



# **Impact of the American Recovery & Reinvestment Act of 2009 on HIPAA Privacy & Security**

**BridgeFront**

**March, 2009**

## The Act & Changes to HIPAA Regulations

### Introduction

On February 17, 2009 President Barack Obama signed the \$787 billion American Recovery and Reinvestment Act of 2009 into law, according to the [New York Times](#). Here's a brief overview of the Act, courtesy of the federal government's website, [Recovery.org](#):

"In the face of an economic crisis, the magnitude of which we have not seen since the Great Depression, the American Recovery and Reinvestment Act represents a strategic -- and significant -- investment in our country's future."

"The Act will create or save three to four million jobs, 90 percent of them in the private sector. It will provide more than \$150 billion to low-income and vulnerable households -- spurring increased economic activity that will save or create more than one million jobs."

"These measures are necessary to help the millions of families whose lives have been upended by the economic crisis. But, this Act will do more than provide short-term stimulus. By modernizing our health care, improving our schools, modernizing our infrastructure, and investing in the clean energy technologies of the future, the Act will lay the foundation for a robust and sustainable 21<sup>st</sup> century economy."

### Changes to HIPAA Privacy & Security Overview

The Act includes a significant portion on Healthcare IT – including updates to the HIPAA Privacy & Security regulations. There are several new provisions, such as:

- **Enforcement Escalation** – Audits will be dramatically increased. The State Attorney Generals will be prosecuting criminal violations and assessing fines in a more aggressive manner.
- **Accountability** – The new regulations require more vigilance over Business Associate privacy practices, requiring Covered Entities to act if they aren't compliant with the terms in your agreement. Business Associates are now expected to report Covered Entities if they know of violations.
- **Increased Liability** – Individuals will be held accountable in addition to organizations.
- **New Disclosure Rules** – If a breach occurs, you will be required to alert those impacted, alert authorities, post announcements in newspapers and report all breaches annually to the Department of Health & Human Services (DHHS).

The Act directed the Department of Health & Human Services (DHHS) to issue specific guidance on many of these items - which will be occurring over the next few months. While there are provisions with both earlier and later effective dates, the Act's provisions are generally effective as of February 17, 2010.

Listed below is a table of all the areas impacted by the Act's legislation.

## Specific Areas in HIPAA Impacted

### **Enforcement** [§13410 & §13411]

Specifies that violations of the Privacy Rule due to willful neglect require the Health & Human Services Secretary to investigate and impose a civil penalty.

Creates a tiered increase in civil penalty amounts tied to level of intent and neglect from \$100 per violation not to exceed \$25,000 to \$50,000 per violation not to exceed \$1.5 million.

Also stipulates that civil penalties collected should be used to fund the Office of Civil Rights and that within 3 years the Secretary must establish a method based on a Government Accountability Office (GAO) report by which affected individuals receive a percentage of penalties collected.

Authorizes a state attorney general to file suit on behalf of state residents.

Requires HHS to conduct periodic audits on covered entities and business associates to ensure HIPAA compliance.

### **Business Associates & Business Associate Agreements** [§13401 & §13404]

HIPAA Privacy & Security rules apply to Business Associates in the same manner as those rules apply to Covered Entities.

- Establish administrative safeguards to protect ePHI
- Implement physical & technical safeguards to limit physical and electronic access to ePHI
- Establish appropriate policies & procedures to comply with these standards
- Now have a legal duty to have a Business Associate Agreement in place and comply with all the terms within that Agreement. BA's must ensure PHI is not used or disclosed in violation of the permitted uses and disclosures in that agreement.

Business Associates are now considered in violation of HIPAA if they know of a pattern of activity or practice that is a violation of the Covered Entities obligations under the Agreement. Before – Covered Entities were required to monitor the Business Associates compliance with HIPAA. Now – Business Associate's are required to take steps to stop violations of which it becomes aware of when doing business with Covered Entities.

