2015

It's Five O'Clock; Do You Know Where Your Records Are: Obligations of Individuals and Entities to Secure Protected Health Information

Brandon S. Kulwicki

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation
Brandon S. Kulwicki, It's Five O'Clock; Do You Know Where Your Records Are: Obligations of Individuals and Entities to Secure Protected Health Information, 18 SMU Sci. & Tech. L. Rev. 455 (2015)
https://scholar.smu.edu/scitech/vol18/iss4/5

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
It’s Five O’Clock; Do You Know Where Your Records Are? Obligations of Individuals and Entities to Secure Protected Health Information

Brandon S. Kulwicki*

I. INTRODUCTION

Federal laws and state laws limit the maintenance, access, and use of protected health information by health care providers. Some requirements focus on implementing security measures that safeguard the confidentiality of patient information. Patient information contains not only potentially embarrassing personal information, but also valuable, personal identifiable information. In the modern era of widely utilized technology, protecting the cyber security of patients’ health information is more crucial than ever. This article will introduce and discuss relevant provisions of the federal scheme—HIPAA, HITECH, and the Omnibus Rule—as well as Texas law. It will outline how these requirements affect the operations of Texas entities with access to protected health information, and how the requirements can ensure security for patients.

* Brandon Kulwicki is a shareholder at Hall, Render, Killian, Heath & Lyman in Dallas, Texas, where his practice is devoted to health care. Website: www.hallrender.com. He holds a Bachelor of Science from Texas A&M University and a Juris Doctorate from Southern Methodist University Dedman School of Law. Mr. Kulwicki would like to thank his associate, Christie Davis, for her enormous assistance in the preparation of this article. He would also like to thank his wife, Kylie, and daughter, Sutton, for their loving support and understanding during the preparation of this article.


II. BACKGROUND ON HIPAA, HITECH, AND THE OMNIBUS RULE

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996.4 HIPAA covers many facets of health care, from billing codes to privacy and security of health data.5 To strengthen HIPAA’s privacy and security requirements, the Health Information Technology for Economic and Clinical Health Act (HITECH) was codified in 2009.6 The federal trilogy was completed in 2013 with the introduction of the Omnibus Rule. The Omnibus Rule is the final rule promulgated by the Department of Health and Human Services (HHS) in an effort to close the remaining gaps in HITECH and HIPAA.7 HITECH and the Omnibus Rule were designed to strengthen both the standards for protection of health information and the penalties for HIPAA violations.8 HIPAA, HITECH, and the Omnibus Rule create requirements that aim to protect the security of patient health data and authorize the enforcement of privacy restrictions against health care providers who maintain such information.9 The salient points of both the federal and state schemes are discussed in this article so as to provide an understanding of compliance and protected information.

The regulations implementing HIPAA are composed of three key rules: the Privacy Rule,10 the Security Rule,11 and the Breach Notification Rule.12 These rules regulate the use and disclosure of “protected health information” (PHI), how such information should be protected, and what to do when the protection fails and confidential information is inappropriately used or disclosed.13 The Privacy Rule established standards “address[ing] the use and disclosure of individuals’ health information . . . as well as standards for

5. See generally id.
8. See generally § 13408, 123 Stat. at 115; id.
individuals' privacy rights to understand and control how their health information is used.'

The Privacy Rule "strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing." The Security Rule will be the primary focus of this article. The Security Rule "establish[es] a national set of security standards for protecting certain health information that is held or transferred in electronic form . . .[and] operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations . . . must put in place to secure individuals' electronic protected health information . . ." Finally, the Breach Notification Rule prescribes how organizations must "provide notification following a breach" of protected information.

In 2009, Congress enacted the HITECH Act as part of the American Recovery and Reinvestment Act. As with HIPAA, HHS subsequently released regulations to implement HITECH's provisions. These regulations primarily amend the civil monetary penalties associated with HIPAA violations. HITECH establishes four categories of violations based on culpability. Monetary penalties range from $100 to $50,000 per violation. HITECH also imposes a $1.5 million limit for all violations of the same provision that occur within the same calendar year. While the HITECH Act certainly created a monetary disincentive to violate HIPAA, HITECH did not introduce any substantive changes to HIPAA's use and disclosure requirements.

The final rule designed to address any remaining holes in HIPAA and HITECH was promulgated in 2013. The so-called "Omnibus Rule" was formulated, in part, to "strengthen the privacy and security protections" for health information. Required compliance with the Omnibus Rule for covered entities began in September 2013. Under the Omnibus Rule, HHS extended to "business associates" the requirements for maintaining the privacy and security of PHI. As a result, a covered entity is permitted to disclose PHI to a business associate and allows a business associate to create, receive, maintain, and transmit PHI on behalf of the covered entity.

15. Id.
19. See id.
20. See id. at 56,127.
21. Omnibus Rule, supra note 1, at 5566.
22. See id.
23. See id. at 5570.
revised the scope of the Privacy Rule by extending the prohibition against unpermitted use and disclosure of PHI to include both covered entities and business associates, thereby creating direct liability for business associate entities that violate HIPAA regulations.24 The requirements of the Security Rule also apply to business associates.25 These statutes and regulations employ a complex framework of defined terms, the most important of which are discussed below.

