HealthITSecurity

HIPAA Best Practices Guide

Sponsored by

LINOMA SOFTWARE

Forward

Whether your organization has been compliant with the HIPAA Omnibus Rule for months or it's still shoring up some compliance gaps, there are likely tips you've picked up along the way. This *HIPAA Best Practices Guide*, however, uses expert analysis and industry expertise to focus directly on exactly what will be expected technically, administratively and policy-wise of HIPAA covered entities and business associates (BAs) during potential audit scenarios. Having a strong understanding of the types of privacy and security measures that the Department of Health & Human Services (HHS) and Office for Civil Rights (OCR) will be looking for from these organizations can help them prepare for audits in 2014 and beyond.

Table of Contents

Part 1: General HIPAA Omnibus Information

HHS posts final HIPAA omnibus rule 1

HHS overhauls Security Rule with HIPAA omnibus provisions 2

Part 2: How OCR Will Enforce HIPAA

OCR Director Leon Rodriguez previews HIPAA audit strategies 5

HHS posts new HIPAA guidance prior to Sept. 23 deadline 6

Part 3: For HIPAA Covered Entities

Prioritizing patient data security in healthcare IT contracts 8

HIPAA omnibus responsibility focus shift: Legal Q&A 9

HIPAA omnibus rules already influencing covered entities 10

SRMC concentrates on secure managed file transfer 11

Part 4: For HIPAA Business Associates

HIPAA omnibus compliance: Collaborating with your BA 13

Business associates prepare for HIPAA omnibus compliance 13

How HIPAA omnibus rule impacts business associates: Q&A 15

Part 5: HHS Encryption Requirements

Encrypting healthcare data at rest: NIST best practices 17

Encrypting healthcare data in motion: NIST TLS best practices 18

Part 1: General HIPAA Omnibus Information

HHS posts final HIPAA omnibus rule

By Pat Ouellette

The long-awaited HIPAA Omnibus Rule was posted by the Department of Health & Human Services (HHS) on the Federal Register public inspection desk yesterday. The new rule will give HIPAA a much-needed update, provide a clearer picture of covered entities' responsibilities and flesh out overlaps and inconsistencies in the rule. The Final Rule is effective on March 26, 2013. According to HHS, covered entities and business associates of all sizes will have 180 days beyond the effective date of the final rule to come into compliance with most of its provisions.

As electronic health record requirements have advanced and healthcare technology in general, the rule needed more specific language that would allow entities more flexibility to adopt technology under the Health Information Technology for Economic and Clinical Health (HITECH) Act while meeting government standards for safety. And the HITECH Act's Breach Notification Rule, which was enacted in 2009, was also altered to better meet current security needs.

The Final Rule is made up of four final rules, which have been combined to reduce the impact and number of times certain compliance activities need to be undertaken by the regulated entities.

First, there were final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, as well as certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. Here are the new responsibilities:

- *Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.*
- *Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.*
- *Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.*
- *Require modifications to, and redistribution of, a covered entity's notice of privacy practices.*
- *Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.*
- *Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule (referenced immediately below), such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.*

Second was the final rule that adopted changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on Oct. 30, 2009.

Third on the list was the final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's "harm" 5 threshold with a more objective standard and supplants an interim final rule published on Aug. 24, 2009.

Lastly, there was a final rule that modified the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

This final rule is also expected to have an annual effect on the economy of $100 million or more, according to HHS, making it an economically significant rule under Executive Order 12866. The total cost of compliance with the rule's provisions is estimated to be between $114 million and $225.4 million in the first year of implementation and approximately $14.5 million annually thereafter.

Costs associated with the rule are:

(i) costs to HIPAA covered entities of revising and distributing new notices of privacy practices to inform individuals of their rights and how their information is protected; (ii) costs to covered entities related to compliance with breach notification requirements; (iii) costs to a portion of business associates to bring their subcontracts into compliance with business associate agreement requirements; and (iv) costs to a portion of business associates to achieve full compliance with the Security Rule.

HHS overhauls Security Rule with HIPAA omnibus provisions

By Pat Ouellette

Healthcare organizations will want to pay close attention to the recently-released HIPAA omnibus rule and how it amended the HIPAA Security Rule. In the final HIPAA rule, the Department of Health & Human Services (HHS) responded to comments based on proposed changes and explained its final Security Rule provisions.

It's not hard for a healthcare provider to get confused between HIPAA Privacy and Security rule specifications. More specifically, business associate agreement (BAA) language had previously been vague. In creating this final rule, according to HHS, it tried to fix that by stating that business associates are (BAs), by definition, separately and directly liable for violations of the Security Rule and for violations of the Privacy Rule for impermissible uses and disclosures pursuant to their BAAs.

HHS agreed with commenters on the HIPAA omnibus rule that hybrid entities, not including BA functions within the health care component of a hybrid entity, could avoid direct liability and compliance obligations for the BA component. So the final rule requires that the healthcare component of a hybrid entity include all BA functions within the entity.

Business associates

Before the HITECH Act, the Security Rule did not directly apply to BAs of covered entities. However, section 13401 of the HITECH Act provides that the Security Rule's administrative, physical, and technical safeguards requirements in §164.308, 164.310, and 164.312, as well as the Rule's policies and procedures and documentation requirements in § 164.316, apply to BAs in the same manner as these requirements apply to covered entities, and that BAs are civilly and criminally liable for violations of these provisions.

To implement section 13401 of the HITECH Act, HHS proposed to insert references in Subpart C to "BA" following references to "covered entity," as appropriate, to make clear that these provisions of the Security Rule also apply to BAs. And it proposed additional changes to §§ 164.306, 164.308, 164.312, 164.314, and 164.316 of the Security Rule, as discussed below.

Some commenters argued that the time, implementation expense, transaction cost, and liability cost burdens on BAs and subcontractors to comply with the Security Rule, especially small and mid-size entities, would be significant. Others supported the direct application of the Security Rule to BAs and subcontractors.

