketing definition, the rules in this area can be complicated and highly fact-specific when applied.

The Minimum Necessary Standard

One of the most misapplied and vital aspects of the Privacy Rule is what is known as the "minimum necessary" standard. This standard applies to business associates and covered entities. Covered entities must make reasonable efforts to use, disclose, and request only the minimum amount of PHI that is necessary to accomplishing the intended purpose of the use, disclosure, or request.[39] Covered entities must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary amount, which is much easier to implement as a matter of policy than in practice. This is a challenging standard because it precludes covered entities from using, disclosing, or requesting an entire medical record or set of records unless the record(s) is reasonably needed for the purpose for which the use, disclosure or request was made. For example, covered entities and business associates that grant workforce members full access to their electronic health record system must have a compelling

reason to do so that matches up with that person's job description or function. The minimum necessary standard requires that entities take steps to ensure that only those members of their workforce who need access to PHI to carry out their job duties have such access, and that it is limited to those categories of PHI that are needed.

The minimum necessary standard does include some exceptions in that it does not apply in connection with disclosures or requests by a health care provider for treatment, disclosures to the subject individual or their personal representative, and certain uses and disclosures that are mandated by law or the government.[40]

Notice of Privacy Practices and Other Individual Rights

Covered entities must provide individuals with a notice of privacy practices that contains certain required elements, including descriptions of how the entity uses PHI and individuals' rights, such as the right to limit disclosures to insurers and the right to complain to HHS and the covered entity if the individual believes their privacy rights were violated.[41] This notice must also state that the covered entity is required to notify the individual of a breach of unsecured PHI, to protect individuals' privacy, provide a notice of privacy practices, and abide by the terms of the notice. The notice must mention a point of contact for further information and for making complaints to the covered entity.

There are specific distribution requirements for this notice that are applicable and tailored to direct treatment providers, all other health care providers, and health plans.[42] For instance, covered health care providers with a direct treatment relationship with individuals are required to make a good faith effort to obtain a written acknowledgment of receipt of the notice from all covered patients and individuals, except in an emergency treatment situations.[43] The Privacy Rule does not prescribe any particular content for the acknowledgement but the provider must document the reason for any failure to obtain this written acknowledgement.

Individual Access Rights

With certain limited exceptions, individuals have the right to obtain and review a copy of their PHI in a designated record set.[44] A "**designated record set**" is the group of records maintained by or for a covered entity that is, (i) the individuals' medical and billing record, (ii) the record that is used, in whole or in part, to make decisions about the subject individual, or (iii) the enrollment, payment, claims adjudication, and case or medical management record systems of a health plan.[45] An individual's right to obtain their medical records or PHI is also clearly spelled out in State law. While HIPAA requires the provision of a designated record set within 30 days of the request, New York generally requires a physician or health care provider to allow for the inspection of requested health records within 10 days and to provide copies within a reasonable time.

The Right to Amend PHI

The Privacy Rule gives individuals the right to have covered entities amend their PHI in a designated record set when that information is inaccurate or incomplete.[46] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment.[47] Additionally, a covered entity must amend PHI in its designated record set upon receipt of notice to amend from another covered entity.

Accounting of Disclosures

Individuals have a right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates for the preceding 6 year period.[48] Numerous disclosures are excluded from the right to request an accounting, including the following: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures.[49] Further, accounting of disclosures made to health oversight agencies and law enforcement officials must be suspended when such an accounting would likely impede these activities.

The Right to Place Restrictions

The Privacy Rule provides for optional and mandatory restrictions on information, at the request of the individual. Individuals whose information is covered under HIPAA have the right to request numerous restrictions on the way that covered entities use and disclose their PHI and how the entity communicates with the individual. For instance, an individual or patient may seek restrictions on a covered entity's use or disclosure of PHI for treatment, payment or health care operations, disclosures to persons involved in the individual's health care or payment for health care, and disclosures to family members or others about the individual's general condition, location, or death.[50] While the covered entity is not obligated to agree to these requests, any covered entity that accepts or agrees with such a request must comply with it.

