

Privacy Breach Benchmarks Compel Care Providers to Deploy Breach Monitoring and Commit to a Culture of Privacy and Compliance

Leading healthcare providers have documented dramatically reduced risk and exposure to privacy breaches by deploying breach monitoring, benchmarking breach rates then eliminating breaches through awareness training, sanctioning and risk assessment.

[A FairWarning® White Paper](#)

[Trust but verify®](#)

Executive Summary

Patient privacy breaches resulting from the misuse of access to electronic health records (EHRs) are empirically shown to be systemic and more voluminous than commonly reported. Routinely detected patient privacy breaches range from curiosity based snooping as seen in the media, to life-altering cases involving fraud, identity theft, criminal activities and abuses of all kinds.

Many care providers are unaware that breaches are prevalent but do recognize breaches carry significant risks. The Institute of Medicine¹ notes in its recent publication related to privacy: “breaches of an individual’s privacy and confidentiality may affect a person’s dignity and cause irreparable harm” and “[unauthorized disclosures] can result in stigma, embarrassment, and discrimination.” Further, care providers are aware that breaches can now carry severe institutional financial, reputational and legal ramifications. Based on statistical evidence, providers without privacy breach monitoring to track and thwart unauthorized access are likely to have at least 25 to 100 privacy breaches per month. Although, providers who deploy privacy breach monitoring coupled with employee training, breach remediation and enforced sanctions, experience a 85 to 99 percent decrease in privacy breach occurrences depending on the effectiveness of their programs.

Simply put, leading care providers have empirically proven they reduce their risk and exposure to patient privacy breaches through the deployment of privacy breach monitoring technology and refinement of awareness training, remediation, sanctioning processes, and risk assessments. The statistics and anecdotes contained in this white paper were provided to FairWarning® by its customers for anonymous use.

¹ Institute of Medicine, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research, February 4, 2009, <http://www.nap.edu/catalog/12458.html>

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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.

MATERIAL FOR USE "AS-IS"

THIS FAIRWARNING® REPORT IS FURNISHED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND AND FAIRWARNING® HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES AS TO NON-INFRINGEMENT, AND IN NO EVENT SHALL FAIRWARNING® BE LIABLE FOR COSTS PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL FAIRWARNING® BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR DAMAGES WHETHER OR NOT FAIRWARNING® HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Industry Perspectives

FairWarning® Privacy Breach and Best Practice Findings Report

"Security and privacy breaches threaten to undermine the public's trust in health IT and electronic health information exchange, just at a time when policymakers are actively promoting it. This report demonstrates that implementation of industry best practices reduces the risk of breach and is key to enabling more widespread adoption and use of e-health technologies."

Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology

"Historically, healthcare providers have relied on intensive and manual procedures to monitor for breaches. As a result, many of these entities are unaware of the actual number of breaches within their organizations and therefore unable to report or thwart these breaches. What should be eye-opening for these organizations that do not have a reliable automated monitoring process, is the vast financial and reputational risk posed by any one of these breaches."

Cliff Baker, VP & Chief Strategy Officer, HITRUST Alliance LLC

"For the first time in this industry, there is data that quantifies the risk of not proactively and systematically monitoring for breaches. More importantly, this report proves that policy without enforcement doesn't work and creates entity-wide risk through empirical data. For EHRs to be successful and secure public trust, the industry as a whole must commit to establishing ongoing breach monitoring, an environment of informed compliance and effective risk mitigation."

Mac McMillan, Chair, HIMSS Privacy & Security Steering Committee, CEO, CynergisTek

FairWarning® Patient Privacy Framework

"Data definitions for EHR enterprise and departmental system audit logs will prove to be very useful to healthcare providers seeking to normalize and automate their response to HITECH's privacy auditing requirements surrounding protected health information (PHI) and consultants and vendors looking to assist them. The [FairWarning® Patient Privacy Framework] guides should increase their understanding of the sources and structure of the PHI."

Barry Runyon, Research Vice President Healthcare Providers, Gartner, Inc.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Lessons Learned from Patient Privacy Breaches in EHRs

The privacy breach statistics, examples and anecdotes referenced in this white paper are derived from FairWarning® privacy breach monitoring experiences with customers representing more than 300 hospitals and 1,400 clinics.

