BUSINESS ASSOCIATE COMPLIANCE
WITH HIPAA AND THE HITECH ACT

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations (the “Privacy Rule”, the “Breach Notification Rule” and the “Security Rule”) establish security and privacy standards to ensure the confidentiality and integrity of Protected Health Information (“PHI”). Their application to Business Associates is summarized below:

- The HIPAA standards apply to Covered Entities, such as health plans, health care clearinghouses, and certain health care providers. Under HIPAA and its implementing regulations, Covered Entities are required to enter into a Business Associate Agreement (“BAA”) that contractually imposes HIPAA privacy and security requirements on each subcontractor that provides certain services for or functions on behalf of Covered Entities that involve the use or disclosure of PHI. The terms of the BAA obligate the Business Associate to safeguard the PHI that it creates or receives under this agreement.

- In addition, the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) applies certain HIPAA security requirements and HITECH privacy provisions directly to Business Associates, enhances the enforcement of HIPAA, and adds provisions that require notification to individuals of any breaches of PHI. These and other changes were implemented in the Omnibus Final Rule, which was effective on September 23, 2013.

Exhibit A (HIPAA Compliance Roadmap and Checklist for Business Associates) explains the key requirements that the HITECH Act imposes on Business Associates and the actions that Business Associates must take to come into compliance with HIPAA. Below, is a brief description of the requirements for HIPAA compliance by Business Associates.

---


2 45 C.F.R. 164, Subparts A and C, D, and E.

3 The Privacy Rule protects all “individually identifiable health information” held or transmitted by a Covered Entity or its Business Associate in any form or media, whether electronic, paper, or oral, with exclusions for employment and educational records. The Privacy Rule calls this information “Protected Health Information.” 45 C.F.R. § 160.103.

4 45 C.F.R. §§ 164.314, 164.502(e), 164.504(e).

II. GUIDANCE ON COMPLYING WITH HIPAA SECURITY RULE

A key HIPAA requirement for Business Associates is compliance with the administrative, technical and physical security standards established by the Security Rule. The first step in HIPAA compliance is to conduct a risk assessment of your organization’s current security policies and procedures for protecting Electronic Protected Health Information (“ePHI”). A Business Associate may use internal staff to conduct such an assessment or may contract out of the conduct of a HIPAA risk assessment. The federal Office of the National Coordinator and the Office for Civil Rights have jointly issued a Security Risk Assessment Tool, which was intended for use by small providers; it can be accessed at http://www.healthit.gov/providers-professionals/security-risk-assessment. Also attached for your reference is an Office for Civil Rights publication, Guidance on Risk Analysis Requirements Under the HIPAA Security Rule and Risk Analysis and Risk Management guidance. Additionally, the National Institute of Standards and Technology (“NIST”) special publication 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule, provides useful technical information regarding assessment of compliance with the standards and implementation specifications of the Security Rule. See, in particular, Table 4 for references to the specific NIST standards that apply to the HIPAA security standards. In addition to completion of a risk assessment, a Business Associate must develop and implement a written HIPAA security plan, which addresses each of the standards and implementation specifications established in the Security Rule.

III. GUIDANCE ON COMPLYING WITH HIPAA PRIVACY AND BREACH NOTIFICATION RULES

A Covered Entity may not disclose PHI to a Business Associate unless it enters into a BAA that includes each requirement of 45 C.F.R. § 164.504(e). Section 164.502(e) of the Privacy Rule requires that PHI be appropriately safeguarded and establishes limits on access to, use, and disclosure of PHI by Business Associates. With respect to breach notification, a Business Associate must have procedures in place to investigate any suspected breaches of ePHI, to determine whether a reportable breach has occurred, and to notify the Covered Entity in a timely manner. In many cases, a Covered Entity will require Business Associates to cooperate with the Covered Entity with respect to the investigation of a breach, required notification of individuals and the Secretary of Health and Human Services, and mitigation of any resulting harm.

An additional requirement under the HIPAA Privacy Rule is that Business Associates impose the same conditions and restrictions to which they have agreed in their BAAs on any subcontractors who assist them in the performance of their Business Associate functions. Therefore, business associates must identify those subcontractors that create or receive ePHI to assist the organization in performing a Business Associate function or service and execute BAAs with these entities.
The terms of BAAs are critical because they govern the business associate’s liability for the costs associated with notification of individuals, mitigation of risks, and any civil actions associated with breaches of PHI.

Business associates should prepare policies and procedures that address, at minimum, breach investigation and notification obligations under the organization’s BAAs with Covered Entities in order to minimize the risk of violating these contracts and the HITECH Act. Business associates may also implement other policies that are relevant to the organization, but are not expressly required by HIPAA.

IV. CONCLUSION

In short, compliance with HIPAA and the HITECH Act requires development of a written HIPAA security plan, negotiation and execution of BAAs with Covered Entities and subcontractors, and development of procedures for compliance with the privacy obligations imposed through BAAs, such as breach notification.
APPENDIX A

HIPAA COMPLIANCE ROADMAP AND CHECKLIST FOR BUSINESS ASSOCIATES

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, marked a fundamental change in the federal government’s approach to ensuring compliance with the HIPAA privacy and security rules.\(^6\) Under the HITECH Act, the federal government, in an effort to strengthen HIPAA, enacted a rigorous enforcement strategy that includes stricter privacy and security standards, increased penalties for violations, and expanded federal and state enforcement authority, all of which are now directly applicable to Business Associates (“BAs’

The HITECH Act is being implemented by an omnibus final rule (“the Final Rule”) that was published in the of Federal Register on January 25, 2013, and will be enforced by the Office for Civil Rights of the U.S. Department of Health and Human Services on September 23, 2013.

In the past, BAs only had contractual liability under HIPAA. The HITECH Act changes BAs’ obligations and exposure under HIPAA from purely contractual to both contractual and statutory. This means that in addition to being liable to their covered entities (CEs) under their business associate agreements (BAAs), BAs will now be subject to many of the legal requirements set forth in the HIPAA privacy and security rules, including civil and criminal penalties. Further, the HITECH Act greatly expands the definition of BAs.

Foley’s Health Care Industry Team has designed this roadmap (Roadmap) to assist BAs in complying with the new HIPAA requirements imposed by the HITECH Act, as implemented by the Final Rule. This Roadmap highlights key provisions and outlines steps BAs should take to achieve HIPAA compliance. To further aid BAs in their compliance activities, a checklist (Checklist) is included at the end of this Roadmap. Although most of the provisions discussed below technically became effective on February 17, 2010 under the HITECH Act statute, the HHS has indicated in the Final Rule that it will not enforce compliance with most of the new requirements until 180 days after the effective date of the Final Rule, which is September 23, 2013 (the Compliance Date).

Who are BAs?

Prior to enactment of the HITECH Act, BAs were generally defined to include entities engaged in certain administrative activities or services for or on behalf of CEs which required access to protected health information (PHI), including claims

\(^6\) Throughout this document, the term “HIPAA” will be defined to include the provisions of the HITECH Act, unless otherwise specifically noted.
processing, billing, benefit management, utilization review, management services, and consulting services.

However, under HITECH, the definition of a BA has been expanded to include the following organizations:

- Organizations providing PHI data transmission to CEs such as Health Information Organizations\(^7\) and E-prescribing gateways; and
- Vendors contracting with CEs to provide personal health record (PHR) systems to patients\(^8\) patient safety organizations.

The Final Rule further expands the definition of a BA to include subcontractors of BAs who perform functions or provide services to a BA which involves access to PHI other than in the capacity of a work force member (Subcontractors). To the extent that they meet this definition, downstream Subcontractors are also included.

This expanded definition of what constitutes a BA now subjects many previously non-covered organizations to the HIPAA requirements governing the privacy and security of medical or health information. This extends the requirements of HIPAA to a vast new class of vendors.