A. What is a “Covered Entity” under HIPAA?

Section 160.103 of HIPAA regulations defines a covered entity as “a health plan,” a “health care clearinghouse,” or “a health care provider.”26 A health plan includes group health plans, health insurance issuers, health maintenance organizations (HMO), Medicare, Medicaid, and employee welfare benefit plans, among other public health plans.27 A health care clearinghouse includes any entity which “processes or facilitates the processing of health information received from another entity” for standardization, such as billing services or community health management information systems.28 A health care provider includes the actual provider of health services, as well as “any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.”29 This includes institutional providers, such as hospitals, as well as non-institutional providers, such as physicians, dentists, and other practitioners.30 HIPPA also defines providers as those that “transmit any health information in electronic form.”31 However, with the increased use of electronic medical records and the requirement by payors to submit the majority of invoices electronically, most providers meet the definition of a covered entity.

B. What is a “Business Associate?”

A “business associate” is an individual or entity that (1) uses or discloses PHI on behalf of a covered entity, such as claims processing, data analysis, or billing; or (2) provides various services to a covered entity when the provision of such services involves the disclosure of PHI, either by the covered entity to the business associate or by the business associate to a third

24. See id. at 5696.
27. Id.
28. Id.
29. Id.
30. See Privacy Rule, supra note 10.
31. Id.
Legal services are among the services that, if provided to a covered entity, may result in business associate status. Therefore, to the extent that a law firm provides legal services to a HIPAA covered entity, which involves the use or disclosure of PHI, the law firm becomes a business associate under the statute. This is of critical importance because with the implementation of HITECH and the Omnibus Rule, business associates are now directly liable for HIPAA’s Privacy and Security Rules violations.

C. What is “Protected Health Information?”

HIPAA protects all “individually identifiable health information . . . that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.” Protected health information (PHI) excludes certain records, including education and employment records. “Individually identifiable health information” includes all “information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and
   a. That identifies the individual, or
   b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

There are not, however, restrictions on the use or disclosure of “de-identified” health information, which is information that “neither identifies nor provides a reasonable basis to identify an individual.” PHI may be unidentifiable either through formal determination by a qualified statistician, or through the removal of specified identifiers of the individual and the individual’s relatives, household members, and employers.

32. 45 C.F.R. § 160.103.
33. See id.
34. See id.
35. Id.
36. Id.
37. Id.
38. See Privacy Rule, supra note 10.
39. Id.
III. BACKGROUND ON TEXAS HOUSE BILL 300

In 2011, the Texas legislature passed House Bill 300 in an effort to strengthen the privacy and security protections of health information amidst concerns that HIPAA did not sufficiently protect health records, particularly given the increased electronic exchange of health information.40 House Bill 300 amends Texas' existing medical record privacy provisions to bolster the federal scheme. Because HIPAA preempts state law except where state law is more stringent, House Bill 300 created stricter health information privacy standards in Texas.41 Of particular importance is the applicability of the medical records privacy provisions amended by House Bill 300. Although HIPAA, HITECH and the Omnibus Rule are applicable only to health care providers, health plans, and health care clearinghouses (as well as any business associates of these covered entities), Texas has taken the protection of health information a step further through a dramatic expansion of the scope of the term “covered entity.”42

Under House Bill 300, an entity becomes a “covered entity” when it comes into possession of PHI.43 Under Texas’ definition, an entity does not need to be directly involved in the health care industry to be considered a covered entity.44 This broad definition drastically increases the number of individuals and entities that must comply with the protective requirements of Texas’ medical records privacy act, and includes any attorneys who come across PHI. Whether the information pertains to the attorney’s own client or is received from an opposing party, any information that qualifies as PHI must be protected in compliance with Texas’ heightened protections.45 This expansive definition of a “covered entity,” raises questions as to what individuals and entities not traditionally associated with the health care field, including law firms, must do to comply with the Texas medical records privacy statute.

A. Texas Definition of “Covered Entities”

House Bill 300 implements a significantly broader definition of “covered entities” than the federal regulations. A covered entity includes any person or entity that:

(1) Engages in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI;

42. See 45 C.F.R. § 160.103.
43. See id.
45. See 45 C.F.R. § 160.203(b).
Securing Protected Health Information

(2) Comes into possession of PHI;  
(3) Obtains or stores PHI; or  
(4) Is an employee, agent, or contractor of a person described in  
(a)–(c) above.46

The statute further states that the term includes business associates, health care payers, governmental units, information or computer management entities, schools, health researchers, health care facilities, clinics, health care providers, or any person who maintains an Internet site.47 This expanded definition means that any individual or entity in possession of medical records will be subject to a penalty for the prohibited use or release of PHI.48 Given the sweeping scope of this definition, law firms and attorneys that are able to obtain their client’s health records during discovery will be considered covered entities, and therefore are subject to the privacy and security standards of House Bill 300.49

