Cloud Services and the Healthcare Alphabet Soup

The healthcare industry seems to be an amalgamation of acronyms, from HIPAA and HITECH to HHS and ACA. While far from comprehensive, this document provides a brief overview of the terminology, federal laws, initiatives and agencies behind some of these acronyms, particularly those impacting cloud and data center services, as well as links to resources for additional information.
While the healthcare industry is subject to countless regulations and laws, the Health Insurance Portability and Accountability Act known as HIPAA seems to have received the most press over the last two decades. Enacted by the United States Congress in 1996, HIPAA is a set of statutes designed to improve the efficiency and effectiveness of the U.S. health care system by:

- Protecting patients’ health information;
- Providing the ability to transfer and continue health insurance coverage for millions of Americans and their families when they change or lose their jobs;
- Reducing health care fraud and abuse; and
- Mandating industry-wide standards for the electronic handling of health care information.

HIPAA directly impacts data centers and cloud services providers (CSPs) because of the fourth bullet above as both may electronically store, transmit or otherwise handle healthcare information on behalf of a wide range of customers. This is addressed later in this document.

HIPAA is comprised of hundreds of pages outlining its various rules and requirements, many of which are amendments to previously enacted regulations. It is divided into five primary provisions, known as titles.

**Title I**
Title I lays out steps to improve the portability and continuity of health insurance coverage for workers when they change employers. It amends three previous federal acts: the Employee Retirement Income Security Act (ERISA), the Public Health Service Act (PHSA) and the Internal Revenue Code of 1986 (IRC).

More specifically, Title I limits the amount of time a group health plan or issuer may exclude an individual’s preexisting condition for coverage, and permits people to reduce this time period by applying prior "creditable coverage" to the new plan. Title I also creates special enrollment rights for people who lose their coverage under certain circumstances, such as job loss, divorce or death.

**Title II**
Title II amends the Social Security Act and the federal criminal code, and contains provisions intended to combat fraud, waste and abuse in both the health insurance and health care delivery systems. It includes an administrative simplification section, which deals with the standardization of healthcare-related information systems. More details are provided on this following the descriptions of the other three HIPAA titles.

**Title III**
Title III amends the IRC to provide tax deductions for medical insurance, specify the amount from a pre-tax medical savings account that may be used for medical expenses and regulate long-term care insurance and long-term care services that must be treated as medical care. It also provides for certain deductions for medical insurance, and makes other changes to health insurance laws.

**Title IV**
Title IV specifies conditions for group health plans regarding coverage of persons with pre-existing conditions, and modifies the requirements for continuing coverage.

**Title V**
Title V includes provisions related to company-owned life insurance and treatment of individuals who lose U.S. citizenship for income tax purposes. Title V also repeals the IRC’s financial institution rule to interest allocation rules.
The Significance of Title II

Of the five HIPAA titles, Title II has the greatest impact on the IT healthcare industry including data center and cloud services. Title II includes what are known as the HIPAA Administrative Simplification provisions, which are rules to protect the privacy and security of health data and are enforced by the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR).

• **The Privacy Rule** establishes national standards to safeguard individuals’ medical records and other protected health information. It requires appropriate safeguards to protect the privacy of protected health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. It also gives patients rights over their health information, including being able to examine their health records, obtain a copy of them and to request corrections.

By law, the HIPAA Privacy Rule applies only to **covered entities**, which are defined as health plans, health care clearinghouses or health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. However, many of these organizations do not carry out all of their health care activities and functions by themselves. Instead, they rely on outside services performed by third parties referred to as **business associates** (BAs).

The Privacy Rule allows covered entities to disclose protected health information to a third party organization in its role as a BA only if it is to help the covered entity carry out its health care functions. The information cannot be shared for the BA’s independent use or other purposes, except as needed for the proper management and administration or to carry out the legal responsibilities of the business associate.

• **The Security Rule** sets federal standards for the security of electronic protected health information (ePHI), and requires HHS to adopt standard transaction formats, code sets and unique identifiers for covered entities to use when electronically transmitting health information. It includes 45 implementation specifications. Required safeguards under the Security Rule are grouped into three categories: administrative, physical and technical.

  • **Administrative safeguards** are requirements related to process-oriented controls, such as policies, risk analysis, termination procedures and training.
  • **Physical safeguards** are the physical controls that protect the ePHI systems and their requisite facilities, equipment, and other infrastructures from natural and environmental hazards, as well as unauthorized intrusion.
  • **Technical safeguards** are the preventative-type controls used to control access to ePHI through and includes unique user accounts, automatic account logout and user authentication. Technical safeguards are also used for the encryption of data “at rest” and “in transit”.

The HIPAA Security Rule also includes “**Organizational Requirements,**” “**Policies and Procedures**” and “**Documentation.**” Under “Organizational Requirements”, **business associate contracts** and the plan documents of group health plans are defined. “Policies and Procedures” and “Documentation” outline the requirements for implementing and maintaining written policies, procedures and documentation. The complete HIPAA Security Rule framework is available at [www.hhs.gov](http://www.hhs.gov).

