Understanding HIPAA Privacy:
What it means for healthcare organizations

As HIPAA's Impact on Healthcare Privacy Practices Continues, Here's What You Need to Know…

In the 20 years since the Health Insurance Portability and Accountability (HIPAA) act was signed into law, the impact on healthcare organizations has certainly been widespread but perhaps none more than the settlement by Anthem Inc. in 2018:

- $16 million--recognized as the largest settlement to date.
- Stemmed from a series of cyberattacks on the Blue Cross Blue Shield carrier between 12/14 and 1/15.
- The electronic health information of 79 million people was exposed.

Since HIPAA was passed into law, there have been major additions and key dates in the enactment of the regulations that have primarily focused on the goal of protecting healthcare information.

HIPAA included Administrative Simplification provisions that required the U.S. Department of Health and Human Services (HHS) to adopt national standards for:

- electronic health care transactions and code sets;
- unique health identifiers; and
- security.

At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information and incorporated provisions that mandated the adoption of federal privacy protections for individually identifiable health information.

1996

August 21 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law.

2005

April 20 Deadline for Covered Entities to comply with the Security Rule.

2009

February 17 The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law. This is the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

2003

April 14 Deadline for Covered Entities to comply with the Privacy Rule.

2006

March 13 The Enforcement Rule goes into effect.

2013

January 17 The U.S. Department of Health and Human Services (HHS) releases the Omnibus Final Rule.

March 26 The Omnibus Final Rule takes effect.

September 23 Covered Entities, Business Associates, and subcontractors must be in compliance with most provisions under the Final Rule.

HIPAA Privacy Goals:

The HIPAA Privacy Rule created national standards to protect individuals' medical records and other personal protected health information (PHI). Whereas the **Security Rule** emphasizes how an organization specifically will go about protecting electronic PHI.

HIPAA's Privacy Rule:

- Gives patients more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that healthcare providers and others must achieve to protect the privacy of health information.
- Holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- Strikes a balance when public responsibility supports disclosure of some forms of data such as protecting public health.

Who Is Covered?

The Privacy Rule and all of the Administrative Simplification rules apply to two types of designations:

1. **Covered Entities**—any health plans, healthcare clearinghouses, and healthcare providers that transmit electronic health information in connection with transactions for which HHS has adopted standards.

2. **Business Associates**—persons or entities that perform certain functions or activities that involve the use or disclosure of PHI on behalf of a covered entity.

For both, the key components of privacy compliance entail having a full set of documented and implemented policies and procedures in the areas defined by the rule. In addition, there are organizational requirements, such as having a formally assigned Privacy Officer with the responsibility of overseeing the privacy program.

PRACTICAL POINTER:

A member of the covered entity's workforce is not a business associate, but a covered entity can function as a business associate of another covered entity.

How Is HIPAA Enforced?

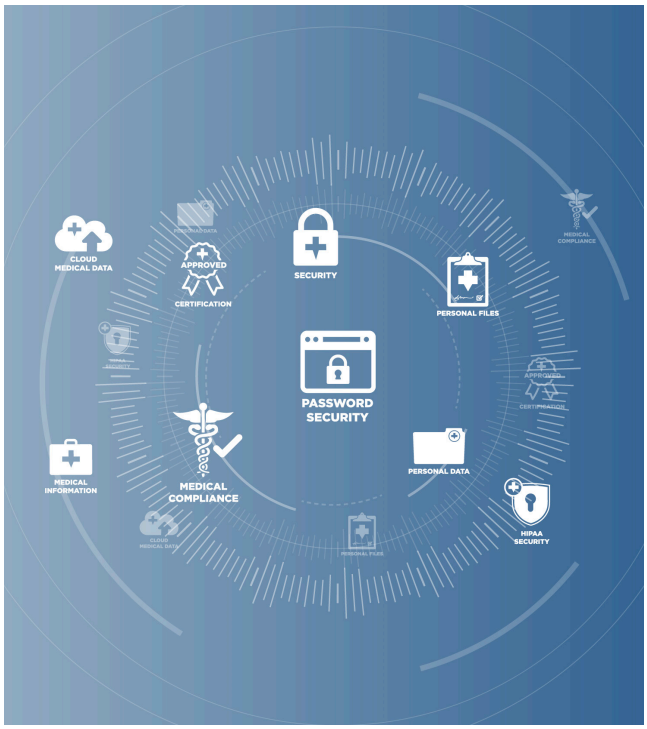
The agency responsible for the enforcement of the HIPAA Privacy Rule is the **Office for Civil Rights** (OCR), an agency of the Department of Health and Human Services (HHS).

OCR carefully reviews all health information privacy and security complaints and may take action on complaints if certain criteria are met. At the end of an investigation, OCR issues a letter describing the resolution of the investigation.

If OCR determines that a covered entity or business associate may not have complied with HIPAA rules, then that entity or business associate must:

- voluntarily comply with the HIPAA rules;
- take corrective action; and
- agree to a settlement.

If the covered entity or business associate does not take satisfactory action to resolve the matter, OCR may decide to impose civil money penalties (CMPs) on the covered entity. If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.



What Are Possible HIPAA Penalties?

Penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Beyond monetary penalties, violations can also carry criminal charges that can actually result in jail time.

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits.