Six gray areas of HIPAA you can't ignore

This guide exists to shed some light on some of the 'gray areas' of HIPAA (the Health Insurance Portability and Accountability Act). With the Office for Civil Rights' Phase 2 HIPAA audits looming, there is no room for complacency when it comes to HIPAA compliance. It is hoped this guide will help anyone concerned with HIPAA compliance gain a better understanding of the areas which may be a cause for confusion or concern.

1. If you think HIPAA is just a healthcare industry issue, think again

HIPAA rules apply to any entity that directly handles health information. The most common examples of HIPAA covered entities include healthcare providers such as hospitals and doctors, health insurance providers, and clearinghouses.

Issues arise when organizations conclude that because they do not explicitly fall into one of the covered entity categories as defined by HIPAA, they do not need to concern themselves with HIPAA compliance.

In reality, the definition of a covered entity is fairly broad, and the rules apply to a wide range of organizations from many different industries. For example, many organizations are affected by HIPAA by virtue of the protected health information (PHI) they hold in the form of employee group health plans.

This issue was highlighted in The 2015 Protected Health Information Data Breach Report by Verizon, which linked around 20 different industries, in addition to healthcare, to a PHI data breach.

2. Business Associates and the conduit exception rule

A Business Associate, or BA, is defined as an organization or individual working in association with, or providing services to a covered entity that handles PHI. Examples include:

- Data storage or document destruction companies
- Data transmission companies or vendors who routinely access PHI
- Third party administrators
- Consultants
- Billing companies
- IT contractors
- Personal health record vendors
- Accountants
- Malpractice insurers
- Lawyers

Generally, any organization or individual that creates, receives, maintains or transmits PHI in the course of performing services on behalf of the covered entity qualifies as a BA.

Under the HITECH Act (Health Information Technology for Economic and Clinical Health Act) the way in which a BA handles PHI must be in accordance with HIPAA, and as such BAs are subject to audits by the OCR, and can be held accountable for noncompliance or a data breach.

This considered, all covered entities should have agreements in place, which offer assurances in writing from BAs of their commitment to appropriately safeguard PHI. Such an agreement is known as a Business Associate Agreement (BAA).

This is where things get complicated: An entity that simply transports or transmits PHI, but does not have regular access to it, may claim the 'conduit exception'. Some examples of this would be the United States Postal Service, internet service providers (ISPS) and couriers.

The conduit rule applies to very few organizations, and would not apply to any organization that creates, receives, maintains or transmits PHI on behalf of a covered entity. However, this doesn't stop some organizations from claiming that they are a 'simple conduit for information' and citing the exception rule to get out of signing a BAA. Put simply, if a company won't sign a BAA, you shouldn't risk working with them.

3. When is PHI not PHI?

While PHI should be protected at all costs, there are instances when health information may be made publically available. HHS states that in recognition of the potential utility of health information, even when it is not individually identifiable, section §164.502(d) of the HIPAA Privacy Rule permits entities to create information that is not individually identifiable by following the de-identification standard and implementation specifications (section §164.514(a)-(b)).

Essentially, these provisions allow an entity to disclose health information providing it does not form a basis to make an individual personally identifiable. The National Center of Health Statistics is a good example of a data source that publishes de-identified health information.

The HIPAA Privacy Rule provides two de-identification methods:

1) a formal determination by a qualified expert, or;

2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual.

Once information is de-identified, it is no longer considered PHI, and it therefore no longer covered by the HIPAA privacy rule. In other words, once de-identified, data can be used freely.

But (and it's a big but) even when properly applied, both de-identification methods retain a degree of risk. This risk may be very small, but it is not impossible that de-identified data could be linked back to the individual to whom it corresponds.

4. Addressable HIPAA Safeguards are not optional

The three sets of safeguards that define security standards to help ensure the confidentiality of patient information and prevent a breach of PHI are physical, administrative, and technical.

The technical safeguards are broken down into 6 standards that focus on the technology that protects and controls access to PHI. Under these 6 standards, there are 9 key areas that organizations need to implement. These standards are classified as either 'required' or 'addressable', and include:

1. **Access Control**
   - Unique User Identification (required): Assign a unique name and/or number for identifying and tracking user identity
   - Emergency Access Procedure (required): Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency
   - Automatic Logoff (addressable): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity
   - Encryption and Decryption (addressable): Implement a mechanism to encrypt and decrypt ePHI
2. **Audit Controls (required):** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI
3. **Integrity - Mechanism to Authenticate ePHI (addressable):** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner
4. **Authentication (required):** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed
5. **Transmission Security - Integrity Controls (addressable):** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of
6. **Transmission Security - Encryption (addressable):** Implement a mechanism to encrypt ePHI whenever deemed appropriate

The 'addressable' standards are where confusion often arises.

