

# Privacy Breach Detection in Healthcare

Healthcare Organizations will be Required to use Privacy Breach Detection with Electronic Health Records to Finally Stop the Proliferation of Snooping, Identity Theft and Avoid Penalties for Non-compliance

[A FairWarning® White Paper](#)

[Trust but verify®](#)

## Overview

The healthcare industry is experiencing an epidemic of high profile privacy incidents involving employees and affiliates using Electronic Health Records (EHRs) to conduct unlawful activities. These activities include VIP record snooping, identity theft, medical identity theft as well as co-worker, family member and neighbor snooping. These incidents have serious consequences for both the patients and institutions involved. Compounding the situation is increasingly aggressive enforcement of privacy and security legislation which carries punitive damages for healthcare institutions and in the case of some states, fines for individual employees involved.

## What is Privacy Breach Detection?

Privacy breach detection systematically identifies users who are engaging in patient access patterns that are indicative of snooping, identity theft or other risky behaviors. Privacy breach detection is performed for all crucial EHRs and applications which provide access to Protected Health Information (PHI). *Privacy breach detection filters out known false positives and brings any remaining potential incidents to the attention of appropriate privacy personnel.* For organizations conducting tedious manual audit log reviews, privacy breach detection automates the work-load and is dramatically more comprehensive.

***This white paper explores why healthcare is so vulnerable to insider privacy incidents and outlines why privacy breach detection is a required component of any entity wide privacy and security program.***

**FairWarning, Inc.**

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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



## Why Healthcare Organizations are Vulnerable to Insider Incidents

A patient's PHI must be accessible by an increasingly wide range of specialized healthcare personnel, including: Registration, Accounting, Nursing, Pharmacy, Physicians, Technicians, Partner Clinics, Partner Physicians and others.

Compounding this wide-scale access is the fact that healthcare must operate with patient safety as the number one priority. This means that generally access to patient records is granted to all clinical personnel that *may* need access which presents even greater privacy challenges. In no case can a limitation of access jeopardize the rendering of care. Lastly, EHRs are built with patient safety in mind, meaning their wide-scale access controls lack granularity. For technical and patient safety considerations, healthcare organizations find themselves unable to reel in access to patient information.

*Necessary and wide-scale access to Protected Health Information by growing numbers of healthcare personnel is proving to be a disastrous recipe for patient privacy, institutional reputation and compliance.*

## Damaging Healthcare Privacy Incidents<sup>1</sup>

The most damaging and high-profile privacy incidents over the last several years were perpetrated by healthcare insiders. It is noteworthy that even the most prestigious, well-funded institutions are not immune from these types of insider incidents. This suggests that insider vulnerabilities are not simply a function of management sophistication or budget size. Rather, these incidents reflect the challenge of balancing privacy considerations with patient safety objectives, and this dilemma will continue to occur until a new privacy approach is taken.

Considering the recent examples below, it is hard to estimate how many similar incidents are not covered in the media or even disclosed in states where disclosure is not mandatory.

### Mayo Clinic in Arizona

- In September 2010, an employee of Mayo Clinic's financial business unit, was fired for snooping an estimated 1,700 patient records. Between 2006 and 2010, the employee, who had access to patient records at all locations, accessed both medical and financial records well beyond those required for his job.

---

<sup>1</sup> <http://www.phiprivacy.net>

## 10 Hospitals Fined for Snooping in California\*

- In June 2010, the California Department of Public Health fined five hospitals a total of \$675,000 for failing to prevent unauthorized access to confidential patient medical records. The affected hospitals were Community Hospital of San Bernardino, Enloe Medical Center, Rideout Memorial Hospital, UCLA Medical Center, and San Joaquin Community Hospital. The hospitals were also required to submit a corrective action plan to the state.

## Health Central Hospital in Florida\*

- In November 2009, celebrity golfer Tiger Woods crashed his Cadillac Escalade and ended up at Health Central Hospital in Ocoee, Florida. The hospital reported more than 6,000 phone calls attempting to get information on Woods, including tabloids offering employees “big payouts” to provide Woods’ medical records. Several employees were fired as a result.

## University Medical Center in Las Vegas\*

- Between January and November 2009, UMC employee Richard W. Charette sold registration information for accident patients to ambulance-chasing attorneys at least 55 separate times. The leak was ultimately uncovered by the media, at which time the health system was forced to investigate. Charette has been indicted on one count of conspiracy to illegally disclose personal health information, and a lawsuit against UMC is seeking class-action status.