HHS adopted the modifications to the Security Rule as proposed to implement the HITECH Act's provisions extending direct liability for compliance with the Security Rule to BAs. In response to the concerns raised regarding the costs of compliance, we note that the Security Rule currently requires a covered entity to establish a BAA that requires BAs to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information (PHI) that they create, receive, *maintain, or transmit on behalf of the covered entity as required by the Security Rule; and to ensure that any agent, including a subcontractor, to whom they provide such information agrees to implement reasonable and appropriate safeguards to protect it. See § 164.314(a). Consequently, BAs and subcontractors should already have in place security practices that either comply with the Security Rule, or that require only modest improvements to come into compliance with the Security Rule requirements.*

Security Rule requirements were designed to be technology-neutral and scalable to all different sizes of covered entities and BAs. Covered entities and BAs have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any given Security Rule standard. In deciding which security measures to use, a covered entity or BA should take into account its size, capabilities, the costs of the specific security measures, and the operational impact. Thus, the costs of implementing the Security Rule for large, midsized, or small BAs will be proportional to their size and resources.

The final rule adopts the proposed modifications to § 164.308. Section 164.308(b) expressly provides that a covered entity is not required to enter into a BAA with a BA that is a subcontractor; rather, this is the obligation of the BA that has engaged the subcontractor to perform a function or service that involves the use or disclosure of PHI.

BA organizational requirements

Organizational requirements can be tricky for healthcare organizations. While Section 13401 of the HITECH Act doesn't include §164.314 among the provisions for which BAs are directly liable, it states that §164.308 of the Security Rule applies to BAs "in the same manner" that the provision applies to covered entities. Section 164.308(b) requires a covered entity's BAA to conform to the requirements of § 164.314. Accordingly, in order for § 164.308(b) to apply to BAs in the same manner as it applies to covered entities, we proposed to revise § 164.314 to reflect that it is also applicable to agreements between BAs and subcontractors that create, receive, maintain, or transmit electronic PHI.

We also proposed a number of modifications to streamline the requirements of §164.314. First, since a BA for purposes of the Security Rule is also always a BA for purposes of the Privacy Rule, we proposed to remove contract provisions that were merely duplicative of parallel provisions in the Privacy Rule's BA contract provisions at § 164.504.

Second, we proposed conforming modifications to the remaining contract requirements in § 164.314(a)(2)(i) to provide that such contracts must require a BA to comply with the Security Rule, to ensure any subcontractors enter into a contract or other arrangement to protect the security of electronic PHI; and with respect to the reporting of security incidents by BAs to covered entities, to report to the covered entity breaches of unsecured PHI as required by § 164.410 of the breach notification rules.

Third, we proposed to add a provision at § 164.314(a)(2)(iii) that provides that the requirements of this section for contracts or other arrangements between a covered entity and BA would apply in the same manner to contracts or other arrangements between BAs and subcontractors required by the proposed requirements of § 164.308(b)(4).

Finally, we proposed to remove the reference to subcontractors in § 164.314(b)(2)(iii) regarding 102 amendment of group health plan documents as a condition of disclosure of PHI to a plan sponsor, as unnecessary and to avoid confusion with the use of the term subcontractor when referring to subcontractors that are BAs.

HHS did not receive substantive public comment on these proposed changes, but the final rule adopts the modifications as proposed.

Part 2: How OCR Will Enforce HIPAA

OCR Director Leon Rodriguez previews HIPAA audit strategies

By Pat Ouellette

Beyond just discussing how Sept. 23, 2013, is a critical compliance day for the HIPAA Omnibus Rule, Director of the Department of Health & Human Services (HHS) Office for Civil Rights (OCR) Leon Rodriguez, paved the path for OCR privacy and security expectations going forward and revealed some HIPAA audit program focuses during the 2013 HIMSS Privacy and Security Forum.

Rodriguez, who at one point worked for HIPAA covered entities, began his address by reminding the audience that patients, customers, and stakeholders need to be confident that those who are in the business of securing protected health information (PHI) really care about their task at hand. In viewing the health IT security threat landscape broadly, Rodriguez said that there are three main types of major enforcement cases to project how OCR will analyze the different data breaches in the future:

Major security failures: Some data breaches involve patient records being left in the dumpster, but those are just the tip of the iceberg. HIPAA/HITECH set out to give entities specific policies and procedures to follow and failure to follow these policies over a long period of time are the cases that OCR tends to prioritize.

Egregious HIPAA violations: An example of this was the Farah Fawcet UCLA breach.

Access: The largest OCR penalty ever imposed ($4.3 million) was dealt to Cignet in 2011 because it not only failed to give patients access to their own records, but also didn't cooperate with OCR resolution. Patient interests define priorities and judgments for the OCR, said Rodriguez. While many are dry breaches in which data is accessed not for any specific, harmful purpose, they do hurt patient confidence in healthcare organizations' abilities to protect patient data.

Rodriguez highlighted the importance of continually conducting risk analysis for healthcare organizations, especially when the organization's IT infrastructure is in a state of transition. For example, there may be a movement to a different system entirely or implementing virtual desktop infrastructure. "Senior leadership needs to take responsibility for privacy and security," Rodriguez said. "It's not enough to delegate those responsibilities to the CIOs or compliance officers."

Future OCR audit plans

Now that business associates (BAs) are directly responsible for HIPAA compliance, Rodriguez said that OCR enforcement activity will be forthcoming. However, this is an area where he envisions a great deal of learning to be done as well. "I think we're going to find that there were a lot of covered entities that didn't realize they have BAs and BAs that didn't know they were BAs," Rodriguez said.

An important part of how OCR tracks reported breaches will be its recently-released electronic complaint portal that, according to Rodriguez, will end up nearly doubling the amount of legitimate breach complaints from 10,000 per year to about 18,000. "About 90 percent of those complaints have been in regard to HIPAA and most of them do represent justifiable issues," he said. "We'll be looking for more efficient ways of tracking cases, determining and prioritizing the most impactful cases for industry-wide learning purposes."

Some have at times questioned where exactly OCR fine penalty money goes beyond just the idea that it goes toward further auditing. Rodriguez stated that OCR will be leveraging its civil monetary penalties even more than it has already. OCR now has authority from the Office of Management and Budget (OMB) to carry civil monetary revenue across fiscal years, which presents OCR the opportunity to plan how it can best utilize those revenues for auditing activities and analysis. Rodriguez said that OCR had a $38 million budget for this year, in addition to the $4 million it collected in civil penalties, and it plans on asking for a higher budget for fiscal year 2014-2015. "We're just about done with the [2014] audit evaluation and we're in the process of hiring specialized audit personnel, and they'll work with contract auditors," Rodriguez said.