By ignoring standards classified as addressable, especially around encryption, covered entities and business associates increase the risk of fines for noncompliance and leave themselves more vulnerable to breaches. Fines are very likely to be handed to organizations should they experience a data breach as a result of not using encryption, even if a risk assessment is in place. This is expected to be one of the key areas OCR focus on when conducting phase 2 HIPAA audits.

In summary, addressable standards must not be misconstrued as optional, because they are not.

5. The differing penalties for noncompliance

Failure to comply with HIPAA can result in both civil and criminal penalties. Civil penalties, which are enforced by OCR, are monetary and vary from $100 to $1.5 million, while criminal penalties, enforced by the U.S. Department of Justice, can result in imprisonment for 10 years or more.

Civil penalties

The "American Recovery and Reinvestment Act of 2009" (ARRA) that was signed into law in 2009, established a tiered structure for civil penalties. The following chart outlines the tiered civil penalty structure for HIPAA violations:

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year
HIPAA violation due to willful neglect but violation is corrected within the 30 day required timeframe	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year
HIPAA violation is due to willful neglect and is not corrected within the 30 day required timeframe	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million per identical violation per year

Criminal penalties

For a HIPAA violation to be considered criminal, the person who committed the violation must have done so willingly. Much like civil penalties, criminal penalties for HIPAA violations vary in severity, and are largely based on the intent of the individual responsible for the violation. The following chart outlines the tiered criminal penalty structure for HIPAA violations:

Tier 1	Reasonable cause or no knowledge of violation – Up to 1 year in jail
Tier 2	Obtaining PHI under false pretenses – Up to 5 years in jail
Tier 3	Obtaining PHI for personal gain or with malicious intent – Up to 10 years in jail

Confusion often arises regarding the differing laws and associated penalties from state to state: different states have different laws, and fines and prison terms may vary depending on the criminal charges the individual faces. California, for example, has the most stringent patient privacy laws in the country, and was also the first state to enact a security breach notification law. Conversely, there are still a handful of states and territories, including Alabama, New Mexico, and South Dakota which do not currently have a data breach notification law at all.

Furthermore, some state and federal laws allow individuals to sue in court for privacy violations, which can result in significant fines or damages awards, while others do not.

For organizations, particularly those who operate in more than one state, getting to grips with HIPAA compliance is really just the start - it's crucial that covered entities and BAs familiarise themselves with federal and state laws too.

6. Digital signature

What are digital signatures?
In simple terms, a digital signature is a method for authenticating electronic documents. By using digital signatures, the recipient can be confident that the sender is who they say they are.

Just like a handwritten signature, digital signatures are unique to each signer, but, when implemented properly, are more difficult to forge.

Digital signature technology providers follow a protocol known as Public Key Infrastructure (PKI), which in most basic terms, PKI is a set of roles, policies, and procedures that are used to facilitate the secure electronic transfer of information.

Digital signatures and electronic signatures
They may sound the same, but as the following definitions go to show, there is a big difference between digital signatures and electronic, or e-signatures.

According to the Electronic Signatures Act, an electronic signature is "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

Essentially, an electronic signature is the action of signing electronically during a digital transaction, while the digital signature is the underlying technology that helps verify the authenticity of the transaction.

Digital signatures and HIPAA compliance
If you're wondering why you can't find any guidance on digital signatures on the HHS.gov website, it's because there isn't any, and there hasn't been since 2003.

The only information you'll find is on the HIPAA FAQs for Professionals page, on which OCR states; "currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, covered entities must ensure any electronic signature used will result in a legally binding contract under applicable State or other law." (You can read more about electronic signatures and the law here.)

Additionally, in answer to a question about to whether or not the Security Rule requires the use of a digital signature, OCR states, "The Security Rule does not require the use of electronic or digital signatures. However, electronic or digital signatures could be used as a security measure if the covered entity determines their use is reasonable and appropriate."

So while digital signatures may not be a HIPAA requirement, they do have the potential to improve security standards, and as such play an important role in HIPAA compliance. To help understand how, it's important to be aware of the specific safeguards covered entities must maintain to protect their patients' PHI under the HIPAA Security Rule, and the associated security benefits of digital signature technology.

The Security Rule requires that covered entities must:
- Ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

Digital signatures help organizations maintain these standards by:
- Protecting the integrity of messages throughout their entire lifecycle, through digital encryption;
- Providing user authentication, helping to ensure sensitive information does not end up in the wrong hands; and
- Ensuring non-repudiation (assurances that a person who signs something cannot later deny that they furnished the signature) by providing digital audit trails.

Digital signatures do not ensure HIPAA compliance, but if used correctly, they can help. Until OCR offers more guidance on this topic, it is best to assess every situation carefully, and use digital signatures as an additional security measure where deemed appropriate.