## Queen Margaret Hospital in Scotland\*

- In March 2009, Queen Margaret Hospital physician Andrew Jamieson was disciplined for accessing the records of a number of celebrities, including Scottish Prime Minister Gordon Brown, several BBC journalists, and others.

## New York – Presbyterian Hospital Identity Theft\*

- From 2006 through 2008, Dwight McPherson, an admissions employee at New York-Presbyterian Hospital in Manhattan, sold almost 50,000 patient files to an identity theft crime ring. The breach was discovered by investigators looking into the identity theft ring, which led them back to the hospital. McPherson has been charged with computer fraud and sale of stolen property, and is awaiting trial.

***Healthcare privacy incidents damage patient lives and harm the trust we have in our healthcare institutions. Next, we will look at why standard security technologies do not address insider vulnerabilities.***

**FairWarning, Inc.**

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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

## Limitations of the Security “Laundry List”

In 2009, as part of the American Recovery & Reinvestment Act, the [Health Information Technology for Economic and Clinical Health Act \(HITECH\)](#) was created, expanding upon HIPAA requirements and increasing the associated penalties. This is motivating healthcare organizations to re-evaluate their security plans and technologies. A number of security technologies are all promising to deliver the silver bullet to stop insider security incidents in healthcare:

- **Encryption:** Many healthcare organizations are implementing encryption on laptops and other endpoint devices, such as flash drives, since they can be carried off-site along with PHI. **Encryption is not a factor in stopping insiders with authorized access to EHRs and applications.**
- **Single Sign On (SSO):** SSO is a good addition for organizations wishing to enforce password policies and provide convenient login to applications. ***While important, SSO technology does not stop authorized users from abusing their access privileges.***
- **Identity Management and Provisioning:** This technology assists with credentials management and fills gaps related to denying access to former employees (their user ids are removed automatically). ***Identity management or provisioning does not stop active, authorized users from abusing their access privileges. In addition, identity management or provisioning deployments can be lengthy and expensive.***
- **Security Information Management (SIM):** SIM or SIEM technology collects information security events from infrastructure systems such as firewalls, routers, IPS, IDS, servers and VPNs. SIM technology was not designed to support EHRs and thus fails to address two major vulnerabilities:
  1. **SIM products leave a significant [HITECH & HIPAA](#) compliance gap.** A core [HITECH & HIPAA](#) requirement mandates that all systems accessing PHI must be systematically reviewed and audited. Clearly, EHRs and healthcare applications access PHI and by definition must be reviewed and audited.
  2. **SIM products do not curtail insider incidents involving EHRs and applications because they do not access EHR audit logs and were not designed to analyze data such as patients, users and function codes.**

***With the above in mind, no matter how much money is spent on security technologies, a healthcare organization will continue to experience a growing number of seriously damaging incidents perpetrated by active employees and partners. Authorized users are turning out to be the largest source of risk.***

**FairWarning, Inc.**

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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

## What is Privacy Breach Detection?

[FairWarning®](#) privacy breach detection centrally and systematically identifies users who are engaging in patient access patterns that are indicative of snooping, identity theft or other risky behaviors. Privacy breach detection is performed for all crucial EHRs and applications which provide access to PHI. FairWarning® privacy breach detection then brings the potential incidents to the attention of appropriate privacy personnel through a web based dash board and / or proactive alerting, such as email. Incidents that previously went undiscovered are identified and managed through a central, point and click web based interface. For organizations conducting tedious manual audit log reviews, privacy breach detection automates the work-load and is dramatically more comprehensive. **Based on reference-able FairWarning® customer studies, manual review processes are reduced by over 90 % and incident visibility is improved by over 80 %, which means that on average, for every incident found by a manual process, at least four (4) more go undetected.** Incident categories include:

- Co-worker / patient snooping
- VIP Medical Record Access
- Financial identity theft
- Medical identity theft
- Inappropriate physician access
- Neighbor snooping
- Others

[FairWarning®](#) privacy breach detection also provides tools to rapidly investigate and resolve patient / user incidents. [FairWarning®](#) maintains a forensically secure environment for preserving information about patient access, this is essential for [HITECH & HIPAA](#) as well as other state and federal legislation.