So, how will the 2014 audits be different than the 115 pilot audits that were conducted in 2012? For one, according to Rodriguez, OCR will not use 200 points of auditing again. He wants to reach more organizations annually in a targeted manner. Even though OCR had a multi-million dollar appropriation from the HITECH Act to conduct the pilots, Rodriguez wants to use the funds in a more widely-distributed way for the 2014 audits. "This way, we can see change year-by-year, depending on where we're seeing vulnerabilities, and one focus in the audits will be on risk analysis," he said.

HHS posts new HIPAA guidance prior to Sept. 23 deadline

By Pat Ouellette

The HIPAA Omnibus Rule goes into effect on Monday, but there is already enforcement delay news and additional guidance coming from the Department of Health & Human Services (HHS) on HIPAA compliance.

First, the Office for Civil Rights (OCR) announced a delay in enforcing the requirement that certain HIPAA–covered laboratories revise their notices of privacy practices (NPPs) to comply with HIPAA omnibus modifications until further notice. The delay applies only to Clinical Laboratory Improvement Amendments (CLIA) certified or exempt and those entities in which the HIPAA Privacy Rule has relieved them from having to provide an individual with access to his or her laboratory test. HHS noted that the delay does not affect labs that are part of larger healthcare organizations that don't have their own lab-specific NPPs.

Given the potential proximity of the two rulemakings, OCR is exercising its enforcement discretion to relieve the possible burden on and expense to the HIPAA-covered laboratories identified above of having to revise their NPPs twice within a short period of time, once by September 23, 2013, to comply with the Omnibus Rule, and again by the impending issuance of any CLIA-related amendment to the individual access requirements under § 164.524 of the Privacy Rule. Specifically, with respect to the HIPAA-covered laboratories identified above, OCR will not take enforcement action or seek to impose civil money penalties where the HIPAA-covered laboratory has not revised its NPP by September 23, 2013, to comply with the Omnibus Rule. OCR will issue a notice at least 30 days in advance to advise the public when this enforcement delay will end.

HIPAA refill reminder exception specifics

Next, HHS presented some more details on marketing refill reminders, as the Privacy Rule excludes these reminders from prohibited communications, assuming that the financial remuneration received by the covered entity in exchange for making the communication, if any, is reasonably related to the covered entity's cost of making the communication. The critical component to that language is "reasonably related", which is both hard to define and can be ambiguous at times. HHS attempts to clear up any confusion here:

Does the Communication Involve Financial Remuneration, and If So, Is It Reasonable?

Within exception:

- Communication does not involve remuneration.
- Communication involves only non-financial or in-kind remuneration, such as supplies, computers, or other materials.
- Communication involves only payment from a party other than the third party (or other than on behalf of the third party) whose product or service is being described in the communication, such as payment from a health plan.
- Remuneration involves payments to the covered entity by a pharmaceutical manufacturer or other third party whose product is being described that cover the reasonable direct and indirect

costs related to the refill reminder or medication adherence program, or other excepted communications, including labor, materials, and supplies, as well as capital and overhead costs.

- Remuneration involves payments to a business associate assisting a covered entity in carrying out a refill reminder or medication adherence program, or to make other excepted communications, up to the fair market value of the business associate's services. The payments may be made by a third party whose product is being described directly to the business associate or through the covered entity to the business associate.

Student immunizations

The Privacy Rule allows a covered healthcare provider to "disclose proof of immunization about a student or prospective student to a school that is required by State or other law to have such proof prior to admitting the student," assuming the provider gets the agreement documents from either a parent, guardian, or other person acting *in loco parentis* of the student, if the student is an unemancipated minor or the unemancipated student himself or herself.

Health information of deceased individuals

While the HIPAA Privacy Rule protects the individually identifiable health information about a decedent for 50 years following the date of death of the individual, HHS wanted to point out some provisions:

(1) to alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct (§ 164.512(f)(4)); (2) to coroners or medical examiners and funeral directors (§ 164.512(g)); (3) for research that is solely on the protected health information of decedents (§ 164.512(i)(1)(iii)); and (4) to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation (§ 164.512(h)). In addition, the Privacy Rule permits a covered entity to disclose protected health information about a decedent to a family member, or other person who was involved in the individual's health care or payment for care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity.

Part 3: For HIPAA Covered Entities

Prioritizing patient data security in healthcare IT contracts

By Matt Henderson, Attorney at Hunter Maclean

It is no wonder that data security concerns keep both corporate directors and company general counsel up at night, as reported by the 2013 Law in the Boardroom study by Corporate Board Member and FTI Consulting. While there is no such thing as perfect health data security, a properly-implemented data security program and contract should provide healthcare executives with enough peace of mind to at least get a good night's sleep.

A data security program should be a significant priority for any healthcare organization and should include, at a minimum, employee screening and training, security policies and procedures that are regularly assessed and updated, breach response plans and appropriate insurance. There are specific contractual protections that a healthcare organization should negotiate in its contracts with third-party vendors that will store, or have access to, its data. Additionally, appropriate due diligence is a crucial prerequisite to every good contract and should include investigation and assessment of potential vendors' data security practices.

Once due diligence is done, and you decide to negotiate a contract with a vendor, you will need appropriate contractual provisions for data security. While each contract will vary somewhat, based on the circumstances, the provisions described below, which can be combined in any number of different ways, are a good basis upon which to build a healthcare IT contract from a data security perspective.

Compliance: A compliance provision typically requires the vendor to comply with all applicable laws and regulations. In the United States, the primary, but by no means only, law governing the security of information that must be addressed by healthcare organizations is HIPAA. HIPAA business associate agreements (BAAs), and similar agreements between business associates and their subcontractors should be required in appropriate circumstances. Other federal laws, such as the Drug Abuse Prevention, Treatment, and Rehabilitation Act, may also apply. In addition, state laws, including data breach notification laws (passed by 46 states) must be addressed. In some situations, laws of other countries, such as the EU Data Protection Directive, may also need to be addressed.

Compliance with all applicable laws, however, is typically not enough. The compliance provision will also likely need to include specific provisions with regard to industry standards that are not laws, such as the Payment Card Industry (PCI) Data Security Standards, or applicable National Institute of Standards and Technology (NIST) standards.

