



# HIPAA CONSIDERATIONS FOR ANATOMIC PATHOLOGY INFORMATION SYSTEMS

PIVOT POINT SECURITY  
957 ROUTE 33  
SUITE 111  
HAMILTON SQUARE, NJ 08690  
PH: 609.890.1131  
FAX: 609.890.1136  
[WWW.PIVOTPOINTSECURITY.COM](http://WWW.PIVOTPOINTSECURITY.COM)

<b>OVERVIEW.....</b>	<b>3</b>
<b>CONTROL OBJECTIVES OF THE HIPAA SECURITY RULE .....</b>	<b>4</b>
<b>ENSURING AN ASP'S COMPLIANCE WITH THE HIPAA SECURITY RULE.....</b>	<b>5</b>
ASP Self-Assessment.....	5
Client Assessment of ASP.....	5
Third Party Attestation of ASP.....	6
Business Associate Contract Strategies Et Issues.....	7
Monitoring an ASP's HIPAA Compliance.....	8
<b>STRATEGIES FOR ASSESSING AN ASP'S HIPAA COMPLIANCE.....</b>	<b>9</b>
10 Questions to Rapidly Gauge ASP HIPAA Readiness.....	9
Sample ICQ for Specification Implementations.....	10
Workforce Security - 164.308(a)(3).....	10
Security Incident Procedures - 164.308(a)(6).....	11
<b>SUMMARY .....</b>	<b>13</b>

## Overview

HIPAA has significantly changed the requirements for the successful operation of a pathology laboratory and has necessitated the reconsideration of many operational elements of key processes including the handling of anatomic pathology data. One key consideration is determination of whether the optimal model for managing an anatomic pathology system is internal or external management.

In light of the new requirements of HIPAA a lab needs to consider whether the potential compliance complications associated with an ASP solution are fully off-set by its potential benefits (lower initial cost, off-site system hosting). Minimally, a laboratory considering an ASP solution should:

- Validate that the ASP has Third Party Attestation to support their HIPAA compliance.
- Develop a Comprehensive Business Associate Contract that details the lab's performance and control objectives. The contract needs to include On-going Monitoring and Termination Provisions.
- Monitor the ASP's compliance moving forward on no less than a quarterly basis. In the event that HIPAA deficiencies are noted, immediate corrective actions should be initiated. In the event that rapid mitigation is not possible, the contract should be immediately terminated and/or the deficiencies should be reported to the Department of Health and Human Services.

This paper introduces these considerations and provides an initial level of guidance to the lab in ensuring HIPAA compliance for an outsourced Anatomic Pathology System.

## Control Objectives of the HIPAA Security Rule

In order to ensure an ASP's compliance, a fundamental knowledge of the HIPAA Security Rule is required. The Final HIPAA Security rule ([www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp](http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp)). The core Control Objectives mandated by the rule require covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and
- Ensure compliance by its workforce.

Implicit in the rule is the obligation of the Covered Entity to ensure HIPAA Compliance for all Business Associates leveraged in their operations with whom EPHI is exchanged.

## Ensuring an ASP's Compliance with the HIPAA Security Rule

The question of "HIPAA compliance" is a crucial issue when considering an application services provider (ASP). An ASP in this situation would be the organization's "business partner," and a health care organization contracting with such an ASP would indeed need to ensure the ASP complied with HIPAA because it owns and operates the applications and host hardware which the health care organization uses to manage EPHI. *(On the other hand, an organization which buys a system/licenses software that it operates itself is not relying upon the vendor to manage protected information, and accordingly has no obligation to review its control environment for HIPAA Compliance).*

There are three elements to ensuring an ASP's compliance with the HIPAA Security Rule:

- Obtaining "Reasonable Assurance" that the ASP is fully compliant with the three key elements of the HIPAA Security Rule
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
- Implementing an appropriate Business Associate Contract
- Monitoring the ASP's Ongoing Compliance with the HIPAA Security Standard

There are numerous strategies, each with their own challenges to gaining reasonable assurance that an ASP is handling your EPHI in a HIPAA compliant manner. A few of these are outlined below:

### *ASP Self-Assessment*

The simplest means to obtain some level of assurance is to ask the ASP to provide formal documentation attesting to their compliance with HIPAA. While this will provide a basal level of assurance, especially if the documentation demonstrates extensive knowledge of HIPAA and its challenges, it is clearly not advisable. At the end of the day it ends up being, "because they told me so" which is not an answer that any lab director/owner wants to be explaining to the Centers for Medicare & Medicaid Services (CMS).