B. Required Employee Training

House Bill 300 also requires that all covered entities “provide training to employees of the covered entity regarding the state and federal law concerning [PHI] as necessary and appropriate for the employees to carry out the employees’ duties for the covered entity.”50 This training should be tailored to address the aspects of federal and state confidentiality laws that apply to each employee’s scope of work within the covered entity.51 Each employee must complete medical record privacy training within the first ninety (90) days of his or her date of hire.52 Further, employee training must be updated in the event that “the duties of an employee . . . are affected by a material change in state or federal law concerning [PHI].”53 such additional training must occur no later than the first anniversary of the date the material change in law takes effect.54

In order to evidence compliance with the statute, a covered entity must require each of its employees who completes the training program to “sign, electronically or in writing, a statement verifying the employee’s completion of the training.”55 House Bill 300 further states that the covered entity must

46. HEALTH & SAFETY § 181.001(b)(2).
47. Id.
48. See id.
49. See id.
50. See id. § 181.101(a).
51. See id.
52. See TEX. HEALTH & SAFETY CODE ANN. § 181.101(b) (West 2015).
53. Id. § 181.101(c).
54. Id.
55. Id. § 181.101(d).
C. State-Level Laws and Rules

As Texas has implemented its own framework of statutes and regulations to strengthen the protection of medical records and PHI, a majority of states have enacted legislation to protect the privacy of such information. While this article discusses only Texas' legislative protections of confidential health information, all local statutes and regulations should be reviewed prior to the use or disclosure of medical records or PHI.

IV. THE HIPAA SECURITY RULE

The HIPAA Security Rule sets forth numerous safeguards to ensure all electronic PHI handled by a covered entity or business associate remains safe and available. The Texas statute does not specifically describe appropriate security measures; instead, it refers back to the federal rules. Therefore, by implication, a Texas covered entity would likely be required to comply with these provisions as well.

A. In General

The HIPAA Security Rule requires covered entities and business associates to:

(1) Ensure the confidentiality, integrity, and availability of all electronic [PHI] 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; and
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [HIPAA].

56. See id.
57. See Lawrence O. Gostin, Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/medical/cdc_survey.html (last visited May 12, 2016) ("Thirty-seven states impose on physicians the duty to maintain the confidentiality of medical records. Twenty-six extend this duty to other health care providers. Thirty-three states and territories require health care institutions to maintain the confidentiality of medical records they hold.").
58. See 45 C.F.R. §164.306(a)(1)–(3).
59. See TEX. HEALTH & SAFETY CODE ANN. § 181.004 (West 2015).
60. 45 C.F.R. § 164.306(a)(1)–(3).
The HIPAA Security Rule identifies three types of safeguards to be implemented: administrative, physical, and technical. Each safeguard will be discussed in turn.

Within each category, the Security Rule sets forth "implementation specifications." Implementation specifications are designated as either "required" or "addressable." As these terms suggest, covered entities and business associates must execute their required implementation specifications. With respect to addressable implementation specifications, a covered entity or business associate must determine whether the specification is a "reasonable and appropriate safeguard in its environment," when compared with the likelihood the specification will contribute to protecting PHI. If reasonable and appropriate to implement, the covered entity or business associate must follow the addressable implementation specification. If the entity determines that the addressable implementation specification is not reasonable and appropriate, the covered entity or business associate must record the reasons for such a determination and put in effect "an equivalent alternative measure if reasonable and appropriate." The covered entity or business associate should periodically review and, as needed, modify its security measures to ensure continued compliance with the implementation specifications of the Security Rule.

Within these parameters, a certain amount of flexibility is provided to covered entities and business associates to determining the specific methods that satisfy their general requirements. When deciding what security measures are most appropriate, each covered entity or business associate should consider factors such as: the size and complexity of the covered entity or business associate; the covered entity or business associate's technical infrastructure and hardware/software security capabilities; the cost of security measures; and the probability and severity of potential risks to electronic PHI.

61. See id. § 164.308.
62. See id. § 164.310.
63. See id. § 164.312.
64. 45 C.F.R. § 160.103 (2016).
66. See id. § 164.306(d)(2).
67. Id. § 164.306(d)(3)(i).
69. Id. § 164.306(d)(3)(ii)(B)(1)–(2).
70. See id. § 164.306(e).
72. Id. § 164.306(b)(2)(i)–(iv).
B. Administrative Safeguards

Section 164.308 addresses the administrative standards for securing PHI. There are nine administrative standards that seek to protect confidential health information: (1) security management process; (2) assigned security responsibility; (3) workforce security; (4) information access management; (5) security awareness and training; (6) security incident procedures; (7) contingency plan; (8) evaluation; and (9) business associate agreements.

i. Security Management Process

The first standard requires policies be implemented to “prevent, detect, contain, and correct security violations.” All of the implementation specifications for this standard are required, which include:

(1) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI.
(2) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
(3) Apply appropriate sanctions against staff and personnel who fail to comply with the covered entity’s or business associate’s security policies and procedures.
(4) Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

73. See id. § 164.308(a)–(b).
74. Id. § 164.308(a)(1).
75. Id. § 164.308(a)(2).
76. Id. § 164.308(a)(3).
77. 45 C.F.R. § 164.308(a)(4) (2016).
78. Id. § 164.308(a)(5).
79. Id. § 164.308(a)(6).
80. Id. § 164.308(a)(7).
81. Id. § 164.308(a)(8).
82. Id. § 164.308(b)(1).
84. Id. § 164.308(a)(1)(ii)(A)–(D).
ii. Assigned Security Responsibility