Confidentiality: A confidentiality provision is often considered "boilerplate," but it is an essential tool for data security and must be carefully considered and drafted. A confidentiality provision should, at a minimum, define the information that is to be treated as confidential, limit the permitted use, prohibit disclosure outside of the permitted use (except in certain circumstances; e.g., when required by law, and then only after notice is provided), and require return or destruction upon termination of the agreement.

Typically, this provision requires a vendor to use the same level of protection used by the vendor for its own similar data, but that is never enough. There must be a minimum level of protection, which may be achieved by referencing industry standards, commercially reasonable standards, or in some cases even higher standards. If there is a HIPAA BAA between a healthcare organization and the vendor, it should take precedence over any conflicting confidentiality provision for the information that is subject to it.

Data security: This provision should set forth any specific security requirements a vendor must follow. These requirements may include situation-specific requirements, such as requiring intrusion detection and counter-measures to terminate unauthorized activity, prohibiting storage of your data on mobile media, requiring encryption, or requiring access controls for the location where your data is stored, with access logs to be kept for a minimum number of years.

In addition to specific security requirements, the provision should require broad protections, such as administrative, physical and technical safeguards designed to protect against unauthorized destruction, loss, and alteration of data, as well as unauthorized access to data. Due to the rapidly changing technological landscape, the vendor's required security protections should be described in flexible ways that can change over time, such as by referencing then-current industry best practices.

If the vendor is in the healthcare space, it should already have an established security program, which you should review before signing the contract. This should also be updated by the vendor and reviewed by you at least annually thereafter. You should also include a provision that requires the vendor to accept any reasonable revisions you may have to the program.

HIPAA omnibus responsibility focus shift: Legal Q&A

By Pat Ouellette

The Department of Health & Human Services (HHS) modified the HIPAA Privacy, Security and Enforcement Rules, as well as the 2009 HITECH Act's Breach Notification Rule and these changes will impact a wide range of covered entities (CEs). Lisa Sotto, head of Hunton & Williams' global privacy and data security practice, which focuses on privacy, data security and records management issues, has great experience on the subject.

Sotto helps clients identify, evaluate and manage privacy and information security risks and she spoke with *HealthITSecurity.com* about her early HIPAA Omnibus Rule impressions. Beyond the fact that the rule was incredibly delayed, Sotto said that with the new road map, the path ahead may be rough for HIPAA CEs and business associates (BAs), who have until Sept. 23 to prove that they are observant of the new HIPAA language.

What portions of the omnibus rule do you see directly affecting covered entities?

The single biggest issue in my mind is the fact that HHS did away with the significant risk of harm threshold for breach notification. And they replaced it with this presumption that a breach occurred unless the covered CE or business associate (BA) demonstrates that there's a low probability that protected health information (PHI) has been compromised. That was based on at least the four new factors in the Breach Notification Rule.

First of all, HHS will presume that a breach as occurred unless the CE or BA proves otherwise. This requires an entity whose data was compromised to prepare a formal risk assessment. That needs to be documented and they'll need to have that on hand to be able to demonstrate, if need-be to HHS, why they didn't notify in a particular instance.

Also, previously the focus was on harm to the individual and now the focus is on violation of the privacy rule and the probability that PHI has been compromised. There has been a shift away from injury of the individual as a result of the issue. As a result, there's been lot of focus on data breaches since HITECH was enacted in 2009. The burden is growing [for CEs and BAs) because there's the need to have a formal, written risk assessment in place will add to a privacy officer's current HIPAA compliance tasks already in place. The other shift here is with the timing piece. We know you have to notify HHS within 60 days, but in the preamble, HHS says that 60 days is the outer limit and that in some cases, 60 days would be an unreasonable delay.

This, to me, is particularly troublesome because, having handled more than 900 data breaches, many data breaches simply aren't ripe for reporting in 60 days. It's sometimes very difficult to understand the scope of a breach and then, once you've understood the scope, you can then pull together your list of names of people whom you need to send notification. And getting the contact information together is no easy feat.

What about BAs?

We know BAs to be HITECH-liable for certain portions of the privacy rule and most of the security rule. Now there is a direct articulation of the fact that they're going to going to be liable for any impermissible uses or disclosures in violation of the privacy rule as well as failure to provide notification to a covered entity. They list five factors, but I think the three that are most important are impermissible use and disclosures, failure to provide breach notification and the failure to comply with the requirements of the security rule.

The difficulty is now that BAs are defined to include subcontractors, this means all subcontractors down the line to the end of the data flow. Every subcontractor involved is going to have HIPAA Security Rule obligations and some of them may not even know it.

If, for example, you're a cloud subcontractor you can have a CE that signs and agreement with a BA. The BA then hires a subcontractor and may fail to present a BAA to the subcontractor, in which case the subcontractor would have zero clue that the BA is housing PHI because, as a cloud provider, you don't look at the content [because you're often a conduit]. The subcontractor part does go too far and become untenable. If you have to go to the end of the data stream and find every subcontractor down the line, it could be a nightmare.

Are there any administrative requirements to be aware of?

Also the administrative requirements such as having formal, written policies and procedures to implement the security rule, is every subcontractor going to do that? One of the other huge bureaucratic burdens is the requirement to amend every BAA, which is a huge undertaking. There are some entities that have 20,000+ BAAs. And every CE is going to have to change its notice of privacy practices. These are very significant bureaucratic tasks. And they're not heavily-resourced functions.

HIPAA omnibus rules already influencing covered entities

By Pat Ouellette

The new HIPAA omnibus rule will have a considerable impact on HIPAA covered entities, business associates (BAs) and subcontractors, but law firms representing both covered entities and BAs can offer unique perspective on how each side is affected by new regulations.

Dianne Bourque, partner at Mintz Levin, works with clients on how to implement HIPAA-mandated policies and procedures. Bourque also reviews of HIPAA contracts and forms that contain language clients may not be familiar with. Bourque recently explained to *HealthITSecurity.com* some of the different types of HIPAA compliance trends she's seen lately. Additionally, she discussed how exactly these new rules have already begun impacting covered entities and BAs alike since the HIPAA omnibus rule went into effect in January**.**

What types of compliance changes have you seen from healthcare clients?