The **OCR** administers the HIPAA Privacy and Security Rules, and investigates privacy violations and enforces penalties for noncompliance. In addition to holding covered entities accountable, the OCR publishes HIPAA Privacy Rule guidance materials, which are intended to help organizations meet requirements for compliance. The OCR also provides a variety of health care compliance resources in the form of **training materials** and **guidance materials** for covered entities.
The Centers for Medicare and Medicaid Services (CMS) administers and enforces the other HIPAA Administrative Simplification Rules, including the:

- Transactions and Code Sets Standards
- Employer Identifier Standard
- National Provider Identifier Standard

CMS also oversees the Enforcement Rule, which provides standards for the enforcement of all the Administrative Simplification Rules.

**HIPAA Follow-up Acts**

Following the passage of HIPAA, two additional laws were enacted that add requirements to the act and strengthen various aspects of administrative simplification: the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Patient Protection and Affordable Care Act of 2010 (ACA).

**THE ENFORCER: HITECH**

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009 to encourage the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronically transmitting health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. Included are four categories of violations that denote increasing levels of responsibility; four corresponding tiers of penalty amounts that increase the minimum for each violation; and a maximum penalty amount of $1.5 million for all violations of an identical provision.

The HITECH Act removed the previous ban on penalties if a covered entity did not know and with the exercise of reasonable diligence would not have known of the violation. It also prohibited penalties for a violation not corrected within a 30-day time period, as long as the violation was not due to willful neglect.

In accordance with the HITECH Act, the disclosure, handling and use of PHI by a business associate (BA) must comply with the HIPAA Security Rule and HIPAA Privacy Rule mandates. Prior to the HITECH Act, the OCR only audited a HIPAA covered entity when a patient filed a complaint with the agency. However, the HITECH Act now requires the OCR to conduct periodic audits of providers and BAs to ensure they are HIPAA compliant.

**ONC**

The HITECH Act also established The Office of the National Coordinator for Health Information Technology’s (ONC). Located within the U.S. Department of Health and Human Services, the ONC is charged with establishing nationwide efforts to improve health care quality, safety and efficiency through advanced health information technology, including electronic health records (EHRs), and private and secure electronic health information exchange.

The ONC establishes regulations that set the standards and certification criteria EHRs must meet to assure health care professionals and hospitals that the systems they adopt are capable of performing certain functions.

**Omnibus Final Rule**

In 2013, modifications to the HITECH Act were released in the HIPAA "Omnibus Final Rule." The Omnibus Final Rule strengthened patient privacy protections, provided individuals with new rights to their health information and strengthened the government’s ability to enforce the law. Enforcement of the changes went into effect on September 23, 2013. The Privacy and Security Rules noted under Title II of HIPAA focused on covered entities. The Omnibus...
Final Rule expanded many of the requirements to business associates (BAs) of these entities that receive protected health information, such as contractors and subcontractors including data centers and cloud services providers (CSPs).

**Business Associate Definition**

The Final Rule specifically changed the definition of a BA to include:

- A health information organization, e-prescribing gateway or other entity that provides data transmission services to a covered entity and requires access on a routine basis to protected health information (PHI). The OCR expressly declined to further define a “health information organization” because the industry is still evolving. However, an entity that is a mere conduit that does not require access to PHI is not included.
- An entity that offers a personal health record on behalf of a covered entity. However, if the personal health record is not offered on behalf of a covered entity then the personal health record vendor is not a business associate.
- A subcontractor. If a business associate subcontracts part of its function requiring access or use of PHI to another organization, that subcontractor is also subject to HIPAA. There must be a HIPAA compliant business associate agreement between the business associate and its subcontractor.
- A person who creates, receives, maintains or transmits PHI on behalf of a covered entity.
- Physical storage facilities or companies that store electronic PHI, which encompasses data center and cloud services providers.

**Changes to HIPAA**

The Omnibus Final Rule also introduced five major changes to the original HIPAA requirements, with some directly or indirectly related to the use of cloud and data center services.

- It strengthens the HITECH Breach Notification requirements by specifying when breaches of unsecured health information must be reported to HHS.
- There are more stringent limitations on the use of patient health information for marketing and fundraising.
- The sale of patient health information is prohibited without individual authorization.
- Business associates — in this case cloud storage providers — are directly liable for compliance with the relevant portions of the HIPAA Privacy and Security Rules stipulated for business associates.
- Penalties were increased for noncompliance with the Security and Privacy Rules based on the level of negligence, using the tiered civil monetary penalty structure established by the HITECH Act.
- The HIPAA Privacy Rule has been adapted to comply with the Genetic Information Nondiscrimination Act, which prohibits health plans from using or disclosing patients’ genetic information.

In addition, the Omnibus Final Rule expands individuals’ rights. Patients can now ask for a copy of their electronic medical record in an electronic form. When they pay by cash patients can instruct their provider not to share information about their treatment with their health plan. New limits are included on how information can be used and disclosed for marketing and fundraising purposes, and the sale of an individual’s health information is prohibited without that person’s permission.