The second mandatory standard requires that covered entities and business associates designate a security official. The security official is “responsible for the development and implementation of the security policies and procedures” that the entity must have in place.

iii. Workforce Security

The third administrative safeguard entrusts covered entities and business associates with ensuring that only appropriate members of its workforce have access to electronic PHI. Unlike the standards discussed, these implementation specifications are addressable, not required, and include implementing procedures:

(1) For the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed;
(2) To determine that the access of a workforce member to electronic PHI is appropriate [via workforce clearance procedures; and]
(3) For terminating access to electronic PHI when the employment of, or other arrangement with, a workforce member ends.

iv. Information Access Management

The fourth standard regulates the process of providing access to electronic PHI. The required implementation specification requires that health care clearinghouses “implement policies and procedures that protect electronic PHI from unauthorized access if the clearinghouse is part of a larger organization.” There are two additional implementation specifications, both of which are addressable and not mandatory. The first specification encourages entities to implement policies and procedures for accessing to electronic PHI “for example, through access to a workstation, transaction, program, process, or other mechanism.” The second specification encourages the establishment, documentation, review, and modification of a user’s right to ac-

85. See id. § 164.308(a)(2).
86. Id. § 164.308(a)(2).
87. See id. § 164.308(a)(3)(i).
88. Id. § 164.308(a)(3)(ii)(A)–(C).
90. Id. § 164.308(a)(4)(ii)(A).
91. See id. § 164.308(a)(4)(ii)(B)–(C).
92. Id. § 164.308(a)(4)(ii)(B).
cess “a workstation, transaction, program, or process” based upon the access authorization policies of the covered entity or business associate.93

v. Security Awareness and Training

The fifth administrative safeguard under the HIPAA Security Rule requires a covered entity or business associate to implement a security awareness and training program for all employees, including management.94 The addressable implementation specifications include periodic security update reminders, procedures for guarding against detecting and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords.95

vi. Security Incident Procedures

The sixth administrative standard focuses on policies and procedures for addressing security incidents, and requires that covered entities and business associates identify and respond to any suspected or known security incidents by mitigating the harmful effects of such incidents to the extent possible.96 All such security incidents and their outcomes should be documented.97

vii. Contingency Plan

In the event of an emergency that damages systems containing electronic PHI, such as fire, vandalism, system failure, or natural disaster, the covered entity or business associate must have established policies and procedures that respond to such emergencies.98 The required implementation specifications for contingency plans include establishing and, as needed, implementing procedures:

(a) To create and maintain retrievable exact copies of the electronic PHI;
(b) To restore any lost data; and
(c) To enable continuation of critical business processes for protection of the security electronic PHI while operating in emergency mode.99

In addition, addressable implementation specifications for this administrative standard include discussing the implementation of procedures for periodic testing of the contingency plan, and assessing the relative criticality of

93. Id. § 164.308(a)(4)(ii)(C).
94. 45 C.F.R. § 164.308(a)(5)(i).
95. Id. § 164.308(a)(5)(ii)(A)–(D).
96. 45 C.F.R. § 164.308(a)(6)(ii).
97. Id.
98. Id. § 164.308(a)(7)(i).
99. Id. § 164.308(a)(7)(ii)(A)–(C).
specific applications and data in support of other contingency plan components.100

viii. Evaluation

Periodically, covered entities and business associates must perform technical and nontechnical evaluations of the administrative safeguard standards described above, and they must also respond to environmental or operational changes affecting the security of electronic PHI.101

ix. Business Associate Agreements

As described above, a business associate is an individual or entity that handles PHI on behalf of a covered entity. In order to comply with the HIPAA Security Rule, a covered entity may provide electronic PHI to a business associate only upon receiving satisfactory assurances that the business associate will “appropriately safeguard” the information.102 Similarly, if a business associate allows its subcontractor to create, receive, maintain, or transmit electronic PHI, it must first obtain such satisfactory assurances.103 These assurances must be documented in a written agreement between the two parties.104 Additional information regarding business associate agreements (BAAs) is discussed with organizational standards hereunder.

C. Physical Safeguards

In addition to administrative safeguards, the HIPAA Security Rule addresses physical protections for electronic PHI.105 These standards limit the physical access to confidential information through workstations and other devices.106

i. Facility Access Controls

Covered entities and business associates must restrict access to electronic PHI at any facility that houses PHI information.107 Addressable implementation standards include the following:

100. Id. § 164.308(a)(7)(ii)(D)–(E).
101. Id. § 164.308(a)(8).
103. Id. § 164.308(b)(2).
104. Id. § 164.308(b)(3).
105. 45 C.F.R. § 164.310.
106. Id.
107. Id. § 164.310(a)(1).
(a) Establishing and implementing (as necessary) procedures that allow facility access in support of restoration of lost data under the disaster recovery and emergency mode operations plans;108
(b) Implementing policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft;109
(c) Implementing procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control access to software programs for testing and revision;110 and
(d) Implementing policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).111

ii. Workstation Use

Beyond generally securing the facility in which electronic PHI is stored, the HIPAA Security Rule requires policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation that can access electronic PHI.112

iii. Workstation Security

In addition to restricting the use of workstations with access to electronic PHI, covered entities and business associates are required to put in place physical safeguards to restrict access to authorized users.113

iv. Device and Media Controls

All hardware and electronic media with access to electronic PHI must be secured, including the receipt and removal of such items and the movement of these items within the facility.114 The required implementation specifications mandate that policies and procedures be established to address the final disposition of electronic PHI, and the hardware and electronic media on which it is stored.115 These required implementation specifications also pro-