Mostly what I'm seeing right now is updating forms, policies and procedures. That's the obvious fix that says "Hey, we read the rules and know what we need to do." Frankly, they need to review and update them on a regular basis anyway. There are a lot of entities that enter new business associate agreements (BAAs) with some frequency and they'd need to have a current form by September, so the sooner they start using an updated form the better. And the forms themselves reflect a changing view of our covered entity clients' landscape as a result of the new rule.

We're seeing covered entities take a more aggressive role when negotiating with BAs in terms of control.

For example, we're seeing more covered entities asking for HIPAA policies and procedures from a BA to ensure they're compliant and a reliable repository for protected health information (PHI). A covered entity will have to answer, in one way or another, for its business associate's failure to protect PHI.

How have the different parties been affected?

BAs and downstream vendors have certainly been heavily impacted. Covered entities now have to worry about their BAs and whether they're going to properly hand the data off to a vendor of theirs. Because if the vendor has a breach, then we have to make sure the breach notification goes all the way up stream to the covered entities that are ultimately on the hook notifying individuals. That new reality is reflected in the forms and the approach we're seeing covered entities take, which is demanding the authority to approve of a BA sharing PHI with a vendor. That's hasn't historically been the case.

I'm also worried about vendors that are downstream from the covered entities who may provide services to a wide range of industries. They may have contracts with IT vendors who have contracts with healthcare organizations and have no idea that healthcare regulations apply to them because they are so far downstream from the health care organization.

How do covered entities update these forms and which responsibilities have changed?

The form revisions that we are making reflect regulatory changes. For example, at the end of BA relationship the BA is obligated to return or destroy PHI and if it can't do either of those things, then they're required to protect (while not using it for anything else) what they can't destroy in accordance with the standards of the Secretary of Health & Human Services (HHS).

Covered entities are now seeking to control the decision about feasibility of destruction. That's a subtle yet really significant change in the form because it previously may just have said "If BA cannot return or destroy..." This meant the BA had the discretion to decide if they can't return or destroy. Now the covered entity looks at your infrastructure and operations determines whether it's reasonable to extract that information.

Of course, it's not a small thing to destroy copies of PHI, especially if it's on the Web. From the BA's perspective, no way do we want a covered entity coming in here and telling us what's feasible with respect to our system, right? And from the covered entity's perspective, they don't want a BA holding Phi just because they don't feel like it. There's so much at stake if the wrong choice is made.

Are potential Office for Civil Rights (OCR) audits a factor in organizations becoming more aggressive with HIPAA compliance?

We know from the OCR that it wants to target BAs in its next round of audits because they weren't included in the first round. Their sense is that a number of healthcare breaches were, in part, caused by BA noncompliance. We operate with that in mind and encourage our BA clients to keep that in mind as well. The other group they wanted to look at in their next round of audits were group health plans. They don't get many complaints about them and OCR is curious why that is the case. Either they're doing everything right or no one has an idea of what they're doing and employees don't realize they can complain.

SRMC concentrates on secure managed file transfer

By Pat Ouellette

Data exchange has become a necessary and organic part of a healthcare organization's daily processes and there are plenty of products out there that can assist them with file transfers. But to do so securely presents a different type of challenge for providers. There are a number of factors that come into play when picking a product that augments productivity while allowing an organization to maintain HIPAA compliance. Albert King, Southeastern Regional Medical Center (SRMC) Integration Coordinator, has been using Linoma Software's GoAnywhere solution since December 2009 and led the effort for his organization bringing the product in. GoAnywhere lets organizations secure and automate data exchange between internal and external systems.

There is a lot going on at SRMC, as there are about 50 employees in its IT department and the organization contains 350 patient beds. It has also acquired a number of outpatient clinics and about 30 belong to the hospital now. When looking for a managed file transfer product, King said that the organization's biggest concern was remaining HIPAA compliant.

"We had to make sure it was encrypted, as we had been emailing with password protections through WinZip, and those types of methods to try to be compliant," King said. "The big focus at that point was on file transfer protocol (FTP) and files going out of the organization. It was cumbersome to "WinZip" the files, put a password on them and then make sure the other side's passwords worked."

King added that there were also size issues with emailing large files, as well as the need for a virtual private network (VPN) if SRMC was going to use FTP. In general, the organization wasn't satisfied with just password protection and it later learned from others that only using passwords isn't the best way to handle email security. It wanted to be able to encrypt and send out data with an FTP, so Linoma seemed to be a good fit at the time for what it needed.

"We've had it here since 2009 and started out with maybe 10 jobs and have more than 100 or more jobs running with it now," said King. "It was easy to use and we liked the support that we received from Linoma. We use it not only for files but to email data with the FTP and can also use it to transfer files from Windows servers to IBM's AS/400 servers."

SRMC set up an FTP server and loaded the GoAnywhere software. From there it provided a Web address for users to access files, which King said was a very clean process.

Part 4: For HIPAA Business Associates

HIPAA omnibus compliance: Collaborating with your BA

By Dom Nicastro

Appreciating, embracing and collaborating with your business associates (BAs) doesn't mean you should put undue stress on your healthcare organization during BA negotiations. Remember, they're liable soon too and they should know it.

Those messages from Frank Ruelas, principal of HIPAA College in Casa Grande, Ariz., and current compliance officer at an Arizona hospital, have never rung more true as we head toward the September 23 HIPAA Omnibus Rule compliance day home stretch. According to Ruelas, healthcare organizations must first know that their BAs will be directly liable for HIPAA Security Rule compliance and parts of the Privacy Rule.

"They now have that direct liability attached to what they're doing as a function of their activity," Ruelas said. "You can no longer say there was no contract executed and they're not liable to HIPAA. Once they start fulfilling that function, they've become defined as a BA."

Since HITECH was signed into law in February 2009, security folks immediately felt concern for BAs' security compliance approaches. But do you really have to overwhelm yourself with ensuring all your BA's compliance — especially when your organization's BA list may number in the 1,000s? Not necessarily, Ruelas said. Instead, make it known in your contracts with BAs that, upon requested, you may ask for copies of policies and procedures if you have particular concerns.

"Covered entities feel like they need to audit BAs," Ruelas said. "Why not say in the contract they'll have to provide their books as requested? When you have someone who is associated with you there is some idea that you and this person are in this together."