Unlike typical audit log tools, privacy breach detection solutions focus on EHR and healthcare application audit logs. **Non audit log data can also be used to detect specific healthcare insider scenarios.** Through patent pending, non-intrusive technology, [FairWarning®](#) centralizes healthcare application audit logs and analyzes information in the form of Patients, Users, Date, Time, Functions Performed and even location information such as Terminal ID, IP address, Bed, Campus and other. **[FairWarning® delivers a user experience that is perfectly suitable for a privacy officer and associated staff.](#)**

***FairWarning® has well over 100 healthcare specific vulnerability scenarios bundled into its solutions, additional scenarios which can be modeled are limited only by imagination and availability of the data.***

### FairWarning, Inc.

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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

## Why is Privacy Breach Detection so Powerful?

Essential to deterring and eliminating insider privacy incidents is creating the right culture through technology, training and an entity wide security plan. Privacy breach detection ties these concepts together to deliver sustainable privacy and compliance.

Privacy officers in today's healthcare environment are "driving blind" without privacy breach detection. For example, patient complaints and employee tips are the primary methods in identifying potentially damaging incidents. Manual random privacy audits may help, but they are unreliable, incomplete and unsustainable. Consider the graph in Figure 1 associated with a typical healthcare organization with a dedicated staff member reviewing audit logs attempting to identify incidents. **Notice that through manual efforts, an average of two to three verified incidents per month were identified. Once FairWarning® privacy breach detection was deployed, a six-fold increase over those identified by manual methods.**

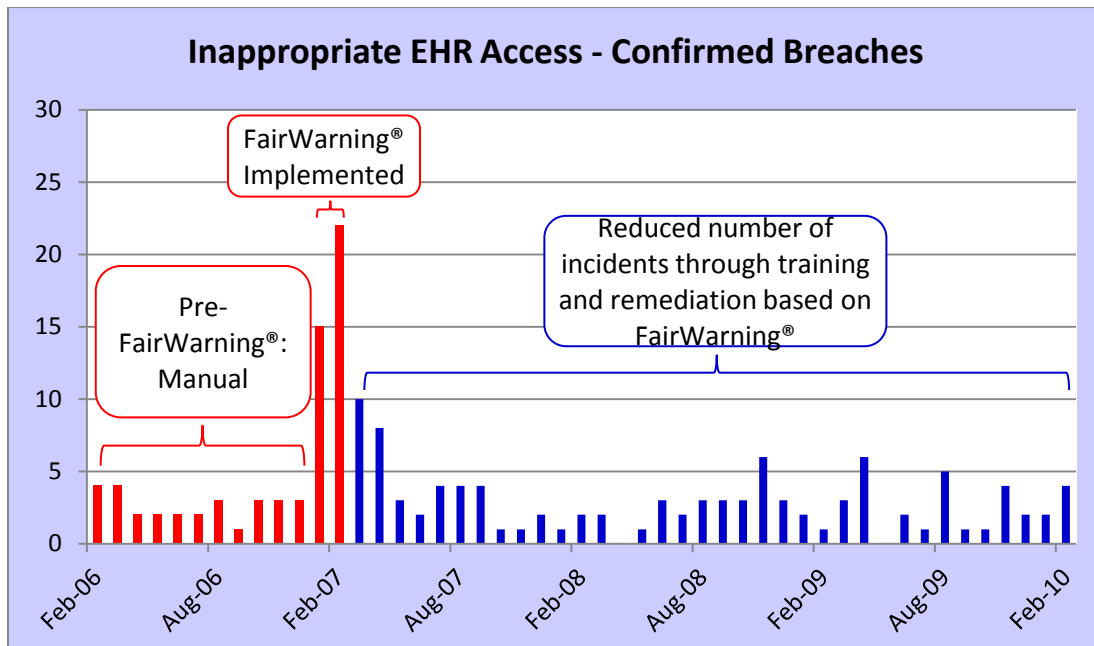


Figure 1. Incidents from Customer Study

After hospital staff received communication that privacy breach monitoring had been put in place and for the two-month period of March and April 2007, breach rates fell to between seven and 10 per month, an approximate 60 percent decrease.

Finally, a program of targeted awareness training combined with sanctioning follow-through with offenders was established and privacy breach rates reduced to less than five incidents per month and fell to as little as one per month. This represents an 85 to 95 percent reduction in privacy breach rates.