108. Id. § 164.310(a)(2)(i).
109. Id. § 164.310(a)(2)(ii).
110. Id. § 164.310(a)(2)(iii).
111. 45 C.F.R. § 164.310(a)(2)(iv).
112. Id. § 164.310(b).
113. Id. § 164.310(c) (2016).
114. Id. § 164.310(d)(1).
115. Id. § 164.310(d)(2)(i)–(ii).
vide procedures for removing electronic PHI from hardware and electronic media before the media is made available for re-use. Further addressable specifications include maintaining records of the movements of hardware and electronic media (as well as the person(s) responsible for such items) and creating exact copies of the electronic PHI stored thereon before movement of equipment in the event that such information should need to be retrieved.

D. Technical Safeguards

Finally, the HIPAA Security Rule addresses technical safeguards that restrict access to only those who “have been granted access rights,” as well as ensuring no unauthorized access or improper transmittal of electronic PHI occurs.

i. Access Controls

To ensure the security of electronic PHI, the covered entity or business associate must be able to limit access “[to only] those persons or software programs that have been granted access rights.” Specifications requiring implementation include “[a]ssign[ing] a unique name and/or number for identifying and tracking user identity,” and “[e]stablish[ing] procedures for obtaining necessary electronic [PHI] during an emergency.” Automatic logoff procedures and encryption are addressable implementation specifications. Despite being labeled an addressable specification, encryption, a topic discussed in detail herein, is an extremely important and highly recommended technique.

ii. Audit Controls

This technical standard requires the implementation of “hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic [PHI].”

116. Id.
117. 45 C.F.R. § 164.310(d)(2)(iii)–(iv).
119. Id. § 164.312(a)(1).
120. Id. § 164.312(a)(2)(i)–(ii).
121. Id. § 164.312(a)(2)(iii)–(iv).
122. Id. § 164.312(a)(2)(iv).
123. Id. § 164.312(b).
iii. Integrity

Another technical safeguard is the protection of electronic PHI from "improper alteration or destruction."\textsuperscript{124} The HIPAA Security Rule includes a single addressable specification describing the implementation of electronic mechanisms to authenticate electronic PHI in order to ensure that "information has not been altered or destroyed in an unauthorized manner."\textsuperscript{125}

iv. Individual and Entity Authentication

In addition to tracking the user name or other electronic identifier, covered entities and business associates must also "implement procedures to verify that [the individual] seeking access" is who he or she claims to be.\textsuperscript{126}

v. Transmission Security

Finally, precautions must be taken to ensure that electronic PHI is protected while being transferred over electronic communication networks.\textsuperscript{127} Addressable implementation specifications include implementing integrity controls and encryption.\textsuperscript{128}

E. Organizational Requirements

The HIPAA Security Rule includes certain organizational requirements related to specific operational relationships.

i. Business Associate Agreements

As discussed above, the administrative safeguards require that when a covered entity provides PHI to a business associate, the two parties must enter into a written agreement giving "satisfactory assurances" by stipulating that the business associate will "appropriately safeguard the [protected] information."\textsuperscript{129} The organizational requirements of the HIPAA Security Rule further enumerate certain required elements of such business associate agreements (BAAs).\textsuperscript{130} A BAA must state "that the business associate will:\textsuperscript{131}

(a) Comply with the applicable requirements of the HIPAA Security Rule;\textsuperscript{132}

\textsuperscript{124} 45 C.F.R. § 164.312(c)(1) (2016).
\textsuperscript{125} Id. § 164.312(c)(2).
\textsuperscript{126} Id. § 164.312(d).
\textsuperscript{127} Id. § 164.312(e)(1).
\textsuperscript{128} Id. § 164.312(e)(2)(i)–(ii).
\textsuperscript{129} FTC Security and Privacy, 45 C.F.R. § 164.308(b)(1), (3) (2013).
\textsuperscript{130} Id. § 164.314(a)(1) (2013).
\textsuperscript{131} Id. § 164.314(a)(2)(i).
\textsuperscript{132} Id. § 164.314(a)(2)(i)(A).
(b) Ensure that any subcontractors utilized by the business associate "that create, receive, maintain, or transmit electronic [PHI] on behalf of the business associate agree to comply with the applicable requirements of" the HIPAA Security Rule via a written agreement between the business associate and such subcontractor;\(^\mathrm{133}\) and

(c) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured [PHI].\(^\mathrm{134}\)

Similarly, these required implementation specifications will be applicable to any agreement or arrangement entered into by the business associate with a subcontractor.\(^\mathrm{135}\) While a written agreement is not strictly required by the HIPAA Security Rule, which provides that a BAA is not required if the covered entity "has another arrangement in place" with the business associate, it is highly advisable to document compliance with the requirements of this provision via a written agreement between the parties.\(^\mathrm{136}\)