For example, let's say a BA sends you its policies and procedures. What if you find issues such as they don't change their passwords as often as you do? Does that mean you have to go in there and rearrange things? Can you go down that path within your resources?

Unless you have a precise need, you may not want to create that massive amount of work on top of your own healthcare facility's security requirements. If a particular issue arises, perhaps your contracts specify that your BAs must include assurances to you that the problem's been corrected. But all the while, don't treat them as your business adversary, but rather your associate. "Many covered entities feel like they need to be a big brother to their BAs," Ruelas says. "We already have a big brother — OCR."

If you want to be proactive about ensuring your BAs are security-compliant, that's okay, Ruelas said. But be proficient and collaborative in this regard. Distribute security tips to email lists that include your key BA contacts or invite them to online webinars on security. "I can't tell you how nice BAs feel when they know the CEs want to share with them," Ruelas said. "They feel like sort of an extended family."

And it helps to go back to square one with your BAs. Why did you select them in the first place? Because they were the most trusted to provide your healthcare organization with a service, right? "Try not to think of this as CEs against BAs. I just don't see that collaborative effort and I have no clue why that is," said Ruelas.

Business associates prepare for HIPAA omnibus compliance

By Pat Ouellette

Since the HIPAA omnibus effective date, Sept. 23, is about a month and a half away, covered entities and business associates (BAs) are preparing themselves, respectively, to be compliant in the eyes of the Office for Civil Rights (OCR). Law firms are beginning to see an uptick in conversation with healthcare organizations and vendors to ensure that if and when OCR pays a visit in 2014, they fully understand their responsibilities and, nearly as importantly, have their compliance efforts documented. Drinker, Biddle and Realth partner Jennifer Breuer and senior advisor David Mayer (former senior advisor for OCR compliance and enforcement) told *HealthITSecurity.com* that some of their clients have begun to update documents and confirm that they've accomplished tasks such as updating notices of privacy practices.

Which of your clients are affected by the HIPAA omnibus rule? What are you seeing out in the field?

Breuer: We work with both covered entities and business associates in a variety of different capacities. [It ranges from] work with EHR vendors as well as companies that provide dietary services to hospitals.

From our standpoint, most organizations that were covered entities that we work with had been fairly HIPAA-compliant before the omnibus rule came into effect. They certainly had notices of privacy practices and business associate agreements (BAAs) in place. As for whether every "i" was dotted is another question, but I know they had them.

Now we're seeing a lot of activity in trying to provide those and ensure that they are up to date. We're reviewing a lot of forms and organizations are asking if they have to update those forms now and wondering how much time they have. The sheer magnitude for big healthcare organizations in terms of the contracting process and making sure that a new BAA entails includes everyone knowing exactly which contracts are already put in place. That is a big push right now.

How are the BAs you work with being affected?

Breuer: With respect to covered entities, it's not so much that there's wholesale change as much as there's tweaks here and there. So [the ones we work with] aren't really concerned with compliance. However, with respect to BAs, it's a whole new world.

We're seeing a lot of organizations that purport or want to work in the healthcare industry, but when you push back on them with a BAA, they won't want to sign it. Or they'll say "we're happy to sign this agreement, but you have to tell us what it means." Then, of course we get concerns with the covered entity side that they're not sure themselves what a BA means. And yet they're obligated by the law to know it means because they don't want to take on the vendor's compliance responsibilities for them and they may be afraid enough of their own information to not use them as vendors if they don't know their own obligations.

Healthcare organizations have real responsibilities for contractors and subcontractors that they choose, so that's something they may need to look at a bit more closely than they had in the past.

Mayer: Business associates, now that this is a direct liability, are examining their responsibilities much more carefully than they had previously.

In looking at the recent Oregon Health and Science University (OHSU) breach involving not having a BAA with Google, what's the current landscape with cloud providers and BAAs?

Breuer: I don't know exactly what Google's policy is now, but I know for a long time it wouldn't sign a BAA agreement* and neither would Microsoft, which now as one with Office 365 and they won't vary from the particulars of their own contract. It's very clear from the new rule that cloud service providers are BAs, and that's something to be concerned about. Historically, there was an argument to be made that if data was encrypted in the cloud, while there still may be vendor responsibility to secure the cloud from a business perspective beyond HIPAA, at least you're in a safe harbor position where there's no disclosure needed from a breach notification standpoint. I don't know if that's always true – that information is protected in the cloud.

The answer right now is that BAs see enough other business out there where they don't have to take on that risk. If they're going to be a healthcare service provider, they're going to have to think about that specifically. Companies didn't think about it as much in the early days of cloud computing. There seems to be enough data out there where they don't need healthcare.

Mayer: The nature of your agreement with the service provider is also important because cloud services are provided in a variety of ways. Covered entities and BAs, when negotiating cloud services, are talking about not sharing a server for certain reasons and that the data must reside in a certain place. It's all about location.

** Editor's note: Since this article was published, Google has agreed to sign BAAs with healthcare providers and IT developers.*

How HIPAA omnibus rule impacts business associates: Q&A

By Kyle Murphy, PhD

One significant impact of the HIPAA omnibus final rule is how dramatically it changes the concept of business associates (BAs). Prior to the final rule, BAs were limited to contractors working with covered entities who had access to protected health information (PHI). However, as soon as the new rule takes effect in a few month, contractors and subcontractors hired by a covered entity will bear new responsibility as well as the potential for penalties should they violate the HIPAA omnibus rule.

We caught up with Andrew Gantt, a partner at Cooley LLP, who specializes in electronic health and data privacy issues, to discuss what effect the ruling by the Office of Civil Rights (OCR) and the Department of Health & Human Services (HHS) will have on independent contractors and the liability stemming from their new role as BAs.

What do you make of the OCR and HHS's final ruling for BAs?

It was in the proposed rule, but the whole idea that BAs include all downstream subcontractors is preserved, and that dramatically increased the original scope of HIPAA. They define a BA to include any subcontractor ad infinitum. The import is that anybody who essentially handles protected health information to provide a service for a covered entity or any downstream contractor of that covered entity is actually subject to HIPAA.

The interesting aspect of that is that it not only subjects them to all regulatory requirements, if you will, but they can come after those BAs or subcontractors for penalties. The problem with that construct is that many people wouldn't really be on notice that they would be subject to HIPAA who are not otherwise in the healthcare industry.