	<p>As new privacy &amp; security regulations come out impacting the responsibilities of Covered Entities, Business Associate Agreements will need to be updated to reflect these changes.</p>
<p><b>Notification Requirement</b> [§13402]</p>	<p>Business Associates are now subject to same criminal and civil penalties as Covered Entities for violations.</p> <p>Both Covered Entities and Business Associates have a legal duty to notify certain parties in the event of a breach of “unsecured PHI.” The definition of “unsecured PHI” will be further defined by HHS.</p>
	<p>A Covered Entity must notify the effected individuals, while a Business Associate must notify the Covered Entity – including the details of the breach, when it happened and who was impacted. Written notice must occur. If there is insufficient contact information for more than 10 affected individuals that precludes a written notice, a conspicuous posting on the covered entity’s web site, or notice in major print or broadcast media that includes a toll-free number.</p>
	<p>If unsecured information of more than 500 residents of a jurisdiction is involved, notice must be made to local media. Notice must be provided to the Secretary and the Secretary must post notice on HHS website if more than 500 individuals are affected. If less than 500 individuals are involved in a breach, the Covered Entity may keep a log and submit it to the Secretary annually.</p>
	<p>Notification must include a brief description of events surrounding the breach, types of information involved, steps individuals should take to protect themselves from harm, steps entity is taking to investigate and mitigate, harm and contact procedures for those seeking more information.</p>
<p><b>Restrictions on Information Disclosures</b> [§13405(a)]</p>	<p>Breach requirements require interim final rule no later than 180 days following enactment to be effective 30 days following.</p>
<p><b>Minimum Necessary</b> [§13405(b)]</p>	<p>Covered Entities must comply with requests from individuals who request PHI not be disclosed to a health plan so long as the purpose of the disclosure does not relate to treatment and the related health care has been paid for out of pocket in full.</p>
	<p>HHS was directed to issue specific guidance on what constitutes “minimum necessary” within 18 months. Until that time, Covered Entities and Business Associates are directed to limit disclosures to the “limited data set” or the minimum necessary to accomplish the intended purpose.</p>

**Accounting for Disclosures**  
[§13405(c)]

In addition to accounting for all non-routine disclosures as currently required under HIPAA, a Covered Entity must account for all non-oral disclosures of PHI used or maintained in an EHR related to Treatment, Payment and Operations (TPO) for a period of 3 years.

An EHR is defined as “an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.”

The Secretary must promulgate regulations on what information must be included in the accounting within 6 months of adopting HIT technical standards on accounting for disclosures.

The regulations must take into account the interest of individuals and the administrative burden. Covered Entities may account for Business Associate disclosures or provide a list of all Business Associates to an individual.

Effective according to when EHR technology is adopted (2011 or 2014). The Secretary may delay compliance but statute would establish a later date certain (2013 or 2016). Covered Entities may not sell EHR or PHI obtained from an EHR without a valid authorization unless:

- The sale is for public health activities.
- The sale is for research activities and the price charged reflects the cost of preparation and transmittal.
- The sale, transfer, or merger of all or part of a covered entity.
- The sale is for a Business Associate function pursuant to a Business Associate agreement.
- The sale is to provide an individual with a copy of his/her PHI to pursuant to his/her right to access.
- The sale is for any other activity the deemed similarly necessary and appropriate by the Secretary.

Secretary must develop regulations for this section within 18 months of enactment, to be effective 6 months after promulgation.

**Right to Individual Access**  
[§13405(e)]

Individuals have the right to obtain a copy, or designate a recipient, of information in an electronic format from any Covered Entity that uses or maintains an EHR with respect to PHI regarding that individual.

Entities may not impose a fee that exceeds the labor costs

<b>Marketing</b> [§13406(a)]	<p>for doing so.</p> <p>Specifies that a communication “about a product or service that encourages recipients...to purchase or use that product or service” is not a health care operation, unless it meets the (i), (ii), and (iii) exceptions under current Privacy Rule. 9</p>
<b>Fundraising</b> [§13406(b)]	<p>Specifies that entities may not receive direct or indirect payment in exchange for communications that fall under (i), (ii), or (iii) unless:</p> <ul style="list-style-type: none"> <li>• The communication describes only a drug or biologic that has been previously prescribed or administered provided payment received is reasonable;</li> <li>• A Covered Entity makes the communication and receives authorization from the recipient of the communication; or</li> <li>• A Business Associate makes the communication consistent with their written business associate contract.</li> </ul>
<b>Personal Health Records</b> [§13400(11), §13423(b), §13407]	<p>The Secretary shall provide that individuals may opt-out of any fundraising communication authorized under the definition of health care operations.</p> <p>Defined as “...an electronic record of individually identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual.”</p> <p>Within one year, HHS and the FTC must conduct a study and submit a report on recommendations for federal privacy and security requirements to apply to non-HIPAA Covered Entities, including Personal Health Records (PHR) vendors.</p> <p>Establishes temporary requirements related to notification in the event of breach similar to those established for HIPAA entities. The FTC has jurisdiction over this provision.</p> <ul style="list-style-type: none"> <li>• The temporary breach requirements take effect 30 days after promulgation of regulations (due 180 days after enactment) and sunset once the FTC has adopted standards for these entities.</li> </ul>
<b>RHIOs and other HIEs</b> [§13408]	<p>Requires organizations, such as Health Information Exchanges, Regional Health Information Organizations, and others, that regularly access PHI from a covered entity to enter into business associate contracts.</p>
<b>Penalties for Employees</b> [§13409]	<p>Clarifies that criminal penalties established by HIPAA statute may apply to an individual or employee of a</p>

**Education and Studies**  
[§13403]

Covered Entity that obtains PHI without authorization.

