

ARRA 2009 & HIPAA

Presentation materials in-line below

[*The webinar replay link is available here*](#)

[*Q&A, plus the summary can be found here*](#)

March 9th, 2009

FairWarning®
Trust but Verify®

<http://www.FairWarningAudit.com>

info@FairWarningAudit.com

727 576 6700 x115 U.S.A.

ARRA 2009: Privacy and Security Provisions

Deven McGraw

Health Privacy Project at CDT

- Health IT and electronic health information exchange have tremendous potential to improve health care quality, reduce costs, and empower consumers
- But for years there was no progress on resolving the privacy and security issues raised by e-health
- Project's aim: Develop and promote workable privacy and security policy solutions for personal health information

ARRA (Title XIII- HITECH)

- ❑ Broke the privacy “logjam”
- ❑ Most significant change to the healthcare privacy and security environment since the original HIPAA privacy rule
- ❑ Not a change to everything about HIPAA – but some significant changes that will need to be addressed by many entities handling health care information
- ❑ Most provisions require further regulatory clarification

Privacy and Security Provisions - Overview

- Substantive changes to HIPAA statutory provisions and privacy and security regulations.
- Enhanced enforcement of HIPAA
- Provisions to address health information held by some entities not covered by HIPAA
- Misc:
Administration/Studies/Reports/Educational Initiatives

Substantive HIPAA Changes

- Breach notification requirement
 - Definition of breach
 - Safe harbor for “protected” data
- Strengthened individual right to restrict disclosures to health plans for payment and operations

Substantive HIPAA changes (cont.)

- ❑ Secretary guidance on minimum necessary
 - ❑ Use of limited data set where possible in interim
 - ❑ Discloser determines minimum necessary
- ❑ Minimum necessary still does not apply to treatment

Substantive HIPAA changes (cont.)

- ▣ Accounting for disclosure requirements for entities using electronic health records
 - ▣ Requirement applies after standard and regulations are developed
 - ▣ Phased in over time
 - ▣ Covers only 3 years
- ▣ Change with respect to how business associates comply

Substantive HIPAA changes (cont.)

- ❑ Prohibition on “sale” of health records or protected health information
- ❑ Exceptions
 - ❑ Public health
 - ❑ Research
 - ❑ Treatment of an individual
 - ❑ Sale of a facility/business
 - ❑ Payments to business associates
 - ❑ Copies to individuals

Substantive HIPAA changes (cont.)

- Patient right of electronic access
 - Can direct record to another entity or individual (PHR)
- Changes to definition of marketing
 - Limited right to use information for marketing if the communication is paid for by an outside entity
 - Exceptions for treatment and communications about current drugs and biologics
- Opt-out for fundraising communications
- BA contracts required for RHIOs – and PHRs in some instances

HIPAA Enforcement

- ❑ Business Associates accountable to authorities for compliance with some HIPAA privacy and security rules (+ new provisions)
- ❑ Application of HIPAA criminal provisions to individuals
- ❑ Ability to civilly enforce where violation qualifies as criminal but no criminal penalties pursued

HIPAA Enforcement (cont)

- ❑ Requirement to impose civil penalties in cases of willful neglect
 - ❑ Corrective action may still be pursued for lesser offenses
- ❑ Tiered increase in civil monetary penalties
- ❑ Distribution of % of civil penalties to individuals (penalties also go to OCR)
- ❑ State AG civil enforcement
- ❑ Secretary required to do periodic audits

Provisions for Entities not Covered by HIPAA

- Temporary breach notification provisions for PHR vendors and internet applications
 - Breach definition
 - Same safe harbor for protected information
 - Enforced by FTC

Provisions for Entities not Covered by HIPAA (cont.)

- Study by HHS & FTC with report to Congress on privacy and security recommendations for PHRs
 - Which agency should regulate?
 - Timeframe for regulations (no specific authority to regulate)

Misc.

(Administration/Studies/Reports/Educational Initiatives)

- ▣ Strengthened authority for ONC
- ▣ New advisory committees on policy and standards
- ▣ OCR public education initiative on uses of PHI and individual rights under HIPAA
- ▣ Privacy Officers in each HHS region
- ▣ Chief Privacy Officer within ONC
 - ▣ Not charged with HIPAA enforcement/oversight

Misc. (Studies/Reports/Educational Initiatives)

- Studies/Reports by HHS Secretary
 - Annual report on enforcement
 - Study on implementation of the de-identification requirements
 - Study of HIPAA definition of psychotherapy notes with respect to inclusion of test data and materials used for evaluative purposes

Misc. (Studies/Reports/Educational Initiatives)

□ GAO Studies:

- Methodology for providing individuals with a % of civil monetary penalties
- Report on best practices for disclosure of PHI for treatment purposes
- Report on Impact of ARRA provisions on health care costs and adoption of EHRs

For privacy to enable health IT, we
have to enable privacy

deven@cdt.org



The Medical Center is taking steps to fire at least 13 employees and is disciplining others, including doctors, for looking at the pop star's confidential files.

Man found guilty in Santa Rosa identity theft case

A former Santa Rosa Medical Center nurse took the stand Thursday and admitted that he stole a patient's identity and used it to get thousands of dollars to purchase vehicles.

POWERED BY YOU AND THE PENSACOLA NewsJournal

Nurse pleads guilty to privacy violation

...She then gave the information to her husband, Justin Smith, who called the patient and threatened to use the information against the patient in "an upcoming legal proceeding,"

Arkansas Democrat  Gazette
NORTHWEST ARKANSAS EDITION

NEW YORK POST

24 HOURS A DAY

'SCAM' GUY HIT 50,000 HOSP ID THEFT SPREE

...employee charged with selling patient information as part of a wide-scale identity-theft ring illegally accessed nearly 50,000 patient files, prosecutors said yesterday.



HIPAA audit: The 42 questions HHS might ask

They cover everything from security to employee status to Internet use

COMPUTERWORLD



Reactionary investigations
Delayed, inconsistent incident discovery
Manual, time consuming processes
Audit logs in stove pipes



Healthcare information systems and applications

Windows Servers, Unix

Single Sign On, PeopleSoft

VPN

✓ **Automates compliance processes**

HIPAA, FTC Red Flags Rule, AB 211, SB 541
PIPEDA, Caldicott

✓ **Streamlines incident investigation & reporting**

✓ **Proactive alerting with filtering**

✓ **Dozens of EHRs supported out-of-the-box**

✓ **Out-of-the-box, in-production, massive scale**



Entity-wide Plan

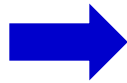
Drivers

HIPAA 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

HIPAA 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.

HIPAA REQUIRED.
Risk management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

Patient privacy risks
Return on investment



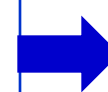
Functional Results

- Investigate & mitigate damages of suspected patient and user incidents

- Detect, track, deter and report vulnerabilities:
 - Medical identity theft
 - Co-worker snooping
 - VIP snooping
 - Neighbor snooping
 - Many other scenarios

- Breach notifications

- Accounting of disclosures



HIPAA REQUIRED.
Sanction policy. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.



HIPAA STANDARD.
Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).



**FairWarning®'s mission is to be the
world's leading supplier of solutions
which monitor & protect patient privacy
in Electronic Health Records.**

Trust but Verify®

**info@FairWarningAudit.com
727 576 6700 x101 U.S.A.**