High level findings from privacy breach monitoring deployments include:

- **Breaches are global phenomena.** Without exception, patient privacy breaches resulting from the misuse of access to EHRs are systemic and occurring in large volumes regardless of provider size, geography, primary clinical system or specialty. This white paper includes benchmark data detailing the number of confirmed breaches when privacy breach monitoring is implemented, as well as once the deployment is in full use.
- **Leading care providers are reducing breach occurrences.** Care providers are experiencing between 85 and 99 percent reduction in breaches and dramatic improvements to patient privacy and institutional compliance by weaving privacy breach monitoring results into the fabric of their training, awareness, sanctioning, and risk assessment programs.
- **Privacy breach monitoring must be supported by training, sanctioning programs and on-going risk assessment.** Care providers must be prepared to follow through with targeted training and sanctions involving valued employees, contractors, and consultants, including physicians. Consistency in sanctioning is critical. A provider must be willing to take action against offenders including physicians who provide a substantial patient draw to the organization because of their specialty and reputation. On a continual basis, privacy and compliance should collaborate with information security to reduce risk exposure and close vulnerability gaps detected by privacy breach monitoring.
- **Care providers without privacy breach detection experience continued risk exposure.** Based on the prevalence of systemic privacy breaches, care providers without adequate privacy breach detection capabilities and related processes in place

Patient privacy breaches resulting from the misuse of EHRs are systemic and are occurring in large volumes regardless of provider size, geography, primary clinical system or specialty.

Leading care providers have empirically proven to reduce their risk and exposure to patient privacy breaches through the deployment of privacy breach monitoring technology and refinement of awareness training, remediation and sanctioning processes.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

are detecting only a very small fraction of patient privacy breaches. Reported privacy breaches constitute an even smaller fraction of breaches actually detected.

Explosion of Regulatory Changes in Healthcare

Between April 2003 and July 2010, Health and Human Services (HHS), Office of Civil Rights (OCR) has investigated, found substantial claims and resolved more than 11,421 cases of privacy violations under HIPAA among healthcare covered entities. In February 2009, the HITECH Act's Section 13402(e)(4) further raised the stakes for an organization with a breach affecting 500 or more individuals. Under law, the organization is required to report the breach to the HHS Secretary, the media and the patients affected. The Secretary of HHS posts an online list of the breaches of unsecured protected health information with a summary of the breach. Since the Interim Final Rule for Breach Notification for Unsecured Protected Health Information became effective on September 29, 2009, HHS has posted 153 breaches of unsecured protected health information (PHI). Collectively, these breaches affected more than 4,847,414 individuals. Of these, 12.4 % were a result of unauthorized access to PHI.

***Since September 29, 2009
HHS Office of the Secretary
has posted 153 breaches,
collectively affecting more
than 4.8 million individuals.***

Several US states have also instituted tough laws making it unlawful to electronically access patient information unless it is in the course of care. January 1, 2009, California's AB 211 law went into effect requiring such protections of PHI and the report of violations to the California Department of Public Health and affected individuals. From January 2009 through May 2010, 3,766 breaches have been reported. 1,953 of these incidents have been investigated, and of these, 98.7% were found to be 'substantiated medical breaches.' Of the breaches categorized as "malicious", 50 percent were perpetrated by healthcare workers.²

***50% of reported
"malicious" privacy
breaches in California
were perpetrated by
healthcare workers.***

In April of 2010, the UK Information Commissioner's Office enacted fines of up to £500,000 for significant data breaches. Between November 2007 and May 2010, there were 287 serious data loss breaches within the UK National Health Service (NHS).

² Dom Nicastro, for HealthLeaders Media, August 26, 2010, With No Harm Threshold, Nearly All Breaches Substantiated in CA, <http://www.healthleadersmedia.com/print/TEC-255666/With-No-Harm-Threshold-Nearly-All-Breaches-Substantiated-in-CA>

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Privacy Breach Benchmarks: Measuring for Success

Healthcare privacy officers report that today's point-and-click society has emboldened EHR users with a sense of entitlement. There is a strong sense that if they can access patient information, then they have every right to do so regardless of whether they are involved in that patient's care. Privacy officers point out that these same users would never walk into physical storage and open the medical file of a patient unless it was related to care, yet in the electronic world, they do so routinely.

Privacy officers describe breaches that are reported through patients, employees or external sources as the tip of the iceberg. They report that when a privacy breach is discovered, their investigation reveals a larger more systemic problem, which is the ultimate motivator for deploying privacy breach monitoring technology.