**What can happen to BAs that fail to comply with HIPAA?**

Like CEs, BAs will now be subject to complaint-driven investigations or random compliance audits by the Office for Civil Rights (OCR), the HHS agency responsible for monitoring and enforcing the HIPAA privacy and security rules. BAs found to be non-compliant and in violation of the law will be potentially subject to the following:

- Civil monetary penalties (CMPs) of between $100 and $50,000 per violation, with maximum penalties of $1.5 million per calendar year for violations of the same standard in any calendar year
- Criminal penalties

---

\(^7\) Organizations which are mere conduits of PHI and do not routinely access it are excluded from the definition of BA.

\(^8\) Vendors that provide PHR systems, but do not do so on behalf of CEs, will be subject to security breach notification under the HITECH Act, which will be enforced by the FTC, rather than HHS.
- A mandatory HHS investigation and assessment of CMPs in cases where a violation is found to be due to “willful neglect”
- Civil actions brought by state attorneys general for HIPAA violations that involve residents in their individual states

**Key HIPAA BA Requirements**

**What must BAs do under the new security breach notification requirements?**

Perhaps the most significant provision in HITECH is a new breach notification requirement which applies to both CEs and BAs. This requirement was implemented by an interim final rule (the Breach Notification Rule) published on August 24, 2009 and was modified by the Final Rule. Under this requirement, BAs must notify the CEs with whom they contract of any breaches of “unsecured PHI” and, to the extent possible, identify the affected individuals if the breach compromises the privacy or security of the information. Upon receiving notice of a reportable security breach, the CEs have the responsibility to notify the individuals whose information has been breached. CEs are also required to provide notice to HHS and, in some circumstances, to local media.

**How do the new security breach notification requirements change a BA’s obligations?**

BAs were initially obligated by their BAAs to notify their CEs of unauthorized uses or disclosures of PHI, as well as security incidents. The HITECH Act modified this requirement and requires BAs to notify CEs of any “security breach” of “unsecured PHI” discovered by the BAs. The HITECH Act defines “security breach” to include the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, with certain exceptions for the inadvertent acquisition, access, or use of PHI by employees and agents. BAs must notify their CEs of any breach that is determined to have more than a low probability of compromising the privacy or security of the information. To make this determination, BAs must conduct a four-factor risk analysis focusing on:

- the nature and extent of the PHI involved;
- the unauthorized person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired of viewed; and the extent to which the risk to the PHI has been mitigated.
What information is covered by the security breach notification requirement?

The breach notification requirement applies only to “unsecured PHI.” HHS has issued guidance (HHS Guidance) defining the technologies and methodologies to secure PHI, thus rendering the data unusable, unreadable, or indecipherable. Essentially, PHI must be either encrypted or destroyed as described in the HHS Guidance to be considered “secured.” If PHI is secured in accordance with the HHS Guidance, then unauthorized access to or use or disclosure of such information will not trigger the breach notification requirements. However, such breaches may still be subject to state law notification requirements as discussed below.

When must CEs and BAs provide notice?

CEs are required to notify patients “without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.” Similarly, BAs must notify their CEs without unreasonable delay and no later than 60 calendar days from discovery. BAs will bear the burden of proof of demonstrating that any delay in notifying the CEs of a security breach was reasonable. The date of “discovery” may not necessarily be the date of actual discovery, but rather, the date that one should have discovered the breach using reasonable diligence. Therefore, CEs and BAs should make sure reasonable measures are in place to detect potential security breaches as well as properly train employees to be able to spot potential breaches. BAs must timely report security breaches to CEs to enable them to notify the individuals within the foregoing deadline. However, HITECH does not preclude CEs from imposing shorter time limits on their BAs and it is likely that many CEs will amend their BAAs to do so in order to ensure that the CEs have sufficient time to meet their obligations.

What information is required in the notification?