\textit{ii. Requirements Specific to Group Health Plans}

Generally, a group health plan is required to "ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic [PHI] created, received, maintained, or transmitted to or by the plan sponsor on behalf of the [ ] plan."\(^\mathrm{137}\) The required implementation specifications mandate that the plan documents "incorporate provisions to require the plan sponsor to:"\(^\mathrm{138}\)

\begin{itemize}
  \item (a) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic [PHI]" handled by the plan sponsor;\(^\mathrm{139}\)
  \item (b) Ensure that adequate separation [of the plan and the plan sponsor] is supported by reasonable and appropriate security measures;\(^\mathrm{140}\)
  \item (c) Ensure that any agent to whom it provides information agrees to implement reasonable and appropriate security measures to protect the information;\(^\mathrm{141}\)
\end{itemize}

\(^{133}\) \textit{Id.} § 164.314(a)(2)(i)(B).

\(^{134}\) \textit{Id.} § 164.314(a)(2)(i)(C).

\(^{135}\) \textit{Id.} § 164.314(a)(2)(ii). (C.

\(^{136}\) \textit{Id.} § 164.314(a)(2)(iii).


\(^{138}\) \textit{Id.} § 164.314(b)(1).

\(^{139}\) \textit{Id.} § 164.314(b)(2).

\(^{140}\) \textit{Id.} at § 164.314(b)(2)(i).

\(^{141}\) \textit{Id.} § 164.314(b)(2)(ii).
(d) Report to the group health plan any security incident of which it becomes aware.\textsuperscript{142}

V. SUMMARY OF HIPAA’S PRIVACY RULE AND BREACH NOTIFICATION RULE

While this article is focused on the appropriate methods of securing electronic PHI, it is important to note that HIPAA also creates parameters for the use and disclosure of PHI. HIPAA also regulates the manner in which covered entities must notify customers if the security of their electronic PHI is breached.

A. HIPAA Privacy Rule

Designed to ensure the confidentiality of an individual’s PHI, and probably the most oft-cited portion of HIPAA, the HIPAA Privacy Rule limits a covered entity or business associate’s ability to use or disclose PHI to third parties.\textsuperscript{143} A covered entity is permitted to use or disclose PHI only in the following circumstances:

(a) To the individual;
(b) For treatment, payment, or health care operations . . . ,
(c) Incident to the use or disclosure otherwise permitted or required by [the HIPAA Privacy Rule];
(d) Pursuant to and in compliance with a valid authorization under § 164.508;
(e) Pursuant to an agreement under, or otherwise permitted by, § 164.510; and
(f) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), or (g).\textsuperscript{144}

It is important to note that covered entities are entitled to charge reasonable, cost-based fees for the production of copies of PHI.\textsuperscript{145} Often, the amount to be charged for the production of such information is capped by state law.\textsuperscript{146} Further, HIPAA regulations require that a covered entity, when disclosing PHI, make reasonable efforts to limit the disclosed PHI to the minimum necessary to accomplish the intended purpose.\textsuperscript{147} However, such

\textsuperscript{142} 45 C.F.R. § 164.314(b)(2)(iv).
\textsuperscript{144} 45 C.F.R. § 164.502(a)(1) (2016) (emphasis added).
\textsuperscript{146} See 22 Tex. Admin. Code § 165.2.
\textsuperscript{147} See 45 C.F.R. § 164.502(b)(1).
limitation is not applicable to uses or disclosures made pursuant to a valid authorization.\textsuperscript{148}

B. Interaction of the HIPAA Privacy Rule and the HIPAA Security Rule

The HIPAA Privacy Rule also addresses the security of PHI through the requirement that covered entities put in place “appropriate administrative, technical, and physical safeguards to protect the privacy” of PHI.\textsuperscript{149} A covered entity must reasonably safeguard [PHI] from any intentional or unintentional use or disclosure that violates the standards, implementation specifications or other requirements of the HIPAA Privacy Rule and must “reasonably safeguard [PHI] to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.”\textsuperscript{150}

Importantly, the HIPAA Privacy Rule’s safeguard requirements encompass PHI in more mediums than the HIPAA Security Rule. While the HIPAA Security Rule is specific to electronic PHI, the HIPAA Privacy Rule “applies to all forms of patients’ [PHI], whether electronic, written, or oral.”\textsuperscript{151} However, the HIPAA Security Rule is far more detailed with respect to specific requirements, whereas the HIPAA Privacy Rule discusses only general safeguarding requirements.\textsuperscript{152}

C. HIPAA Breach Notification Rule

In the event of a breach of unsecured PHI, a covered entity is obligated to inform any individuals whose information was compromised, or may reasonably have been compromised, by the breach.\textsuperscript{153} A “breach” is defined as “the acquisition, access, use, or disclosure of [PHI] in a manner not permitted . . . which compromises the security or privacy of the [PHI].”\textsuperscript{154} The HIPAA Breach Notification Rule sets forth various requirements for such notices, including requirements for business associates who experience a breach.\textsuperscript{155} However, such notice requirements are not applicable if the PHI, which is improperly used or disclosed, is secured. Unsecured PHI is information that has not been “rendered unusable, unreadable, or indecipherable to unautho-