**Business Associate Agreement Changes**

The Omnibus Final Rule included modifications to business associate agreements (BAAs):

- Business associates must have written business associate agreements with their subcontractors. The subcontractor may not use or disclose PHI in a manner that would not be permitted by the business associate.
• A provision is now included that requires the business associate to comply with the Security Rule with respect to electronic PHI.
• To the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, a provision is also now included that requires the business associate to comply with the requirements of the Privacy Rule that previously only applied to the covered entity.

The Patient Protection and Affordable Care Act (PPACA), referred to as the Affordable Care Act (ACA), is a federal statute that was signed into law in 2010. The ACA was enacted with the goal of reforming the healthcare industry by making insurance more affordable and accessible to a greater range of patients. It includes a variety of provisions, including a mandate for all Americans to obtain health insurance coverage. In addition, insurance companies can no longer drop patients due to pre-existing conditions.

The ACA builds upon HIPAA with expanded provisions for administrative simplification, including requirement to adopt operating rules for each of the HIPAA covered transactions; a unique, standard Health Plan Identifier; and a standard for electronic funds transfer. ACA requires that health plans certify their compliance with the standards and operating rules, and increases penalties for noncompliance.

The ACA impacts the IT infrastructure of healthcare in several ways, including through the funding of grants to improve the quality of care at community health centers through implementation and adoption of health information technology (HIT).

One of the more significant changes from HIPAA to the ACA was the addition of the Physician Quality Reporting Initiative (PQRI), under which physicians are encouraged to make greater use of electronic medical records technology. Under PQRI and ACA, $27 billion will be directed toward the adoption of EMR technology. The funding for this electronic medical records legislation will be expended over the course of 10 years. At the end of that span, the hope is that the majority of, if not all, practices will have improved efficiency and service through the implementation of electronic medical records.

As an additional incentive to medical practices to implement EMR technology, the federal government created a program that provides payments to professionals, as well as institutions, for meeting specific requirements for EMR. To ensure that institutions are making appropriate use of new electronic medical records technology and the funding that goes along with it, several meaningful use requirements were established. These include structured formats for areas such as medical billing, patient records and employee communication. The purpose behind these standards is to guide practices as they attempt to make better use of new technology.

Visit the CMS Meaningful Use page at www.cms.gov for more information.

So what does this all mean for data center operators and, more specifically, for the cloud services they provide? Each of the acts, agencies and incentives outlined in this document somehow impact healthcare information that is stored and/or shared electronically which is what data centers and cloud services providers (CSPs) are often charged with doing by their customers who are in the healthcare industry. While they may or may not directly impact these vendors, they likely do impact the customers of these vendors that are healthcare organizations. What impacts a customer ultimately can affect how a vendor delivers services to that customer.

The Omnibus Final Rule eliminates any doubt about this by stating: “a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus,
document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of ‘business associate’ to generally provide that a business associate includes a person who ‘creates, receives, maintains, or transmits’ (emphasis added) protected health information on behalf of a covered entity.”

To be HIPAA compliant, data storage providers – whether internal or outsourced – must undergo an independent audit, ideally adhering to the OCR HIPAA Audit program to be compliant with the most current requirements. Compliance relies on extensive administrative, physical, technical and organizational safeguards that ensure electronic PHI is secure and protected. The data center and CSPs that are compliant tend to have a comprehensive culture of security with policies and governance standards that are designed to protect PHI and ongoing HIPAA awareness programs and training for employees.

It is important to keep in mind that data centers and CSPs may claim to be “HIPAA certified” or “HIPAA ready,” but this does equate to HIPAA compliance. In fact, there is no such thing as “HIPAA certified” so be careful of companies that say they are.

Vendors that are HIPAA compliant will be able to provide a copy of their HIPAA compliance report. They also should be willing to sign a business associate agreement. If an organization that is classified under HIPAA as a “covered entity” chooses to use a vendor that is not compliant, that company will have to have the vendor evaluated for compliance to prove due diligence.

Keeping pace with what seems to be an endless tide of federal regulations and oversight that impact the IT side of the healthcare industry is a seemingly impossible task – particularly for healthcare organizations already immersed in dealing with these regulations in other aspects of their operations. Working with a data center or CSP that is knowledgeable in healthcare regulatory issues, has a proven track record of performance in working with healthcare organization and can meet compliance requirements can at least take away some of the burden.

To learn more about any of the specific federal healthcare acts, agencies or other programs cited in this paper, please use the links below. To learn more about Peak 10’s compliance program and our HIPAA-compliant cloud offerings, you can visit:

- ONC: [http://www.healthit.gov/newsroom/about-onc](http://www.healthit.gov/newsroom/about-onc)
- The Patient Protection and Affordable Care Act: [http://www.hhs.gov/healthcare/rights/law/](http://www.hhs.gov/healthcare/rights/law/)

Contact a solutions engineer today!
(866) 473-2510
[Peak10.com](http://www.peak10.com)