### FairWarning, Inc.

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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

## Privacy is an Ongoing Process, Not an Event

Using the analysis from [FairWarning®](#), the privacy officer was able to reprimand or remove repeated and egregious offenders. Secondly, departmental level training sessions were held on privacy and security awareness, **with analysis from [FairWarning®](#) used to reinforce the training.** The reader will see that over time, using privacy breach detection and training, **the insider incidents were driven out of this healthcare organization's environment.** Also obvious is that during the period of time without automated privacy breach detection this organization was suffering from dramatically more insider incidents than they knew. This represents risk to the patients and the institution. As this privacy team was freed up from the tedious tasks of incident investigation and manual audit log reviews, they were able to work on other security initiatives.

## How Long Does Privacy Breach Detection Take to Deploy?

Based on reference-able customer deployments, privacy breach detection solutions from [FairWarning®](#) can provide first productive use within three months, obviously, very large and sophisticated deployments can take longer. However, even these large projects can be phased to provide rapid use. According to Gartner's Barry Runyon, Research Vice President and Healthcare Analyst, "This [privacy breach detection] is the low hanging fruit of [HIPAA](#) security rule safeguards. Without the proper technical controls like system auditing, personal healthcare information (PHI) can be put at risk".

FairWarning's privacy breach detection technology leverages existing interfaces for every major healthcare application including: McKesson, Cerner, Eclipsys, Epic Systems, GE, MEDITECH, Siemens, as well as dozens of others. [FairWarning®](#) has worked with hundreds of healthcare organizations to identify privacy scenarios that run "out-of-the-box" once the audit data is provided. This means that healthcare Information Technology personnel simply coordinate with [FairWarning®](#) to identify and access the audit sources, [FairWarning®](#) does the rest.

***The combination of addressing insider incidents, rapid deployment times and pricing designed for healthcare makes privacy breach detection the "low hanging fruit of privacy and compliance."***

## Compliance Considerations

### ARRA HITECH and HIPAA

[FairWarning®](#) privacy breach detection customers (some of whom have been audited for HIPAA by the United States Federal Government) consistently assert that without privacy breach detection they would be non-compliant with key portions of [HITECH and HIPAA](#) specifically with the mandates to:

- Systematically review and audit systems that access Protected Health Information

### FairWarning, Inc.

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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

- Mitigate damages when there is reason to believe a patient privacy incident has occurred
- Take preventive measures against reasonably anticipated patient privacy incidents

## **State Laws**

State laws expanding patient privacy are being adopted rapidly and every privacy and compliance professional should make themselves aware of the specifics for their respective state. California has taken a leadership position on this topic and has not only expanded disclosure law CA SB 1386 to include healthcare institutions, Governor Schwarzenegger has endorsed state laws AB 211 and SB 541 which impose financial penalties for violations of patient confidentiality.

Texas, Massachusetts, and other states have enacted similar legislation.

## **Federal Trade Commission**

At the time of this writing, the FTC is reported to have verbally committed that healthcare organizations will be subject to identity theft FTC regulations. As we know, most identity theft scenarios in healthcare are perpetrated by insiders.

The Federal Trade Commission has issued Final Rules regarding actions specific to policies and procedures surrounding monitoring of internal ‘red flags’ and activities that may signal identity theft. The final rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

1. Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks from identity theft.

### **FairWarning, Inc.**

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

Page | 8

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

## Summary of FairWarning® Privacy Breach Detection

Privacy breach detection is being rapidly adopted at leading healthcare organizations to protect their institutions and patients against damaging insider incidents that are now so common in the headlines. Privacy breach detection automatically, centrally and non-intrusively reviews and audits usage patterns in EHRs to identify snooping, identity theft, medical identity theft as well as non-compliance issues. Privacy breach detection provides the privacy and compliance office with a suite of tools to adequately perform their responsibilities. Privacy breach detection was built to dovetail with existing privacy processes and leverages the best practices of many healthcare organizations. By automating intensely manual processes, privacy breach detection provides an extremely positive return on investment (ROI) and is more affordable and much faster to deploy than security technology such as identity management and provisioning. The laundry list of existing security technologies such as encryption, single sign on, SIM and identity management do little to address insider incidents as demonstrated by on-going privacy and compliance incidents. Lastly, privacy breach detection addresses the core [HITECH and HIPAA](#) requirements of systemically reviewing and auditing all systems which access protected health information.

**For more information on privacy breach detection solutions from FairWarning®, e-mail [solutions@FairWarningAudit.com](mailto:solutions@FairWarningAudit.com) or contact us using the information below.**

### **FairWarning, Inc.**

Email: [solutions@FairWarning.com](mailto:solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

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