This mechanism may seem appropriate if the ASP is a large organization with many clients in the Pathology space. However, size and client base are not an indicator of control environment maturity. It is not uncommon, even in those organizations with high asset value systems and/or high risk data, and heavy regulatory compliance to find poorly designed controls and weak compliance.

### *Client Assessment of ASP*

The optimum mechanism to obtain a high level of assurance is for the lab (or a lab-contracted party) to conduct a HIPAA Assessment against the ASP themselves. Assuming the Lab

engaged Information System Auditors knowledgeable of HIPAA and their operations, the lab would be able to ascertain with a very high degree of certainty the HIPAA Compliance level of the ASP. Unfortunately this approach may not be practical from two perspectives:

- Dependent upon the size and complexity of the ASP and their HIPAA readiness this effort would likely range into tens of thousands of dollars. While this may be justifiable for a Hospital or larger lab, this may be impractical for a smaller lab.
- Dependent upon the ASP's number of clients, this approach could put an onerous burden on them if each client were to conduct its own audit.

This approach has another, oft overlooked advantage; the lab can audit the ASP's compliance to its control framework in addition to HIPAA. HIPAA is a least common denominator, it's a minimum standard enforced by CMS. There are many areas not addressed by HIPAA that a well-run lab will want to ensure its control framework addresses. For example, fundamental issues such as change management, and performance/capacity management are not mandated by HIPAA. *(See Strategies for Assessing ASP Compliance Section)*

### ***Third Party Attestation of ASP***

Assuming that validation of the ASP's control environment is not practical, and that ASP Self Validation is not acceptable, the likely best choice is to seek Third Part Attestation of the ASP's HIPAA Compliance/Control Environment. In this scenario, an independent, qualified third party essentially conducts an audit on your (and other clients of the ASP's) behalf. Leveraged appropriately, this is an excellent mechanism to obtain an appropriate level of assurance. Several considerations of note;

- If an ASP has not had or refuses to have a Third Party Attestation (Audit) strong considerations should be given to finding a different Anatomic Pathology Information Systems provider. The most likely reasons for an ASP not being willing to subject themselves to an audit are cost or concern about Audit results. In the former, having insufficient resources to invest in a business critical requirement represents a concern regarding the ASP's viability. In the latter, a lab can almost certainly be assured that the ASP is not HIPAA compliant.
- Ensure that the Third Party conducting the audit is qualified to do so. Information systems auditing and HIPAA expertise should be clearly demonstrated. Ideally, the audit will have been conducted by a Certified Information Systems Auditor (CISA) the premier Information Systems Auditing Certification.
- Ensure that the scope of the audit aligns properly with HIPAA.
- Ensure that the audit provides "positive assurance", that is that the audit report details all Control Objectives evaluated, an opinion on control design, evidence of compliance and substantive testing, and an opinion on the effectiveness of the controls relating to each control objective.

- To the extent possible seek to verify the auditing organization has maintained sufficient objectivity. Be wary of any audit Report that is absolutely "clean" (no deficiencies noted at all. In this event, request copies of previous audit reports showing deficiencies and documentation to support the subsequent mitigation of these deficiencies.

As noted above, HIPAA is a minimum control baseline enforced by CMS. Ideally, a lab's Internal Control Framework will be more comprehensive than HIPAA. In these circumstances the Audit Report should be reviewed with consideration of the Lab's Control Objectives as well as to those specified by HIPAA. *(See Strategies for Assessing ASP Compliance Section)*

### ***Business Associate Contract Strategies & Issues***

Once a pathologist or laboratory has determined that it will be a party to a Business Associate contract (either as the Covered Entity or as the Business Associate), the pathologist or laboratory will need to ensure that the contract includes the appropriate language. A Business Associate agreement is likely to include three major components:

- An explanation of permitted uses and disclosures that the Business Associate may make;
- an explanation of the Business Associate's responsibilities;
- and other supporting provisions.

As it is not generally feasible to directly detail the required Administrative, Physical, and Technical objectives for HIPAA to the ASP's environment, the best strategy is to impose performance specifications which are consistent with the Lab's HIPAA compliance needs.

Of note is that when leveraging an ASP the compliance requirement is contractual, under a business partner agreement, and the ASP may not be directly regulated by HIPAA. The challenge under a business partner agreement is to ensure that the ASP properly understands, assumes, and complies with the health care organization's own HIPAA obligations, as imposed on the ASP via the business partner agreement. Accordingly, it is critical that the lab explicitly details the obligations imposed on the ASP, rather than rely on the ASP's generalized understanding of "HIPAA compliance."