Other restrictions are mandatory. For instance, an individual has the right to elect restrictions with regard to the method of communication used by certain covered entities. Health plan and health care provider covered entities must permit individuals to request an alternative means or location for receiving

communications of PHI by means other than those that the covered entity typically uses.[51] For example, a health plan or health care provider covered entity must agree to an individual's request that PHI be communicated via email or through a designated address or phone number, even if it is less secure than the covered entity's alternative and has the potential to compromise the security of the PHI.

Administrative and Documentation Requirements

The Privacy Rule was designed to allow flexibility and scalability based on the size, nature and particularities of the covered entity's business. The Rule is intended to allow covered entities to analyze their own needs and challenges and implement solutions appropriate based on their needs, resources and environment. While this scalability standard is present in the Privacy Rule and the broader set of HIPAA requirements, compliance with these standards necessarily means that covered entities must undertake certain mandated actions and create the necessary policies, procedures and documentation, even if there is flexibility in the manner in which this is accomplished.

Designate Privacy Personnel

Covered entities must assign responsibility by designating a person(s) to serve as their HIPAA privacy officer, and document the designation in writing.[52]

Establish Privacy Policies and Safeguards

A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[53] This means that the covered entity should document in the form of policies and procedures those required issues, such as the entity's designation of privacy personnel, proper use and disclosure of PHI and how it will comply with individual rights and the minimum necessary standard.

In addition, covered entities must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and that limit incidental use and disclosure to those instances where it is truly permitted or required.[54] These mandated safeguards are not just policies and general instructions to the workforce but they are supposed to facilitate and operationalize in an efficient and effective manner the standards and requirements imposed on the covered entity. Examples include procedures for securing and accessing e-PHI on the covered entity's EHR system, document and media destruction practices and securing and limiting access to paper PHI by lock and key or pass code.

HIPAA Training

A frequently overlooked requirement and cornerstone to an effective HIPAA compliance program and culture is training. Covered entities are required to train all workforce members on its privacy policies and procedures, as necessary and appropriate to carry out their job duties and functions.[55] Importantly, workforce members include not just employees, but also volunteers, trainees, and potentially anyone whose conduct is under the direct control of the entity.[56] Covered entities must have a sanctions policy or standard and apply appropriate sanctions against workforce members who violate its privacy standards or the Privacy Rule.[57]

Mitigation

Another vital requirement that all covered entities must comply with is the need to mitigate violations of the Privacy Rule. More specifically, the mitigation standard requires each covered entity to mitigate, to the extent practicable, any harmful effects caused by a use or disclosure of PHI by its workforce or business associates in violation of its privacy policies or the Privacy Rule.[58] In practice, mitigation is about taking reasonable and prompt steps to avoid repeating a violation or improper disclosure or use of PHI in response to a known failure, misstep or violation. Proper mitigation means that the entity will not be repeatedly making the same mistake or find itself struggling with the same type of security incident over and over again. Depending upon the nature of the problem, appropriate mitigation sometimes requires an outside expert and perspective to help address the issue and present and institute a best practice.

Complaints and Anti-Retaliation Provisions

A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[59] Among other things, covered entities must identify to whom individuals can submit complaints and advise that complaints can be submitted to the Secretary of HHS.

A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[60] Similarly, a covered entity may not require an individual to waive any right under the Privacy Rule "as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits".[61]

THE SECURITY RULE

The Security Rule applies to covered entities and the majority of its provisions apply to business associates, namely the requirement to implement administrative, physical and technical safeguards. The Security Rule applies strictly to "**electronic protected health information**" or **e-PHI**, a subset of the broader universe of PHI, and is defined as PHI that is transmitted or maintained by or in electronic media.[62] As a result, the Security Rule does not apply to PHI that is maintained in paper form or that is transmitted orally or in writing.

