

FAIRWARNING®



HIPAA & FairWarning®

Ramifications of the American Recovery and Reinvestment Act of 2009 on Healthcare privacy and compliance

February 18, 2009

FairWarning, Inc.

United States of America

Phone: 727 576 6700

Web: www.FairWarningAudit.com

Email: info@FairWarningAudit.com

This document is meant to be general guidance for organizations which may be impacted by HIPAA and does not constitute legal advice. Copyright FairWarning.com, all rights reserved. If you read the document and have a recommendation on how to improve, correct or bring greater objectivity to the assessment, we ask that you send an email your suggestion to info@FairWarningAudit.com.

Overview

The American Recovery and Reinvestment Act of 2009 (the 2009 Stimulus Bill) legislates ambitious investments in Electronic Health Records (EHRs) which will benefit the health of those living in the United States as well as reduce the long-term cost structure required to deliver the best care possible. To further trust in EHRs, U.S. Federal legislators included privacy, enforcement, and administrative language that has a far-reaching impact on the way HIPAA covered entities and their partners handle and protect patient information.

There are several information technology, procedural, business and legal considerations in assessing the impact of the new law. However, there are a few basic ideas which are essential to protecting patient privacy and mitigating the associated institutional risk of privacy breaches - we cover those in a tabular form within this document. Conceptually, the newly expanded law establish timelines to put in place a holistic framework which ensures EHRs can grow securely and rapidly.

In recent years, the information security industry has made great strides in protecting information from external threats and these standard practices are now in place in most healthcare organizations. However, insider misuses of protected information have spread rampantly in recent years. In fact, *according the Computer Security Institute, insider breaches have recently passed viruses as the most reported information security incident.* Within the healthcare industry we have all come to learn that insider abuses of access to EHRs include:

- **Medical identity theft**
- **VIP snooping**
- **Co-worker snooper**
- **Family member snooping**
- **Neighbor snooping**
- **and Identity theft amongst many other forms of EHR misuse**

Unfortunately, it is more often than not, that these forms of Protected Health Information (PHI) breaches injure the patients involved, and cost individuals, healthcare institutions and our industry many billions of dollars. As a companion to this document, the FairWarning® [Privacy Surveillance White Paper](#) provides a detailed overview of why healthcare is vulnerable to insider abuses and how [leading organizations](#) are addressing the challenge.

Under the expanded HIPAA law of the American Recovery and Reinvestment Act of 2009 patient breaches like these will bring dramatically increased risk to the parties involved. This document outlines some of the essential HIPAA compliance considerations from the 1996/2003/2005 law as well as the recently expanded law.

This document has been prepared by [FairWarning®](#), the world's leading supplier of healthcare [privacy monitoring solutions](#). FairWarning® [privacy monitoring solutions](#) are out-of-the-box, affordable, rapid to deploy and bring healthcare organizations into compliance with Federal and state laws such as HIPAA, AB 211, SB 541, FTC Red Flags Rule, PIPEDA, NHS Information Governance Toolkit, Caldicott Guardian Guidelines and others.

FairWarning® & HIPAA of 1996 / 2003 / 2005

§ 164.308 Administrative safeguards (HIPAA)	FAIRWARNING® OUT-OF-THE-BOX PRIVACY AUDITING
<p>REQUIRED. PHI Information system activity review. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports</p>	<ul style="list-style-type: none"> • Core provision for all covered entities • FairWarning® provides automated best-practices with proactive alerting & privacy dashboard, reporting, investigation • Automated, non-intrusive review of all audit sources that access Protected Health Information (PHI) • Dozens of audit sources supported out-of-the-box. Add entirely new audit source in eight (8) business hours
<p>REQUIRED. Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.</p>	<ul style="list-style-type: none"> • This provision supports a patient's right to request an investigation of access to their records as well as entity's responsibility to mitigate damages of suspected incident • FairWarning® rapid patient and user investigation across all electronic health record systems and applications • Proactive patient & user incident detection • Ticket & reporting system to track potential incidents and their outcome
<p>REQUIRED. Risk management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level</p>	<ul style="list-style-type: none"> • Electronic records vulnerable to snooping, identity theft by insider, etc • FairWarning® detects, tracks and deters medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a "breach"
<p>REQUIRED. Sanction policy. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.</p>	<ul style="list-style-type: none"> • Use FairWarning® reporting and monitoring results to apply and re-enforce sanctions. Without specific reporting and monitoring results the sanctioning process can be ambiguous and risky.
<p>STANDARD. Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).</p>	<ul style="list-style-type: none"> • Use FairWarning® reporting and monitoring results to apply and re-enforce training processes. Without specific reporting and monitoring results the sanctioning process can be ambiguous and in-effective.
<p>STANDARD. Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.</p>	<ul style="list-style-type: none"> • Use FairWarning® to detect , track, deter and investigate medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a "breach"
§ 164.306 Security standards: General rules.	FairWarning® Privacy auditing & monitoring
<p>Protect against any reasonably anticipated uses or disclosures of such information that are not permitted.</p>	<ul style="list-style-type: none"> • Use FairWarning® to detect , track, deter and investigate medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a "breach"
<p>Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.</p>	<ul style="list-style-type: none"> • Use FairWarning® to detect , track, deter and investigate medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a "breach"