A required supporting provision is one that identifies when a CE may terminate the Business Associate agreement. Specifically, the contract must authorize the CE to terminate the contract if the CE determines that the Business Associate has violated a material term of the contract. When a lab is entering into a Business Associate Contract as the CE, it has some responsibility to ensure that the CE complies with the contract's requirements. If the lab has actual knowledge of non-compliance by the Business Associate, the lab *must* take appropriate, reasonable steps to resolve such non-compliance. If such steps are unsuccessful, the lab should terminate the contract or, if termination is unfeasible, report the non-compliance to CMS. As a practical matter, this requirement of actual knowledge imposes a standard for monitoring.

### *Monitoring an ASP's HIPAA Compliance*

An integral part of any Controls Framework, including HIPAA, is ongoing monitoring. The challenge of meeting the monitoring requirements of HIPAA is exacerbated by the use of a Third Party (e.g., ASP) covered under a Business Associate Agreement. The fundamental challenge is "How do I monitor someone else's (e.g., ASP) control environment?"

In a sense it is not truly feasible to do so. It would require the ASP to risk violation of HIPAA during its disclosure of compliance/system auditing information in support of your request that may contain EPHI from another of the ASP's clients. Accordingly, the optimal strategy is likely to monitor that another entity is monitoring the ASP. In this scenario the ASP would be audited for compliance on a periodic basis (ideally no less than quarterly) by an independent, qualified Information Systems Auditing firm.

These reports would be reviewed for compliance against HIPAA and the lab's own internal control objectives. Critical to this effort is taking immediate corrective actions (in compliance with HIPAA) in the event that deficiencies are noted.

## Strategies for Assessing an ASP's HIPAA Compliance

The provision of detailed Internal Control Questionnaires (ICQs) and Audit Programs is beyond the scope of this document, but CE's can use a simple ten question method to initially gauge an ASP's HIPAA Security Rule status. An excerpt from a sample ICQ for several of the HIPAA Security Rule Implementation Specifications is also included. These samples can be used as guidelines for a CE that develops its own audit programs or be used as a baseline for comparison when reviewing the Audit Program or Audit Report provided by the ASP.

### *10 Questions to Rapidly Gauge ASP HIPAA Readiness*

Whether directly auditing the ASP under consideration, or reviewing the attestation of a Third party there are some very basic steps that can be taken that should allow a Lab to quickly gauge the likelihood of HIPAA compliance of an ASP. These 10 questions/issues should be directed at the personnel responsible for compliance at the ASP.

1. Have you obtained and read copies of the HIPAA Security rules from the Federal Register?
2. Have you established a Security Awareness program? *(Please explain the program)*
3. Do you have a dedicated HIPAA project manager? *(Who is it?)*
4. Do you have a privacy officer? Do you have a security officer? *(Who are they?)*
5. Has the HIPAA project manager met with key staff in information services to discuss the requirements, identify the people who need to be involved, and develop a plan of action for HIPAA compliance? *(Please explain the program)*
6. Can you provide an up-to-date copy of all Information Security policies and procedures? Have you performed a gap analysis of your existing policies and procedures compared to the requirements of the proposed standards?
7. What Internal Control Framework are your HIPAA Compliance efforts leveraging?
8. Can you provide an up to date copy of your Risk Assessment?
9. Have you been audited by an independent third party? If so, can you provide the audit report?
10. Who is responsible for HIPAA compliance monitoring on an ongoing basis? *(Please explain the program)*

If the individual answers "No" to more than one of these questions or is unable to adequately and knowledgeably answer the follow on questions or provide the requested materials you should be concerned. An organization that does not fully understand the HIPAA Security rule, has not formally assigned responsibility for compliance, and has not adequately addressed foundational issues is virtually assured of not being HIPAA-compliant.

### *Sample ICQ for Specification Implementations*

The HIPAA Security Rule is Hierarchical in nature with three Safeguards (Administrative, Physical, Technical) encompassing 18 Standards that define 42 Implementation Specifications. The Audit Program will need to address each of the 42 Implementation Specifications. For illustrative purposes we have provided ICQ excerpts for two of the Implementation Specifications.