\footnotesize{148. Id. § 164.502(b)(2)(iii).}\
\footnotesize{149. Id. § 164.530(c)(1).}\
\footnotesize{150. Id. § 164.530(c)(2)(i)–(ii).}\
\footnotesize{152. Id. at 4–5.}\
\footnotesize{153. See 45 C.F.R. § 164.404(a)(1) (2016).}\
\footnotesize{154. Id. § 164.402.}\
\footnotesize{155. See id. §§ 164.404(b)–(d), 164.410.}
rized persons through the use of technology or methodology." § 164.402. As discussed further herein, the most common form of securing PHI is through the use of encryption. Because the improper use or disclosure of secured PHI is not subject to the HIPAA Breach Notification Rule requirements, electronically securing the PHI is extremely useful. As a result, although the HIPAA Security Rule does not require encryption, it is highly advisable to encrypt electronic PHI. Encryption of PHI is discussed in further detail below.

VI. PRACTICAL ADVICE FOR COMPLYING WITH THE HIPAA SECURITY RULE

HIPAA provides various administrative, physical, and technical standards. However, these standards have general descriptions, making daily implementation of the HIPAA Security Rule, as well as the rule itself, less than clear. The implementation specifications do not adequately describe the specific security measures needed for compliance with the HIPAA Security Rule. As such, covered entities and business associates are left to determine the appropriate security steps. This article provides a non-exhaustive set of practical tips for securing PHI in order to comply with the HIPAA Security Rule.

A. Encryption

One of the most beneficial security measures that a covered entity or business associate can take is encrypting electronic PHI. This security measure is crucial because the HIPAA Breach Notification Rule creates a safe harbor for unauthorized disclosures of encrypted PHI. While such a breach could result in severe monetary penalties, covered entities and business associates that encrypt their PHI, as described in the HIPAA Breach Notification Rule Summary, supra note 12 (setting forth "three exceptions to the definition of 'breach'").
Securing Protected Health Information Notification Rule, are relieved from liability.\textsuperscript{164} Therefore, while the HIPAA Security Rule does not require the encryption of electronic PHI, encrypting PHI stored electronically can be hugely beneficial if a breach should occur.

\textbf{i. What is Encryption?}

The HIPAA Security Rule defines encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."\textsuperscript{165} To be considered secured, the "confidential process or key," which would enable decryption of electronic information, must not be breached because the disclosure of both the encrypted PHI and the key would give the recipient full view of the PHI.\textsuperscript{166} Thus, HHS has suggested that "[t]o avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt."\textsuperscript{167} The confidential process or key should be safeguarded as closely as the PHI itself because a failure to prove that the process or key was confidential may negate the benefits of encryption.\textsuperscript{168}

\textbf{ii. Encryption Methods}

To better describe the encryption methods appropriate for protection of PHI, HHS released guidance that includes certain encryption processes that meet the HIPAA Security Rule standard.\textsuperscript{169} The National Institute of Standards and Technology (NIST) also released guidance for both data at rest and data in motion.\textsuperscript{170} It is important to ensure that PHI is encrypted across all devices, particularly portable devices like USB hard drives and CDs, as these

\textsuperscript{164} See 45 C.F.R. § 160.410 (2016) (setting forth the affirmative defenses to monetary penalties).
\textsuperscript{165} 45 C.F.R. § 164.304 (2016).
\textsuperscript{166} Guidance, supra note 161.
\textsuperscript{167} Id.
\textsuperscript{168} See id.
\textsuperscript{169} Id.
items are more likely to be lost or stolen.\textsuperscript{171} Similarly, data should be encrypted across all storage platforms, including computer drives, servers, and even PHI stored in the cloud.\textsuperscript{172} In the event that PHI is shared via email, encryption should be utilized to ensure the security of the sensitive information.\textsuperscript{173} Whichever encryption method is utilized, covered entities and business associates should maintain adequate and up-to-date records that detail the method used and the devices and information encrypted.\textsuperscript{174} Under the HIPAA Breach Notification Rule, the covered entity or business associate bears the burden of proving that its encryption standards are adequate and that a breach of unsecured data did not occur.\textsuperscript{175}

B. Disposal/Destruction

Improper disposal or destruction of paper and electronic files frequently leads to violations of PHI security.\textsuperscript{176} To protect confidential information, properly disposing of all files is critical because a failure “to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.”\textsuperscript{177} Proper removal of PHI from computers, cell phones, and other electronic devices is necessary to prevent the disclosure of protected information.\textsuperscript{178} Both the Office for Civil Rights (OCR), which investigates complaints of HIPAA violations,\textsuperscript{179} and HHS recommend adopting appropriate techniques for electronic media disposal.\textsuperscript{180} These techniques include “clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing

\textsuperscript{171}. See Guidance, supra note 161.
\textsuperscript{172}. See id.
\textsuperscript{173}. See id.
\textsuperscript{174}. See 45 C.F.R. § 164.414(b) (2016).
\textsuperscript{175}. Id.
\textsuperscript{177}. Id. (citing 45 C.F.R. § 164.530(c) (2015)).
\textsuperscript{178}. Id.
the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)." Further, these methods are appropriate for both destroying a device and preparing a device for reuse.

