

HIPAA, ARRA HITECH & FairWarning®

Ramifications of the American Recovery and Reinvestment Act of 2009 on
Healthcare Privacy and Compliance

[A FairWarning® White Paper](#)

[Trust but verify®](#)

Overview

Title XIII of the American Recovery and Reinvestment Act of 2009: Health Information Technology for Economic and Clinical Health Act (ARRA HITECH) legislates ambitious investments in Electronic Health Records (EHRs) which 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 ARRA HITECH. However, there are a few basic ideas which are essential to protecting patient privacy and mitigating the associated institutional risk of privacy breaches. Conceptually, the law establishes 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 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.*

Unfortunately, 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 Breach Detection 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 ARRA HITECH, 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 ARRA HITECH of 2009.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 1

Phone: U.S. 727 576 6700, U.K. 0-800-047-0933



About FairWarning®

FairWarning® is a global leader in appliance-based software solutions which monitor and protect patient privacy in electronic health records enabling healthcare providers and health information exchanges to confidently connect physicians, clinics, patients and affiliates. FairWarning®'s turn-key privacy auditing solutions are compatible with healthcare applications from every major vendor.

Notices

COPYRIGHT NOTICE

© 2010 FairWarning®. All rights reserved.

Copyright and Trademark Notices

The materials in this document and available on the FairWarning® web site are the property of FairWarning®, and are protected by copyright, trademark and other intellectual property laws.

TRADEMARKS

FairWarning®, the logo, Trust but Verify® and other trademarks of FairWarning® may not be used without permission.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 2

Phone: U.S. 727 576 6700, U.K. 0-800-047-0933

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 • Advanced 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" • Governance, risk & reporting dashboard allows tracking of highest risk areas and vulnerabilities
<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 reinforce sanctions. Learn best practices from other customers for the best implementation and roll-out of sanctioning policies
<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 reinforce training processes. Without specific reporting and monitoring results the sanctioning process can be ambiguous and ineffective.
<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, investigate and deter medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a "breach"

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Phone: U.S. 727 576 6700, U.K. 0-800-047-0933

§ 164.306 Security standards: General rules.	FairWarning® Privacy auditing & monitoring
Protect against any reasonably anticipated uses or disclosures of such information that are not permitted.	<ul style="list-style-type: none"> Use FairWarning® to detect, track, investigate and deter medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a “breach”
Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	<ul style="list-style-type: none"> Use FairWarning® to detect, track, investigate and deter medical record snooping, identity theft, medical identity theft, etc. These unauthorized uses of PHI are defined as a “breach”

Highlights of Title XIII of the American Recovery and Reinvestment Act of 2009: Health Information Technology for Economic and Clinical Health Act (ARRA HITECH)

HIPAA in ARRA HITECH	General Description of Expansion	FAIRWARNING® IMPLICATION
HIPAA of 1996 / 2003 / 2005 PRIVACY, SECURITY, ADMINISTRATIVE SAFEGUARDS.	Maintained or expanded per below	See table, FairWarning® & HIPAA of 1996 / 2003 / 2005
EFFECTIVE DATE OF HITECH PRIVACY EXPANSION.	<ul style="list-style-type: none"> Most provisions became effective February 18, 2010 (one year after passage of the bill) The Enforcement Interim Final Rule, issued October 30, 2009, became effective November 30, 2009. See “Penalties” below. The Notification Interim Final Rule, issued August 24, 2009, became effective September 24, 2009. See “Disclosure & Notification” below. HHS OCR has specified that Covered Entities will have 180 days beyond the effective dates to become compliant. 	FairWarning® provides OUT-OF-THE-BOX, rapid deployment solution in production use in nearly 400 hospitals and 1,400 clinics. Customers include organizations as small as 500 employees up to 50,000. The implementation process is streamlined for optimal compliance positioning.
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	Medical record snooping by employees, partners, etc, clearly covered by definition of “breach”. FairWarning® detects and deters medical record snooping. SNOOPING IN ALL FORMS &

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Phone: U.S. 727 576 6700, U.K. 0-800-047-0933

	retain such information. Excludes unintentional access.	INSIDER IDENTITY THEFT, MEDICAL IDENTITY THEFT COVERED AS BREACH
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 misusing 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 a preliminary investigation of the facts of the complaint indicate such a possible violation due to willful neglect. 	Administrative safeguards addressed by FairWarning@ clearly defined in elements in FairWarning@ & HIPAA of 1996 / 2003 /2005 – see 164.308
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, 	FairWarning@ detects and deters insider privacy breaches which could result in penalties against covered entity

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 5

Phone: U.S. 727 576 6700, U.K. 0-800-047-0933

	not to exceed \$ 1,500,000 per calendar year	
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 • limitation on state action while Federal action pending 	FairWarning® detects and deters insider privacy breaches which could result 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.		Not applicable for FairWarning®
MARKETING.		Not applicable to FairWarning®

For more information on privacy breach detection solutions from FairWarning®, please contact Solutions@FairWarningAudit.com or visit www.FairWarningAudit.com.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 6

Phone: U.S. 727 576 6700, U.K. 0-800-047-0933