#### **Workforce Security - 164.308(a)(3)**

*HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*

IMPLEMENTATION SPECIFICATION	KEY ACTIVITIES
Authorization and or Supervision	
	Review Written Job Descriptions for all EPHI impacting roles to ensure; <ul style="list-style-type: none"> <li>• They are correlated with appropriate levels of access.</li> <li>• They address security oversight and training</li> <li>• They address the business need to view, alter, retrieve, and or store EPHI at what times, under what circumstances, and for what purpose.</li> </ul>
	Verify key roles in IT are formalized, along with the activities related to each role. Assure that responsibilities are appropriate to support execution of the role and are allocated to roles rather than to organizational positions.
	Validate that segregation of duties is considered when defining an individual's responsibilities relating to EPHI and that this is enforced through preventive and detective controls (e.g., physical and logical security).
	Ensure that management initiates regular training and awareness campaigns to reinforce staff knowledge of their responsibilities, which should be supplemented by occasional assessments of their understanding and compliance.
	Ensure that log reviews of EPHI systems are being conducted by the data/system owner on a daily basis with appropriate audit ability.
	<i>Supporting Policies &amp; Procedures that will be relevant include; System Audit, Data Segregation, Data Classification.</i>

## Security Incident Procedures - 164.308(a)(6)

*HIPAA Standard: Implement policies and procedures to address security incidents.*

IMPLEMENTATION. SPECIFICATION	KEY ACTIVITIES
Response & Reporting	
	<p>Obtain a copy of the Incident Response Plan; Validate</p> <ul style="list-style-type: none"> <li>• That it correlates with the HIPAA-security risk assessment resulting in a list of potential physical or technological events that could result in a breach of security?</li> <li>• Clear, unambiguous procedures are in place to ensure that there is a standard method for categorizing, prioritizing, recording, maintaining and managing different types of incidents and problems.</li> <li>• Incident Response procedures are clearly communicated throughout the organization, with appropriate personnel receiving training, as required. Procedures are assessed periodically and enhanced as appropriate.</li> <li>• It clearly defines reporting requirements relating to the different classifications of EPHI</li> <li>• It coordinates with the Contingency Plan and Emergency Mode Operation Plan to ensure restoration of key functions of the organization in a prioritized manner</li> <li>• It is supported by procedures that ensure that all necessary information related to the incident is documented and investigated.</li> <li>• Procedures are in place for hierarchical escalation, if more effort or resources are needed, and for functional escalation, if other expertise is needed.</li> <li>• That it defines under what conditions information related to a security breach will be disclosed to whom including critical entities including; Senior management, Business Associates, Law Enforcement, CMS, patients, and the media</li> </ul>
	<p>The responsibility and approval process for approval of emergency and temporary access authorizations is clearly defined, properly documented and supported by management.</p>
	<p>Obtain a copy of the Incident Response Team membership. Validate:</p> <ul style="list-style-type: none"> <li>• The roles and responsibilities for addressing problems</li> </ul>

	<p>and incidents are defined and assigned.</p> <ul style="list-style-type: none"> <li>• The required skills for this task are available to the organization through internal resources and/or external service providers.</li> <li>• An incident/problem manager is responsible for managing the work of the support staff, monitoring the efficiency and the effectiveness of the problem management system, and developing and maintaining the problem management system.</li> <li>• Members of the team have adequate knowledge of the organization's hardware and software</li> <li>• Members of the team have the authority to speak for the organization to the media, law enforcement, and clients or business partners in an emergency</li> <li>• Members of the team the incident response team has received appropriate training in incident response</li> </ul>
	<p>Review Previous Security Incidents. Validate:</p> <ul style="list-style-type: none"> <li>• That adequate documentation of security incidents is kept and that weaknesses that were exploited and EPHI exposure are documented.</li> <li>• That evidence of procedure changes to support challenges to specific Incidents exist</li> <li>• That evidence to support appropriate reporting is maintained</li> <li>• That evidence to demonstrate risk mitigation is maintained</li> </ul>
	<p><i>Supporting Policies &amp; Procedures that will be relevant include; System Audit, Data Segregation, Data Classification, Disaster Recovery &amp; Business Continuity Plan, &amp; Change Management</i></p>

## Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a broad piece of legislation aimed at reforming health care and recognizing the health care industry's increased use of, and reliance on electronic technology. It has placed significant requirements on laboratories as they relate to developing an Internal Control Environment that provides an acceptable level of protection to Electronic Patient Health Information.

In addition to HIPAA compliance for the lab itself, the CE may be faced with ensuring the HIPAA compliance of Business Associates, including Anatomic Pathology Information Systems. This paper was intended to provide a point of reference for those labs considering the HIPAA implications associated with working with an outsourced Anatomic Pathology Information Systems.