As care providers globally begin to elevate privacy and security in their list of priorities, they are looking to leading institutions who have already implemented patient privacy monitoring and breach detection for empirical data to support their privacy and security purchases and educational initiatives.

When a privacy breach is manually discovered, the investigation reveals a larger more systemic problem which is the ultimate motivator for deploying privacy breach monitoring technology.

As part of privacy breach monitoring deployments, it is recommended that the number of privacy breaches occurring per month is measured prior to incorporating the results into a full corporate communications and sanctioning plan. This establishes a baseline against which to gauge the effectiveness of the privacy breach deployment. Benchmarking is a critical component of a deployment for several reasons:

- Enabling the organization to identify the types of breaches that are occurring and breach trends including individual offenders
- Benchmarking demonstrates the effectiveness or ineffectiveness of past training and sanctioning programs
- Establishing corporate buy-in from key stakeholders including the C-suite, operations, risk management, IT and privacy officers by demonstrating existing risks to the organization

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Benchmarking Background

Care providers representing more than 300 hospitals and 1,400 clinics have deployed FairWarning® [privacy breach monitoring](#). Many of these institutions are industry leaders in patient care, with 52 percent having been recognized as Verispan 100, 100 Most Wired, or a U.S. News Best health system.

FairWarning® hospital system customers range widely in size from 500 employees to more than 50,000 employees. By bed count, hospital system customers range from a 140-bed stand-alone hospital to a 4,500-bed system representing 20 hospitals and several hundred facilities. On average, FairWarning® hospital system customers have 858 beds, and represent four hospitals and 1,061 physicians. 85 percent are based in the United States with the remaining 15 percent based in Canada and United Kingdom. FairWarning® also has mid and large size physician group customers and associated experiences are included in this report.

The cited hospitals and physician groups use clinical or healthcare related applications from every major healthcare vendor as well as specialty vendors and home-grown solutions. Case studies are available upon request.

Some health systems which are highlighted through example, statistic or anecdote in this white paper include:

- Metropolitan based Top 20 U.S. health system with over \$ 1 Billion in revenue
- Top 50 U.S. based health system comprising of multiple award-winning hospitals
- Premier U.S. based physician-owned practice with over twenty clinics
- Small hospital of under 200 beds located in a rural northwest U.S. community
- Small hospital of under 300 beds located in a rural southeast U.S. community
- Very large health system with premier teaching hospital operating across multiple U.S. states
- Large government operated health system located in the United Kingdom
- Very large government operated health systems located in Canada

These leading care providers were deploying privacy breach monitoring well in advance of the ground-breaking ARRA HITECH of 2009 which increased penalties for allowing patient privacy breaches to continue undetected and unreported. Many of these privacy breach monitoring deployments have now been in production for three or more years. As a result, FairWarning® has amassed a solid base of experiences on patient privacy breaches through the misuse of access to EHRs.

This white paper details some of the lessons learned and what leading healthcare providers are doing to protect patient privacy, comply with a heightened regulatory environment, reduce the risk of damages, achieve meaningful use and build further confidence in their EHR expansion.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 7

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

Benchmarking Occurrences of Patient Privacy Breaches

Privacy Breach Baselines

Breach occurrences per month from four representative privacy breach monitoring case studies are provided in Table 1. These four case studies are covered in detail within this white paper.

Health System Description	Number of confirmed monthly breaches at outset of FairWarning® deployment
200-bed hospital with a few small clinics – Rurally based	24 confirmed incidents per month
U.S. based physician practice with 20 clinics metro and rurally dispersed	29 confirmed incidents per month
UK based teaching hospital in major metropolitan area as well as rurally based facilities	130 confirmed incidents per month
Top 50 U.S. Health System with multiple affiliated hospitals and clinics – Based in a major metropolitan area	125 confirmed incidents per month

Table 1. Example Privacy Breach Benchmark Measures

The exact number of confirmed breaches for a given health system varies widely depending on the number of healthcare applications monitored, and the types of privacy breach detection being performed.

Typically, larger health systems initially monitor for fewer but more common types of privacy breach across critical clinical applications. Over time, these larger health systems typically expand monitoring to additional applications and types of privacy breaches.

Smaller care providers are able to monitor more aggressively for privacy breaches of all types since their environments and associated volumes tend to be more manageable.