How has the scope of HIPAA changed as a result of the final ruling?

It's very far-reaching and safe to assume that the universe of BAs and subcontractors is much larger potentially than the universe of covered entities. The scope of HIPAA now is dramatically increased by virtue of this to cover a whole host of entities when originally covered entities were considered to be subject to HIPAA. Particular with the increased penalties and enforcement weapons, it's a totally different risk profile for people now dealing with health information than previously.

What concerns you most about this understanding of BAs?

My concern is that if they are not required to sign a business associate agreement (BAA) for some reason, which they should be, but if they're not I suspect that they'll be many entities that aren't aware that they are in fact subject to HIPAA and up the compliance. As long as you're either directly or indirectly an independent contractor and you require access to protect health information to provide a service then you'd be subject to HIPAA. Keep in mind now that that's both contractual and legal, so if you sign a BAA you have contractual liability between a BA and covered entity or a subcontractor and a BA but you also have direct liability to the government now so that even if you never signed one of those BAAs, the government can view you as a BA and come after you.

Are there any other unintended consequences of the ruling?

The other thing to keep in mind is that some of these folks don't have the capability to comply with BA obligations. You got to be able to modify records, provide access to particular records, provide accounting of disclosures potentially, and other things they may not actually operationally be able to do. That may require if they want to become HIPAA-compliant, then they may have to change their operations to enable that functionality that doesn't currently exist. The bottom line is the business issue that any covered entity is likely to want somebody to be a BA, so there's a business decision to make even if they don't think they're technically subject to HIPAA

How are BAAs likely to change to accommodate the final rule?

The HIPAA rules prescribe certain language to be included in BAAs, but there are things I think will change by virtue of the fact that enforcement is more likely now and the penalties are much more significant; for example, indemnification provisions. They're not required by HIPAA, but the question is should a BA agree to an indemnity provision that is requested by a covered entity, and certainly I represent entities on both sides of that, but certainly I see it being teed up at least much more frequently now because the practical reality is that if something bad happens, the fallout can be much more significant from a public relations and financial perspectives. I'm seeing indemnity provisions negotiated more strenuously than in the past.

Are there areas where the OCR and HHS have not gone far enough with the ruling?

It's still presumes that the covered entity and the payers are still the source and rightful locus, if you will, of the data. And when that changes so that the bulk of the data is no longer within a healthcare facility — for example, it's actually outside in the cloud or on people's cell phones or all over the place — this model really need to be revisited. It's unfortunate that we're 17 years out of when HIPAA was passed that they didn't work harder to address that specifically.

Part 5: HHS Encryption Requirements

Encrypting healthcare data at rest: NIST best practices

By Pat Ouellette

Whether it's full disk encryption, volume and virtual disk encryption or file/folder encryption, the Department of Health & Human Services (HHS) requires that HIPAA covered entities use storage encryption technologies as part of their storage security controls for data at rest. HHS refers to NIST's Guide to Storage Encryption Technologies for End User Devices for which encryption processes for data at rest are valid for healthcare organizations.

While the guide dates back to 2007, HHS still defers to NIST Special Publication 800-111under its "Guidance to render unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals" section. Take a look at NIST's guidelines for full disk encryption, volume and virtual disk encryption and file/folder encryption below and see how they stack up to your organization's encryption practices:

Full Disk Encryption

Full disk encryption (FDE), or whole disk encryption, involves encrypting all the data on the hard drive used to boot a computer, including the computer's operating system (OS), and permitting access to the data only after successful authentication to the FDE product. Because the majority of FDE products are software-based NIST focused on software-based FDE solutions. But remember that FDE may also be built into a hard drive disk controller. NIST says that hardware and software-based FDE offer similar capabilities through different mechanisms. For example, if a user tries to boot a device protected with hardware-based FDE, the hard drive prompts the user to authenticate before it allows an OS to load.

For a computer that is not booted, all the information encrypted by FDE is protected, assuming that pre-boot authentication is required. When the device is booted, then FDE provides no protection; once the OS is loaded, the OS becomes fully responsible for protecting the unencrypted information. The exception to this is when the device is in a hibernation mode; most FDE products can encrypt the hibernation file.

Virtual Disk Encryption and Volume Encryption

Virtual disk encryption calls for container file encryption, which is a single file that resides within a logical volume and is able to hold many files and folders, and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk. Virtual disk encryption is used on all types of end user device storage.

Alternatively, volume encryption is the process of encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided. According to NIST, volume encryption is most often performed on hard drive data volumes and volume-based removable media, such as USB flash drives and external hard drives. Volume encryption of boot and system volumes is essentially a special form of FDE, and it is not discussed in this section; see the FDE material in Section 3.1.1 for additional information.

Volume and virtual disk encryption have many similarities, according to NIST, as software running on the OS used to access the volume or container handles all attempts to read to or write from the protected volume or container. And after the OS has been loaded, if the user needs to use the encrypted volume or container, it will be mounted after the user has provided the required authentication. From there, the software will then automatically decrypt and encrypt the appropriate sectors as needed.

When virtual disk encryption is employed, the contents of containers are protected until the user is authenticated for the containers. If single sign-on is being used for authentication to the solution, this usually means that the containers are protected until the user logs onto the device. If single sign-on is not being used, then protection is typically provided until the *user explicitly authenticates to a container. Virtual disk encryption does not provide any protection for data outside the container, including swap and hibernation files that could contain the contents of unencrypted files that were being held in memory. Volume encryption provides the same protection as virtual disk encryption, but for a volume instead of a container.*

File/Folder Encryption

Folder encryption and file encryption (encrypting individual files on a storage medium and permitting access to the encrypted data after authentication) are alike, except for the fact that it addresses individual folders instead of files. Both can be implemented via drivers, services, and applications.

Some OSes offer built-in file and/or folder encryption capabilities and many third-party programs are also available. Although folder encryption and virtual disk encryption sound similar—both a folder and a container are intended to contain and protect multiple files—there is a difference. A container is a single opaque file, meaning that no one can see what files or folders are inside the container until the container is decrypted. File/folder encryption is transparent, meaning that anyone with access to the file system can view the names and possibly other metadata for the encrypted files and folders, including files and folders within encrypted folders, if they are not protected through OS access control features. File/folder encryption is used on all types of storage for end user devices.