The General Rule

The Security Rule requires the implementation of reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, the general rule is that "Covered entities and business associates must do the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
4. Ensure compliance with this subpart by its workforce."[63]

It is important to keep these aims of ensuring the confidentiality, integrity and availability of e-PHI in mind when reviewing the safeguard requirements as this requires an ongoing balancing act in which compliance is dependent on maintaining all three standards or perspectives. The Security Rule defines "confidentiality" to mean that e-PHI is not used or disclosed improperly or to unauthorized persons or processes, which is the part of the Security Rule that we can all relate to.[64] But it is equally important to consider the integrity and availability components in establishing compliant security measures. Under the Security Rule, data "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner, while "availability" means that e-PHI is accessible and usable on demand by an authorized person.[65] Sometimes decisions and security measures that would foster greater confidentiality result in compromising or weakening data integrity or availability. Organizations must find a way to strike the proper balance between these three aims.

Technical Yet Flexible

The safeguard requirements contained in Sections 164.308, 164.310 and 164.312 of the Security Rule are highly technical in nature. To a significant degree, the Security Rule codifies technology standards and best practices. While covered entities and business associates are free to implement the Security Rule

safeguard requirements on their own, most covered organizations engage Information Technology and/or Cybersecurity experts to assist them with this process.

Although the Security Rule's implementation is largely a technical process, the Rule was made to be flexible and scalable to allow covered entities and business associates to analyze their needs, risks, vulnerabilities and implement solutions appropriate and tailored to their specific environments. HHS readily acknowledges that what is appropriate for one entity may not be for another, and that implementation depends on the nature of the organization's business, size and resources. Accordingly, when a covered entity or business associate is deciding what measures to implement, the Security Rule allows the organization to use "any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications …"[66] In making this determination, the Security Rule requires that the organization consider the following factors in determining what security measures to use:

1. The size, complexity, and capabilities of the covered entity or business associate.
2. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
3. The costs of security measures.
4. The probability and criticality of potential risks to e-PHI.[67]

The Security Rule imposes an ongoing obligation on all covered entities and business associates to review and modify their security measures to adapt and continue to ensure the confidentiality, integrity and availability of e-PHI as the environment and risks change.[68]

Risk Analysis and Management

The Administrative Safeguards section of the Security Rule requires covered entities and business associates to perform a risk analysis. The risk analysis and risk management standards in the Security Rule are viewed by OCR as cornerstones to a compliant and effective response to HIPAA and the security of e-PHI. In particular, the risk analysis is essential because it helps determine which security measures are reasonable and appropriate for a particular entity and largely dictates how the Security Rule safeguard requirements are addressed.

An organization's risk analysis process must include, but is not limited to, the following considerations:

1. An assessment of the potential risks and vulnerabilities to the organization's e-PHI.[69]
2. Reasonably anticipated threats or hazards to the security or integrity of e-PHI.[70]
3. The probability and criticality of the potential risks to e-PHI.[71]
4. Implement appropriate security measures to address the risks identified in the risk analysis.[72]

The Rule dictates that a covered entity or business associate document its risk analysis and the security measures that it elected to implement and, if required, the rationale for adoption.[73] The risk analysis process should be ongoing, as the covered entity or business associate should regularly review its records to monitor access to e-PHI and detect security incidents,[74] periodically evaluate the effectiveness of its security measures,[75] and routinely re-evaluate potential risks to e-PHI.[76]

Administrative, Physical and Technical Safeguards

The Security Rule requires covered entities and business associates to implement or address a wide range of safeguards or security measures. These safeguards are classified into three categories: administrative, physical and technical. The administrative safeguards include issues such as risk assessment and risk management processes,[77] designating a security officer,[78] applying the "minimum necessary" standard,[79] workforce training,[80] management and supervision,[81] and sanctions.[82] Physical safeguards address access and control of facilities,[83] workstation and device security and access,[84] and the transfer, removal, disposal and re-use of electronic media.[85] The technical safeguard requirements address issues that include access to e-PHI,[86] audit and integrity controls,[87] and security of e-PHI transmission.[88] Attached as **Exhibit A** is a chart containing all of the specific administrative, physical and technical safeguards imposed by the Security Rule.