FairWarning® customers increasingly ask for assistance in planning corporate communications, remediation and reporting activities in conjunction with their privacy breach monitoring deployments. This combination enables care providers to effectively decrease the number of privacy breaches occurring in their organizations without inundating privacy and compliance staff members with extra work.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

General Categories

In this initial publication of results, generalizations are provided which show that some types of privacy breaches occur systemically regardless of location, whereas other types are highly dependent on whether the care provider is primarily based in a metropolitan or rural area. In future publications of findings FairWarning® will detail by percentage the types of privacy breaches with further break down by locality.

Care Provider Locality (Metropolitan / Rural)	Examples of Privacy Breaches
All care providers regardless of locality	<ul style="list-style-type: none"> • Care provider employees visiting as a patient • Immediate Family member snooping • Child custody cases • Criminal suspects covered in media • Billing and fraud related
Rurally based care providers	<ul style="list-style-type: none"> • Local government official snooping • Neighbor snooping • Extended family member snooping
Metropolitan based care providers	<ul style="list-style-type: none"> • Sports star snooping • Federal or state government official snooping • High profile business personality snooping • High profile celebrity/media personality snooping • Traditional identity theft • Medical identity theft

Table 2. Privacy breach categories by locality

Privacy Breach Anecdotes

Firsthand anecdotes provide insights on how patient privacy breaches underlie fraudulent, criminal or nefarious behaviors:

- Employee of a premier specialty hospital owned an assisted living facility as a side business and was mining patients from their EHR account to feed his own business
- Major physician practice in which a valued senior physician hired several low-paid junior physicians to enter notes in the senior physician's name resulting in billing fraud
- Many locations and incidents involving sports star snooping (football, baseball, soccer, basketball) particularly during media coverage immediately before or after major games, most common in the metropolitan area where the sports team is based
- Major teaching hospital involved in a homicide investigation in which law enforcement requested audit trail of suspected coconspirators who were employees of health system and examining soon to be deceased victim through electronic health record system
- Multiple reports from metropolitan and rural based care providers detecting staff using EHR access to systematically steal the identities of deceased patients to commit financial identity theft
- Staff members of metropolitan health system using pharmacy dispensing system to self-prescribe oxycodone
- Thousands of occurrences of family member snooping, self examination, employee as patient, and general VIP snooping. Career gain, child custody, blackmail, lawsuits as well as general curiosity are reported as motivations during the remediation process

Four Representative Case Studies of Baseline Privacy Breach Levels

In the majority of healthcare organizations, care providers and employees are unaware that their EHR activities are or will be monitored. The privacy breach rates in Figures 1 through 4 detail the number of confirmed breaches detected by privacy breach monitoring prior to fully communicating to the care provider staff that their EHR activities were being monitored. Evidence suggests that privacy breach rates decrease only when the care provider incorporates the results into awareness training and follows through with sanctions against offending parties.

Privacy breaches detailed in the graphs are actual confirmed breaches. These breaches are represented in red. Any false positives were filtered out through the privacy breach monitoring technology or through a follow-on investigation by the privacy staff of the care provider.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 10

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

Case 1: U.S. Top 50 Large Metro Based Multi-Hospital System

In this case no historical data regarding privacy breach rates were available prior to the deployment of automated breach monitoring technology.

Initial rates of confirmed privacy breaches once breach monitoring was deployed ranged between 115 and 120 privacy breaches per month. No initial communication to the staff was given that breach monitoring was in place, represented by February 2008 through April 2008 in Figure 1.

In May 2008, staff members received communications that privacy breach monitoring had been put in place and breach rates dropped to between 75 and 80 breaches per month represented by May 2008 through August 2008 in Figure 1, this represents a 36 percent reduction.

In September 2008, the privacy office began a program of individualized and directed communications with follow-on sanctions to offending staff members and privacy breach rates dropped to 1 to 2 per month which represents a 99.2 % reduction in privacy breach rates.