Computers and cell phones may be the most common devices that lead to HIPAA violations. However, all electronic equipment that can store PHI requires careful assessment. For example, in 2013, a health plan reached a $1.2 million settlement with HHS and OCR for a HIPAA breach resulting from the use of photocopiers leased by a third party. The photocopiers stored records of the copied documents, which the health plan did not properly erase before returning the copiers. From photocopiers to USB hard drives, all potential PHI storage devices must be appropriately "wiped . . . before [they are] recycled, thrown away or sent back to a leasing agent."

Paper records are also prone to inappropriate disposal. Covered entities "are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by any unauthorized person." In 2015, a pharmacy settled for $125,000 due to its disposal of PHI "in an unlocked, open container on [its] premises." HHS and OCR suggest shred-

---

181. Id.


184. *See, e.g., HHS settles with health plan in photocopier breach case, U.S. Dep’t Health & Hum. Servs.* (Aug. 14, 2013), https://wayback.archive-it.org/3926/20150618191048/http://www.hhs.gov/news/press/2013pres/08/20130814a.html (OCR Director Leon Rodriguez said, "HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals’ data, and have appropriate safeguards in place to protect to this information.").

185. Id.

186. Id.

187. Id. (setting forth the OCR Director’s statements about the matter).

188. PHI Disposal FAQ 1, supra note 176.

189. Id.

ding, burning, pulping, or pulverizing paper records that contain PHI. Each method will accomplish the desired result that “PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.” Once the PHI is deconstructed, the remnants may be discarded in publicly accessible trash containers.

Many businesses, including law firms, place confidential information in containers for destruction by a third party vendor. HHS and OCR allow such practices if the temporary container is secure and the vendor appropriately destroys the documents. For entities subject to HIPAA, these vendors qualify as business associates and, therefore, require a contract or other agreement. But, instead of destroying the paper records, covered entities may return them to the individuals whose PHI they contain.

C. Physical Controls

Many HIPAA violations result from the inadvertent disclosure of PHI, as opposed to malicious, intentional attacks. Despite their accidental nature, such inadvertent security breaches are no less costly; even small events, such as the theft of a portable USB hard drive, have led to settlements larger than $1.5 million with OCR. The covered entity must store paper medical records and small, easily-removed electronic devices containing PHI in locked filing cabinets or other facilities, restricting access only to those who need to review such records. Further, it is important to keep thorough records of what electronic devices contain or have access to PHI.

191. PHI Disposal FAQ 1, supra note 176.
192. Id.
193. PHI Disposal FAQ 2, supra note 180.
194. Id.
195. Id.
197. PHI Disposal FAQ 1, supra note 176.
200. See Incidental Uses and Disclosures, supra note 198.
201. See Alaska Settles, supra note 199.
Securing Protected Health Information

foregoing example, the stolen USB drive possibly contained PHI, but there lacked definitive proof. The burden of proof lies with the covered entity to demonstrate that a breach of information did not occur, so even the possibility of a disclosure of PHI could constitute a violation. Thus, covered entities can better prove that a breach of HIPAA did not occur by diligently maintaining and updating records on devices that have the capability to access electronic PHI.

D. Workforce Training

To comply effectively, the covered entity must impress on personnel the importance of compliance with all privacy and security measures relating to PHI. With this same motivation, the Texas legislature, through House Bill 300, implemented mandatory employee training. Texas requires that all employees of a Texas-covered-entity receive training for both federal and state health information confidentiality laws. Employers may specifically tailor the training to reflect each employee’s duties and access to PHI.

Beyond meeting the training requirements of House Bill 300, employees must also understand the extremely sensitive nature of the information being handled and the significance of their compliance with applicable laws and regulations. Inadvertent disclosures are usually seen in everyday activities, such as mailing letters, sending e-mails, and even oral conversations. Employers must ensure that all employees who access and utilize PHI, whether in paper or electronic format, act vigilantly in protecting the confidentiality of the information.

202. See id.
203. 45 C.F.R. § 164.414(b) (2009).
204. See Incidental Uses and Disclosures, supra note 198.
206. See id.
207. Id.
208. Id.
209. Id.
210. See Incidental Uses and Disclosures, supra note 198.
212. See Health & Safety § 181.101(a).
VII. CONCLUSION

An increasingly digital world constantly puts electronic PHI at risk.213 The federal trilogy of HIPAA,214 HITECH,215 and the Omnibus Rule,216 as well as Texas’ House Bill 300,217 created a complex set of requirements that work together to ensure health information remains private and protected.218 In particular, the HIPAA Security Rule establishes a variety of safeguards to protect electronic PHI from inappropriate and unauthorized use or disclosure.219 Thus, covered entities can better ensure the security of PHI, protecting not only the patient’s information but also safeguarding the covered entity from costly fines and penalties, by assessing the potential risks and implementing the necessary administrative, physical, and technical procedures.

218. See supra Part II.
219. See 45 C.F.R. §§ 164.308 (administrative safeguards); 164.310 (physical safeguards); 164.312 (technical safeguards).