BAs are required to include certain information about affected individuals in their reports to CEs to enable the CEs to properly notify affected individuals, HHS and, when required, the media. The notification should include a brief description of the incident, including the date of the breach and date it was discovered, and the type of unsecured PHI that was breached. CEs may require BAs to include additional information regarding the breach as CEs may need additional information to satisfy their notification requirements. In some circumstances, CEs may look to contractually obligate BAs who are involved in a security breach to make the required notifications on behalf of the CEs. In such cases, the BAs will need to ensure their notification is compliant with HIPAA requirements. Some CEs will require any BA which has caused a reportable breach to underwrite the cost of the required notifications and any mitigating steps that may be necessary.
How do the HIPAA security breach notification requirements affect BAs’ obligations under state security breach notification requirements?

HIPAA does not preempt more stringent state laws. Essentially, this means that BAs who are subject to state security breach notification laws will continue to be required to comply with those laws. BAs should consult with legal counsel for assistance with defining these obligations and conducting any necessary preemption analysis.

What should BAs do to comply with the HIPAA security breach notification requirements?

BAs should develop policies and procedures to ensure a coordinated system for internal detection and reporting of breaches of unsecured PHI, prompt internal investigation of alleged breaches, and reporting to the CEs with whom they contract. Please see the Checklist below for further guidance on compliance with the security breach notification requirements.

What if BAs use Subcontractors to provide services requiring access to PHI?

BAs that use Subcontractors must ensure that they contractually bind their Subcontractors to report security breaches in sufficient time to allow the BAs to report back to the CEs. BAs must also contractually bind their Subcontractors to all additional terms required of BAs by HIPAA, since the Subcontractors themselves are now deemed BAs. This includes, but is not limited to, requiring Subcontractors to develop similar policies, procedures, and processes for investigating and reporting breaches.

HIPAA Security Rule: What must BAs do to comply with the HIPAA security rule?

Pursuant to the HITECH Act, BAs (including Subcontractors) must also be in full compliance with the HIPAA Security Rule standards and implementation specifications for administrative, physical, and technical safeguards. Compliance with the Security Rule means that many BAs will need to do more than they have previously done in terms of securing electronic PHI. Even though BAs have been contractually required under HIPAA prior to HITECH to implement appropriate “administrative, physical and technical safeguards” to protect electronic PHI, the measures, policies, and procedures that many BAs have had in place up to now may be insufficient for HIPAA compliance as of the Compliance Date (as noted above, September 23, 2013). The HIPAA Security Rule contains a series of very specific standards and implementation specifications. No later than the Compliance Date, BAs are required to comply with each of the specific standards and implementation specifications to the same extent as CEs.
What is the first step BAs should take to become compliant with the HIPAA security rule?

The first step in compliance is to understand the HIPAA Security Rule requirements and to conduct a “gap analysis” to identify the areas where the BA’s information security systems and programs fall short of meeting those requirements. To aid in this process, see the Checklist below.

If BAs use Subcontractors that will have access to the BAs’ electronic systems, including electronic PHI, what should the BAs do to protect themselves?

As noted above, Subcontractors are now included within the definition of BAs. This means that BAs are, in effect, required to enter into a BAA with their Subcontractors incorporating all of the requirements that the BAs themselves must satisfy. Without limiting the foregoing, BAs should ensure that contracts with Subcontractors contain appropriate language to address information security and protect BAs from costs and liabilities associated with Subcontractors’ security breaches or other violations of contract terms related to information security. BAs should consider development of an information security due diligence questionnaire to be provided to potential Subcontractors in order to evaluate their ability to protect PHI and other valuable data.

Direct Liability for Business Associate Agreement Terms: What else must BAs do to comply with other HIPAA requirements?

Under the HITECH Act, BAs will have direct statutory as well as contractual liability for violations of HIPAA or the terms of their BAAs. BAs should evaluate their current policies, procedures, and processes for assuring compliance with HIPAA to make sure they are robust and effective Training of personnel will be even more critical. Policies on employee sanctions for violations of HIPAA should be evaluated and strengthened.