This document is meant to be general guidance for organizations which may be impacted by HIPAA and does not constitute legal advice. Copyright [FairWarning®](#), all rights reserved. *If you read the document and have a recommendation on how to improve, correct or bring greater objectivity to the assessment, we ask that you send an email your suggestion to info@FairWarningAudit.com.*

HIPAA Highlights of the American Recovery and Reinvestment Act of 2009 (Stimulus Bill)

HIPAA in U.S. American Recovery & Reinvestment Act of 2009	General Description of Expansion	FAIRWARNING® IMPLICATION
HIPAA of 1996 / 2003 / 2005 PRIVACY, SECURITY, ADMINISTRATIVE SAFEGUARDS.	Maintained or expanded as in-line below	See table, FairWarning® & HIPAA of 1996 / 2003 / 2005
EFFECTIVE DATE OF STIMULUS PRIVACY EXPANSION.	<ul style="list-style-type: none"> -Breach & notification responsibilities as outlined below start 180 days after enactment of Bill -HHS Regional privacy officers established within 180 days -HHS OCR shall initiate privacy training within 12 months -Prohibition on sale of PHI 6 to 18 months depending 	FairWarning® provides OUT-OF-THE-BOX, rapid deployment solution in production use in over 100 hospitals, 600 clinics. Customers include organizations as small as 2,000 employees up to 50,000+ employees. Customers include many of the world's most sophisticated healthcare organizations.
DEFINITION OF BREACH.	"Breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Excludes unintentional access.	<p>Medical record snooping by employees, partners, etc, clearly covered by definition of "breach". FairWarning® detects and deters medical record snooping.</p> <p>SNOOPING IN ALL FORMS & INSIDER IDENTITY THEFT, MEDICAL IDENTITY THEFT COVERED AS BREACH</p>
BUSINESS ASSOCIATES.	Rules, treatment, penalties have same applicability to business associates as cover entities	Note: When FairWarning® handles data under BAA, has same general risks & responsibilities as customers
DISCLOSURE & NOTIFICATION.	<ul style="list-style-type: none"> -Clear definition of discovery date -Individual notification 60 days after discovery -Prominent media outlets notified when breach involves 500+ -Immediate HHS notification for 500+ and breach published on HHS web site -Burden of proof on covered entity to demonstrate notifications delivered - Every twelve (12) months Congress shall be provided an update of breach levels during previous year 	FairWarning® used to streamline the discovery process of patients impacted by an internal user mis-using access (snooping, id theft, medical identity theft, etc).
NON-COMPLIANCE DUE TO WILLFULL NEGLECT.	<ul style="list-style-type: none"> -A violation of a provision of this part due to willful neglect is a violation for which the Secretary is required to impose a penalty - REQUIRED INVESTIGATION. The Secretary shall formally investigate any complaint of a violation of a provision of this part if 	Administrative safeguards addressed by FairWarning® clearly defined in elements in FairWarning® & HIPAA of 1996 / 2003 /2005 – see 164.308

This document is meant to be general guidance for organizations which may be impacted by HIPAA and does not constitute legal advice. Copyright [FairWarning®](#), all rights reserved. *If you read the document and have a recommendation on how to improve, correct or bring greater objectivity to the assessment, we ask that you send an email your suggestion to info@FairWarningAudit.com.*

	a preliminary investigation of the facts of the complaint indicate such a possible violation due to willful neglect.".	
TIERED PENALTIES.	<ul style="list-style-type: none"> -Unintentional, not to exceed \$ 25,000 in fines per calendar year - Violation due to a reasonable cause – at least \$ 1,000 per violation up to \$ 100,000 fines per calendar year - Violation due to willful neglect and corrected – at least \$ 10,000 per violation, not to exceed \$ 250,000 per calendar year - Willful neglect and uncorrected violations – at least \$ 50,000 per violation, not to exceed \$ 1,500,000 per calendar year 	FairWarning@ detects and deters insider privacy breaches which could result in penalty against covered entity
STATE ATTORNEY GENERAL.	<p>If the attorney general of a State has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision, the attorney general of the State, may bring a civil action on behalf of such residents of the State in a district court of the United States of appropriate jurisdiction:</p> <ul style="list-style-type: none"> - to enjoin further such violation by the defendant; - or to obtain damages on behalf of such residents of the State, in an amount equal to the amount determined under paragraph <p>-Limitation on state action while Federal action pending</p>	FairWarning@ detects and deters insider privacy breaches which could in action by state attorney general
ACCOUNTING OF DISCLOSURES.	<ul style="list-style-type: none"> -Individuals shall have the right to receive an accounting of disclosures for the three (3) years prior to when the request is made -BAA covered under this section as well 	FairWarning@ can produce detailed access report across applicable audit sources accessing PHI over previous three (3) years
PROHIBITION ON SALE OF PHI.	Page 392 of Stimulus Bill	Not applicable for FairWarning@
MARKETING.	Page 395 of Stimulus Bill	Not applicable to FairWarning@