These safeguards should be implemented by covered entities and business associates and documented. The application and implementation of these safeguards is not straightforward as the Security Rule categorizes certain security specifications as "Addressable," while others are "Required." To state the obvious, covered entities and business associates must implement all "Required" specifications. "Addressable" specifications must be assessed and a determination must be made as to whether the specification is "reasonable and appropriate" for the entity's environment, as it relates to protecting e-PHI. If the entity concludes that implementation is not reasonable, the Security Rule allows the covered entity or business associate to adopt an alternative measure that achieves the "Addressable" specification's purpose, provided that the alternative measure is reasonable and appropriate.[89] If the entity concludes that implementing the "Addressable" specification is not reasonable and appropriate, it must document "why it would not be reasonable and appropriate to implement the implementation specification" and implement an "equivalent alternative measure if reasonable and appropriate."[90] This is a prime example of the flexibility that the HIPAA regulations offer as it relates to the security of e-PHI.

In practice, this means that a covered entity or business associate has three options regarding addressable specifications: (a) implement the addressable specification; (b) implement an alternative security measures that accomplishes the same purpose; or (c) not implement the addressable implementation specification or an alternative. In conducting this assessment and determination, the covered entity or business associate must assess the relevant factors specific to that organization, including but not limited to its environment, security framework and needs, risk analysis, risk mitigation strategy and the cost of implementation.[91] An entity must implement those addressable implementation specifications that are

determined to be reasonable and appropriate based on its particular security framework. The entity's determination must be documented and this documentation should include the factors considered and the results of the risk assessment on which the determination was based.

Policies and Procedures and Documentation Requirements

Covered entities and business associates must to create and implement "reasonable and appropriate policies and procedures" to comply with the standards, implementation specifications, or other requirements of the Security Rule. These policies and procedures may be amended at any time, as long as the changes are documented and are implemented in accordance with the requirements. Written security policies and procedures and other documentation of required actions, activities or assessments must be kept until at least six years following their creation date or last effective date, whichever is later.[92] Covered entity and business associates are also required to periodically review and update this documentation, as needed, "in response to environmental or organizational changes affecting the security" of e-PHI.[93]

State Law

When it comes to matters of data confidentiality and security, it is critically important to compare federal standards like those created under HIPAA against applicable State law. The general rule is that any HIPAA standard or requirement that is "contrary" to State law will preempt the State law provision.[94] The term, "contrary" means that a covered entity or business associate would "find it impossible to comply" with both the State and federal requirements, or that the State law is an "obstacle to the accomplishment and execution" of the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[95]

---

[1] 45 C.F.R. § 160.103.
[2] 45 C.F.R. § 160.103.
[3] 45 C.F.R. § 160.103.
[4] 45 C.F.R. § 160.103.
[5] 45 C.F.R. §§ 164.308(b) and 164.502(e).
[6] 45 C.F.R. § 160.103; 78 Fed.Reg. 5571-5572.
[7] 45 C.F.R. § 164.504(e).
[8] 45 C.F.R. § 164.314(a)(2).
[9] 45 C.F.R. § 164.314(a)(2).
[10] 45 C.F.R. § 164.504(e)(2)(ii)(H).
[11] 45 C.F.R. § 164.314(a)(2)(i)(C).
[12] 45 C.F.R. § 164.504(e)(1).