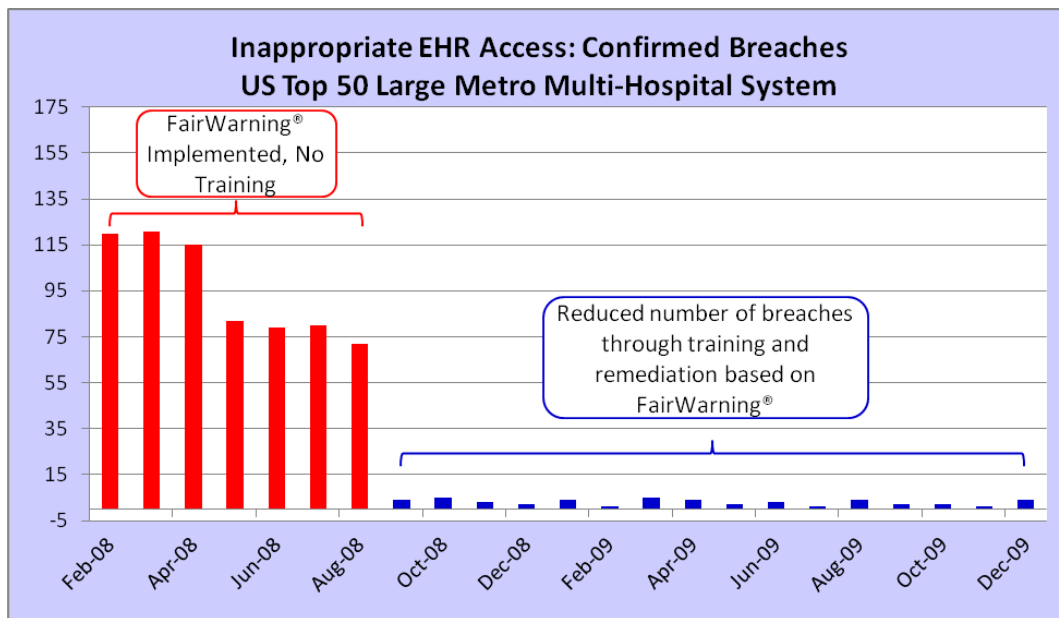


Figure 1. Privacy Breach Rates of U.S. Top 50 Metro Based Health System

This precipitous reduction occurred only when privacy breach monitoring was combined with awareness training and directed sanctioning against offending parties.

Further, this care provider fully recognizes there are likely other types of undetected breaches occurring in their environment and the 99.2 % decline is only for breaches types which are monitored. This health system plans to continue to identify the highest impact privacy breaches and initiate an expanded monitoring program.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 11

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

Case 2: 200 Bed, Rurally Based Hospital with Remote Clinics

In this case, historical data documenting privacy breaches detected by manual processes is reflected in Figure 2 by the months February 2006 to January 2007. During this time an employee was dedicated to reviewing audit logs, and was finding two to three privacy breaches per month.

In February 2007, automated privacy breach monitoring was deployed and for a period of 60 days no communication was sent. During this time 38 confirmed privacy breaches were detected, an approximate six-fold increase over breaches detected by manual methods.

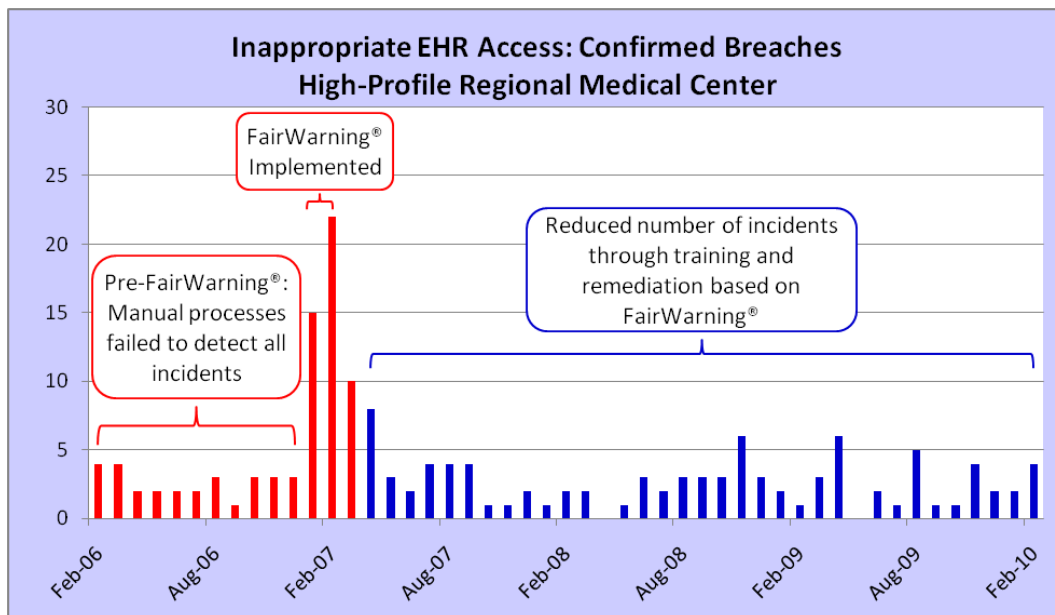


Figure 2. Privacy Breach Rates of U.S. Based Two Hundred (200) Bed Hospital

In late March 2007, 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.