Encrypting healthcare data in motion: NIST TLS best practices

By Pat Ouellette

An important piece of valid encryption processes for data in motion is Transport Layer Security (TLS), a protocol meant to ensure there are mechanisms in place to protect and provide authentication, confidentiality and integrity of sensitive data during electronic communication. The Department of Health & Human Services (HHS) defers to NIST Special Publication 800-52 Revision 1, released in September 2013, for data in motion encryption best practices.

800-52 Revision 1 offers guidance to the selection and configuration of TLS protocol implementations while using Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms. It also stipulates that TLS 1.1 configured with FIPS based cipher suites as the minimum appropriate secure transport protocol and recommends that agencies develop migration plans to TLS 1.2 by Jan. 1, 2015. Here are the similarities and differences, according to NIST, on the baseline requirements for TLS servers and TLS clients:

Minimum requirements for TLS servers

Protocol Version Support: TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended. Servers that support government-only applications shall be configured to support TLS 1.1, and should be configured to support TLS 1.2. These servers will not support TLS 1.0 or any version of SSL. TLS versions 1.1 and 1.2 are represented by major and minor number tuples (3, 2) and (3, 3), respectively. Agencies must develop migration plans to support TLS 1.2 by January 1, 2015.

Server Keys and Certificates: The TLS server shall be configured with one or more public key certificates and the associated private keys. TLS server implementations should support multiple server certificates with their associated private keys to support algorithm and key size agility. There are six options for TLS server certificates that can satisfy the requirement for Approved cryptography: an RSA key encipherment certificate; an RSA signature certificate; an ECDSA signature certificate; a DSA9 564 signature certificate; a Diffie-Hellman certificate; and an ECDH certificate.

At a minimum, TLS servers conforming to this specification shall be configured with an RSA key encipherment certificate, and also should be configured with an ECDSA signature certificate or RSA signature certificate. If the server is not configured with an RSA signature certificate, an ECDSA signature certificate using a Suite B named curve for the signature and public key in the ECDSA certificate should be used. TLS servers shall be configured with certificates issued by a CA, rather than self-signed certificates. Furthermore, TLS server certificates shall be issued by a CA that publishes revocation information in either a Certificate Revocation List (CRL) [RFC5280] or in Online Certificate Status Protocol (OCSP) [RFC6960] responses. The source for the revocation information shall be included in the CA-issued certificate in the appropriate extension to promote interoperability.

Server Certificate Profile: The server certificate profile, described in this section, provides requirements and recommendations for the format of the server certificate. For these guidelines, the TLS server certificate shall be an X.509 version 3 certificate; both the public key contained in the certificate and the signature shall have at least 112 bits of security. The certificate shall be signed with an algorithm consistent with the public key11 596:

- Certificates containing RSA (key encipherment or signature), ECDSA, or DSA public keys shall be signed with those same signature algorithms, respectively;
- Certificates containing Diffie-Hellman public keys shall be signed with DSA; and
- Certificates containing ECDH public keys shall be signed with ECDSA.

Obtaining Revocation Status Information for the Client Certificate: The server shall perform revocation checking of the client certificate, when client authentication is used. Revocation information can be obtained by the server from one of the following locations:

1. Certificate Revocation List (CRL) or OCSP [RFC6960] response in the server's local store;
2. OCSP response from a locally configured OCSP Responder;
3. OCSP response from the OCSP Responder location identified in the OCSP field in the Authority Information Access extension in the client certificate; or
4. CRL from the CRL Distribution Point extension in the client certificate.

Server Public Key Certificate Assurance: After the server public key certificate has been verified by a client, it may be trusted by the client on the basis of policies, procedures and security controls used to issue the server public key certificate. The server is required to possess an X.509 version 3 public key certificate. The policy, procedures and security controls are optionally represented in the certificate using the certificate Policies extension, specified in [RFC5280] and updated in [RFC6818]. When used, one or more certificate policy OIDs are asserted in this extension. The actual policies and procedures and security controls associated with each certificate policy OID are documented in a certificate policy.

Minimum requirements for TLS clients

Protocol Version Support: The client shall be configured to support TLS 1.1, and should be configured to support TLS 1.2. The client may be configured to support TLS 1.0 to facilitate communication with private sector servers, where necessary. If TLS 1.0 is supported, the use of TLS 1.1 1324 and 1.2 shall be preferred over TLS 1.0. The client shall not support SSL version 3.0 or 1325 earlier. Agencies shall develop migration plans to support TLS 1.2 by January 1, 2015.

Client Keys and Certificate: Client Certificate Profile: When client authentication is needed, the client shall be configured with a certificate that adheres to the recommendations presented in this section. A client certificate may be configured on the system, or located on an external device (e.g., a PIV card). For this specification, the TLS client certificate shall be an X.509 version 3 certificate; both the public key contained in the certificate and the signature shall have at least 112 bits of security. The certificate shall be signed with an algorithm consistent with the public key:

- Certificates containing RSA (signature), ECDSA, or DSA public keys shall be signed with those same signature algorithms, respectively;
- Certificates containing Diffie-Hellman certificates shall be signed with DSA; and

- Certificates containing ECDH public keys shall be signed with ECDSA.

Obtaining Revocation Status Information for the Server Certificate: The client shall perform revocation checking of the server certificate. Revocation information can be obtained by the client from one of the following locations:

1. Certificate Revocation List (CRL) or OCSP [RFC6960] response in the client's local certificate store;
2. OCSP response from a locally configured OCSP responder;
3. OCSP response from the OCSP responder location identified in the OCSP field in the Authority Information Access extension in the server certificate; or
4. CRL from the CRL Distribution Point extension in the server certificate.

Client Public Key Certificate Assurance: The client public key certificate may be trusted by the servers on the basis of the policies, procedures and security controls used to issue the client public key certificate as described in Section 3.5.1. For example, as the implementation of Personal Identify Verification (PIV) [FIPS201-1] becomes more established in Federal Agencies, these guidelines recommend that the PIV Authentication certificate be the norm for authentication of Federal employees and long-term contractors. For users who do not have PIV Cards, such as external users, the set of certificate policies to accept should be determined as specified in Appendix B of [SP800-63], based on the level of assurance required by the application. PIV Authentication certificate policy is defined in [COMMON] and PIV-I Authentication certificate policy is defined in [FBCACP].