Educational and outreach initiatives as follows:

- Within 6 months of enactment, HHS regional offices must designate an individual to offer guidance and education to Covered Entities, Business Associates, and individuals on federal rights and responsibilities related to privacy and security.
- Within one year, HHS must conduct a national education initiative to enhance public transparency regarding the uses of PHI.

Additional studies as follows:

- GAO must, within 18 months, submit a report on recommendations for a methodology under which individuals harmed by HIPAA violations could receive a percentage of penalties collected. §13410(c)(2)
- HHS must prepare a report to Congress regarding complaints submitted to the Office of Civil Rights regarding potential HIPAA violations and audit findings. §13424(a)
- Within one year, HHS must issue guidance on how best to de-identify data to meet HIPAA requirements. §13424(c)
- GAO must, within one year, submit a report on best practices related to provider disclosure of PHI for treatment purposes. §13424(d)
- GAO must, within one year, submit a report on the impacts of any provisions of or amendments to the HIPAA Privacy Rule on insurance premiums, overall health care costs, adoption of electronic health records, and reduction in medical errors and other quality improvements. §13424(e)
- HHS must study the definition of “psychotherapy notes” with regard to including test data that are part of a mental health evaluation and may, based on the study, revise the definition.

## Compliance with New HIPAA Regulations

### Introduction

An auditor won't be showing up at your door tomorrow – but this is a wake-up call that the government will be taking a more serious approach to HIPAA enforcement. This is an opportunity to take a fresh look at your policies and procedures and in particular staff training. Keeping your staff aware of their responsibilities is the cheapest insurance you have to protect yourself and your organization.

### Action Plan – Education

[HIPAA Solutions Rx](#) / [BridgeFront](#) guide both large and small organizations through the difficult task of HIPAA compliance. To help you navigate through these new regulations and ensure you are compliant, we have an extensive array of HIPAA training products and consulting services.


We offer several [electronic manuals](#), [templates for policies and procedures](#), [online training courses](#) and [complete HIPAA training packages](#) designed for:


- [Business Associates](#)
- [Chiropractors](#)
- [Clinics & Practices](#)
- [Employers](#)
- [Hospitals](#)
- [Health Plans](#)

If you have a more complex situation, we can help with a detailed risk assessment and develop an action plan to help you gain and maintain compliance.

### Client Testimonials

Over 10,000 organizations have found [BridgeFront](#) to be a reliable and trusted provider of healthcare training products and services. And many of our clients receive special pricing, newsletters, online seminars and other value added services.

	<p>“Over 5,775 Doctors of Chiropractic practices and their staff have successfully used this program. It is simply the best available...easy to follow and affordable.” – <i>Rod Warren, President, NCMIC</i></p>
---	---

	<p>“I’ve seen a lot of material out there on HIPAA and this is the best I’ve seen. Most of the other products aren’t clearly written or are just plain wrong. The manual and training really made my life easier.” – <i>Chad Somers, Benefit Management</i></p>
---	---



We are honored to be the provider of choice to organizations large and small across the country. If your organization is looking for a trusted leader in online healthcare education and an organization that values its clients, [BridgeFront](#) is the right company for you.

### **How to Get Started**

Visit [www.bridgefront.com](http://www.bridgefront.com) or [www.hipaarx.net](http://www.hipaarx.net) for specific information on HIPAA risk assessments or our many comprehensive healthcare training products and learning services. You can also contact one of our specialists by calling **(866) 447-2211** or via email at [info@bridgefront.com](mailto:info@bridgefront.com).

Our specialists can offer assistance in deploying HIPAA training within your organization. Services include creating and identifying staff education needs, developing learning plans, educating managers on administrative and monitoring processes, and being a resource for all of the 'getting started' questions.

### **More Information**

To learn more about how the American Recovery & Reinvestment Act of 2009 affects your organization's HIPAA policies and procedures, please contact us at **(866) 447-2211** or send us an email at [info@bridgefront.com](mailto:info@bridgefront.com).