Amendment to BAAs: What should BAs expect, and what proactive steps should they take?

The changes in BA’s responsibilities under the HITECH Act and the Final Rule will require amendments to existing BAAs. In the Final Rule, HHS indicated that CEs and BAs will have up to a year after the Compliance Date to amend their BAAs to conform to the new requirements. Nevertheless, some CEs and BAs may choose to implement amendments sooner rather than later. In addition, CEs and BAs may want to develop new templates to use in contracting with any new BAs or Subcontractors.

What new terms should BAs expect to find CEs inserting into BAAs?

With the increased public exposure that may result from breaches of unsecured PHI and the implications for their businesses, many CEs will likely seek to renegotiate
some of the key terms. Responsibility for costs associated with security breaches and risk mitigation strategies in the event of a security breach are likely to be key issues in BAAs. CEs will likely press for broad indemnification from BAs. Certain CEs may require BAs who are the subject of a security breach, to make the required notifications on behalf of the CEs and/or to be responsible for all costs associated with a security breach.

**What can BAs do to proactively address the required amendment to BAAs?**

BAs should consider drafting their own form amendments and should create or revise their existing template BAAs to incorporate the changes required under the HITECH Act and the Final Rule. This may help BAs avoid more onerous terms inserted by CEs in their template documents.

**What should BAs do about existing subcontracts with Subcontractors who now meet the definition of Business Associates?**

These agreements should be amended to reflect the new applicable obligations of the BAs, and to address the fact that the Subcontractors themselves are now deemed BAs. BAs should insert appropriate language to address information security and protect the BAs from costs and liabilities associated with Subcontractors’ security breaches or other violations of contract terms related to information security. The agreement between the BA and the Subcontractor will need to flow through the contractual requirements established in the BAA between the CE and the BA. HHS makes it clear in the Final Rule that the BAAs between first-tier or upstream BAs and their downstream Subcontractors must be at least as stringent as the PAA between the CE and the first-tier BA.

**Other new HIPAA requirements: what other new HIPAA requirements will now be applicable to BAs?**

Pursuant to the HITECH Act, both BAs and their CEs will be required to comply with a series of additional HIPAA privacy requirements, including changes to the rules governing prohibition on sale of PHI, and new conditions on marketing communications. These requirements are addressed in the Final Rule. As noted above, HHS has indicated that it will not enforce these requirements until the Compliance Date.

**CHECKLIST FOR BUSINESS ASSOCIATES**

To assist BAs in complying with the changes to HIPAA under the HITECH Act and the Final Rule, we have created the Checklist below. This document is intended to provide general, high-level guidance only and is not intended to provide or be a
substitute for legal advice. BAs should consult legal counsel to fully understand their obligations under HIPAA and the HITECH Act.

The following Checklist highlights key provisions in the HITECH Act and the Final Rule that apply to BAs and provides a high-level outline of some important steps to aid a BA to achieve HIPAA compliance.

Compliance with the HIPAA breach notification requirements

In the Final Rule, HHS substantially modified the Breach Reporting requirements which have been in effect since 2009; however, the obligations imposed by these modifications will not be enforced until the Compliance Date. BAs should take the following steps to bring their organizations into compliance on that date.

- Review and modify existing policies and procedures to assure that they comply with the security breach notification requirements as modified by the Final Rule.

- Determine whether the organization is also subject to state breach notification requirements. If so, assess state law preemption and compliance issues as they relate to the HIPAA security breach notification requirements.

- Develop or refine security breach notification procedures to ensure that a centralized, coordinated security breach reporting system is in place. Consider the following:
  - The procedures should designate the individual responsible for ensuring that breaches involving PHI are investigated fully. The procedures should also indicate who has the ultimate decision-making authority for determining whether there has been a reportable breach. Procedures should provide for consultation with the organization’s legal counsel as necessary.

  - The procedures should ensure that breaches are reported to the CEs without unreasonable delay and in time to meet the deadlines specified in the organization’s BAAs. The procedures must ensure that individuals whose information has been compromised are appropriately identified, if possible, and reported to the CEs.

  - The procedures should require that employees be trained on the reporting procedures and the requirements for handling PHI.
• The procedures should include appropriate sanctions for employees who mishandle PHI.

• Evaluate the PHI that the BA’s organization controls and determine whether that PHI can be encrypted or destroyed so that it will be considered “secured” and not subject to the HIPAA security breach notification requirements.

• Consider risk prevention and mitigation strategies for security breaches.

• Consider how the organization can enhance its security system to decrease the risk of breach of unsecured PHI.

• Evaluate the organization’s insurance coverage to determine if it covers costs associated with security breaches of PHI.

Compliance with the HIPAA Security Rule

BAs should take the following steps to assure compliance with the HIPAA security rule:

• Conduct an organizational risk analysis to identify whether the HIPAA security standards and implementation requirements are met. An audit tool should be used to assist with the initial risk assessment or “gap analysis.”

• The gap analysis should address each of the following implementation standards:

  • **Administrative safeguards:** HIPAA requires that BAs have certain administrative safeguards, including the following: (i) a security management process, (ii) an individual with assigned security responsibility, (iii) appropriate workforce security policies and procedures, (iv) policies and procedures for information access management, (v) a program of security awareness and training, (vi) security incident procedures, (vii) a contingency plan, and (viii) periodic evaluations of compliance with the HIPAA Security Rule. The Security Rule also requires appointment of a security officer.

  • **Physical safeguards:** HIPAA requires that BAs have certain physical safeguards, including: (i) implementation and maintenance of policies and procedures on facility access
controls, (ii) policies and procedures on workstation use, workstation security, and (iii) device and media controls.

- **Technical safeguards:** HIPAA requires that BAs implement certain technical safeguards, including: (i) access controls, (ii) audit controls, (iii) integrity policies, (iv) person or entity authentication procedures, and (v) transmission security procedures for PHI.

- Develop written policies and procedures for each HIPAA standard listed above. **Please note that each of the implementation standards above has numerous requirements.** HIPAA requires that written policies and procedures be created that address each standard and each of the specific implementation specifications in the HIPAA Security Rule. These written policies and procedures are subject to record retention requirements of six years.

- Obtain review of policies and procedures to ensure legal compliance.

- Train staff on HIPAA privacy and security rule requirements and the consequences of violation.

**Amendment of BAAs**

Amend BAAs to incorporate applicable changes to HIPAA under the Final Rule. BAs should consider the following:

- Draft template amendments and revise (or create) new template BAAs to incorporate the changes required under the Final Rule. Proactively provide such templates to CEs.

- Be prepared for increasing complexity in negotiating BAAs with CEs, including the following:
  - CEs may conduct due diligence prior to contracting to determine whether BAs are HIPAA-compliant and whether a BA’s security profile provides sufficient protection for PHI.
  - CEs may attempt to negotiate broad indemnification or cost allocation provisions with their BAs to cover the CEs’ exposure to costs associated with security breach notification requirements, potential reputational damage, and civil liability arising from BAs’ breaches of unsecured PHI.
Check underlying services agreements for provisions addressing data privacy, security, and confidentiality to identify terms that conflict with the BAAs or place additional obligations on the BA.

- Amend Subcontractor agreements to address new obligations that have been imposed on the BA and its Subcontractors under the Final Rule. Consider inserting appropriate language to address information security and to protect the BA from costs and liabilities associated with Subcontractors’ security breaches or other violations of contract terms related to information security.

**Inventory HIPAA-related policies**

BAs are directly liable under HIPAA for violations of the Privacy, Security and Breach Notification Rules. BAs should consider the following:

- Evaluate current policies, procedures, and processes applicable to compliance with these rules to ensure they are robust and will facilitate compliance.

- Evaluate training procedures for personnel. Review and strengthen policies on employee sanctions for violations of HIPAA, the HITECH Act, or requirements in BAAs.

- Appoint security officer.