[13] 45 C.F.R. § 160.402(c).
[14] 45 C.F.R. §§ 164.314(a)(2) and 164.504(e)(1).
[15] 45 C.F.R. § 160.103.
[16] 45 C.F.R. §§ 164.314(a)(2) and 164.504(e)(5).
[17] 45 C.F.R. § 164.502(b)(1).
[18] 45 C.F.R. § 160.103.
[19] 45 C.F.R. § 160.103.
[20] 20 U.S.C. § 1232g.
[21] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).
[22] 45 C.F.R. § 164.514(b)(2).
[23] 45 C.F.R. § 164.514(b)(2).
[24] 45 C.F.R. § 164.502(a).
[25] 45 C.F.R. § 164.502(a)(2).
[26] 45 C.F.R. § 164.502(a)(1).
[27] 45 C.F.R. §§ 164.506 and 164.522(a).
[28] 45 C.F.R. §§ 164.501 and 164.506.
[29] 45 C.F.R. § 164.510.
[30] 45 C.F.R. § 164.502(a)(1).
[31] 45 C.F.R. § 164.512.
[32] 45 C.F.R. § 164.512(a).
[33] 45 C.F.R. § 164.514(h).
[34] 45 C.F.R. § 164.502(b).
[35] 45 C.F.R. § 164.508.
[36] 45 C.F.R. 508(b)(4).
[37] 45 C.F.R. §§ 164.501 and 164.508(c).
[38] 45 C.F.R. §§ 164.501 and 164.508(a)(3).
[39] 45 C.F.R. §§ 164.502(b) and 164.514(d).
[40] 45 C.F.R. § 164.514(d).
[41] 45 C.F.R. § 164.520.
[42] 45 C.F.R. § 164.520(c).
[43] 45 C.F.R. § 164.520(c).
[44] 45 C.F.R. § 164.524.
[45] 45 C.F.R. § 164.501.
[46] 45 C.F.R. § 164.526.
[47] 45 C.F.R. §§ 164.526(c) and 164.526(d).
[48] 45 C.F.R. § 164.528(b).
[49] 45 C.F.R. § 164.528(a).
[50] 45 C.F.R. § 164.522(a).
[51] 45 C.F.R. § 164.522(b).
[52] 45 C.F.R. §§ 164.308(a)(2) and 164.530(a).
[53] 45 C.F.R. § 164.530(i).
[54] 45 C.F.R. § 164.530(c).

[55] 45 C.F.R. § 164.530(b).
[56] 45 C.F.R. § 160.103.
[57] 45 C.F.R. § 164.530(e).
[58] 45 C.F.R. § 164.530(f).
[59] 45 C.F.R. § 164.530(d).
[60] 45 C.F.R. § 164.530(g).
[61] 45 C.F.R. § 164.530(h).
[62] 45 C.F.R. § 160.103.
[63] 45 C.F.R. § 164.306(a).
[64] 45 C.F.R. § 164.304.
[65] 45 C.F.R. § 164.304.
[66] 45 C.F.R. § 164.306(b)(1).
[67] 45 C.F.R. § 164.306(b)(2).
[68] 45 C.F.R. § 164.306(e).
[69] 45 C.F.R. § 164.308(a)(1)(ii)(A).
[70] 45 C.F.R. § 164.306(a)(2).
[71] 45 C.F.R. § 164.306(b)(2)(iv).
[72] 45 C.F.R. § 164.308(a)(1)(ii)(B).
[73] 45 C.F.R. §§ 164.306(d)(3)(ii)(B)(1) and 164.316(b)(1).
[74] 45 C.F.R. § 164.308(a)(1)(ii)(D).
[75] 45 C.F.R. §§ 164.306(e) and 164.308(a)(8).
[76] 45 C.F.R. §§ 164.306(b)(2)(iv) and 164.306(e).
[77] 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.308(a)(1)(ii)(B).
[78] 45 C.F.R. § 164.308(a)(2).
[79] 45 C.F.R. § 164.308(a)(4)(i).
[80] 45 C.F.R. § 164.308(a)(5)(i).
[81] 45 C.F.R. § 164.308(a)(3) & (4).
[82] 45 C.F.R. § 164.308(a)(1)(ii)(C).
[83] 45 C.F.R. § 164.310(a).
[84] 45 C.F.R. §§ 164.310(b) and 164.310(c).
[85] 45 C.F.R. § 164.310(d).
[86] 45 C.F.R. § 164.312(a).
[87] 45 C.F.R. §§ 164.312(b) and 164.312(c).
[88] 45 C.F.R. § 164.312(e).
[89] 45 C.F.R. § 164.306(d).
[90] 45 C.F.R. § 164.306(d)(3).
[91] 45 C.F.R. §§ 164.306(b) and 164.306(d)(3).
[92] 45 C.F.R. § 164.316.
[93] 45 C.F.R. § 164.316(b)(2)(iii).
[94] 45 C.F.R. § 160.203.
[95] 45 C.F.R. § 160.202.