In June 2007, a program of targeted awareness training combined with sanctioning follow-through with offenders was established and privacy breach rates reduced to less than five breaches per month and fell to as little as one per month. This represents an 85 to 95 percent reduction in privacy breach rates.

Over the next 18 months, periodic spikes in privacy breach rates are observed. This represents the monthly on-boarding of new employees or the addition of a new facility to the health system, with additional employees to be trained. Generally speaking, privacy breaches continue to spike when there is addition of new staff, new applications being monitored, and/or a high-profile patient checks into the hospital.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Case 3: Midsized Multi-Clinic System

In the first two months after privacy breach monitoring was implemented, this midsized multi-clinic system was experiencing 27 to 29 breaches per month. A corporate communications plan was established alerting employees that a privacy breach monitoring solution would assist the organization in uncovering any unauthorized access to patient records. A communications campaign was rolled-out and reiterated in April and May.

During these two months, the organization experienced a 66 percent reduction in the number of breaches, down to an average of eight per month.

For the months of June, July and August, the organization instituted and carried out remediation efforts, further reducing the number of breaches down to an average of two incidents per month, or an additional 24 percent reduction. This represents a total reduction of approximately 95 % in privacy breaches from the baseline occurrences.

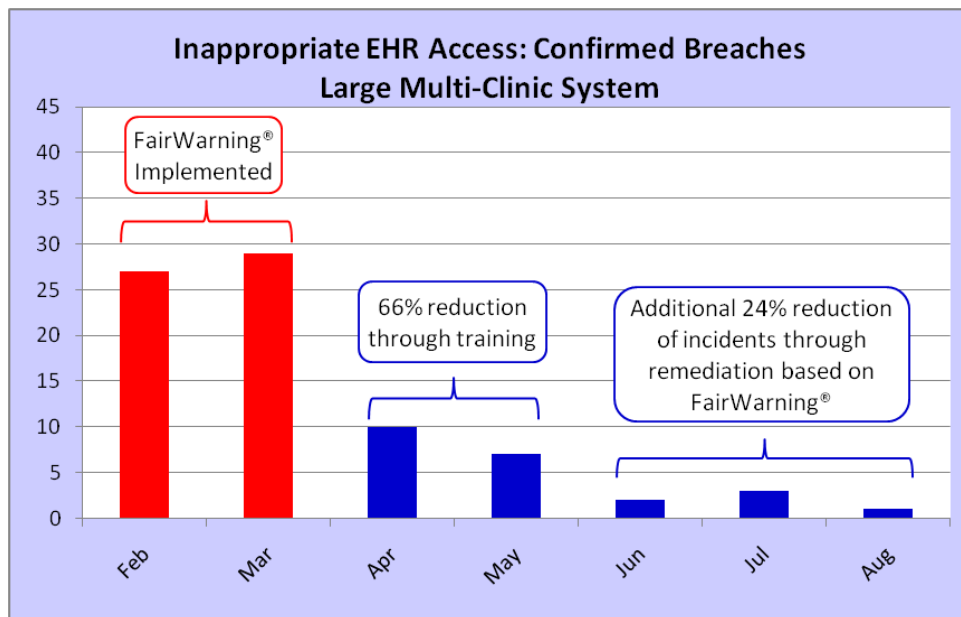


Figure 3. Midsized Multi-Clinic System

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 13

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

Case 4: Large UK Based NHS Teaching Hospital in Major Metro with Outlying Clinics

This large teaching hospital experienced a series of privacy breaches over a short period of time which forced manual investigations. The privacy and information security staff discovered further breaches with each investigation. While the staff had no historical empirical data, they believed they were seeing only the tip of the iceberg in privacy breaches. Thus, they elected to deploy automated privacy breach monitoring.

The initial reports generated from the FairWarning® deployment revealed an average of 130 privacy breaches per month. After the NHS hospital began a corporate communications plan on privacy breach monitoring, a steady decline in privacy breaches occurred.

However, after several months of the corporate communications, the hospital began to see diminishing returns in terms of the reduction of privacy breaches.

In June 2010, the hospital initiated targeted sanctions and reprimands. The result was an overall 77 percent reduction in the number of monthly breaches. Further reductions are expected as the hospital continues its sanctioning program.

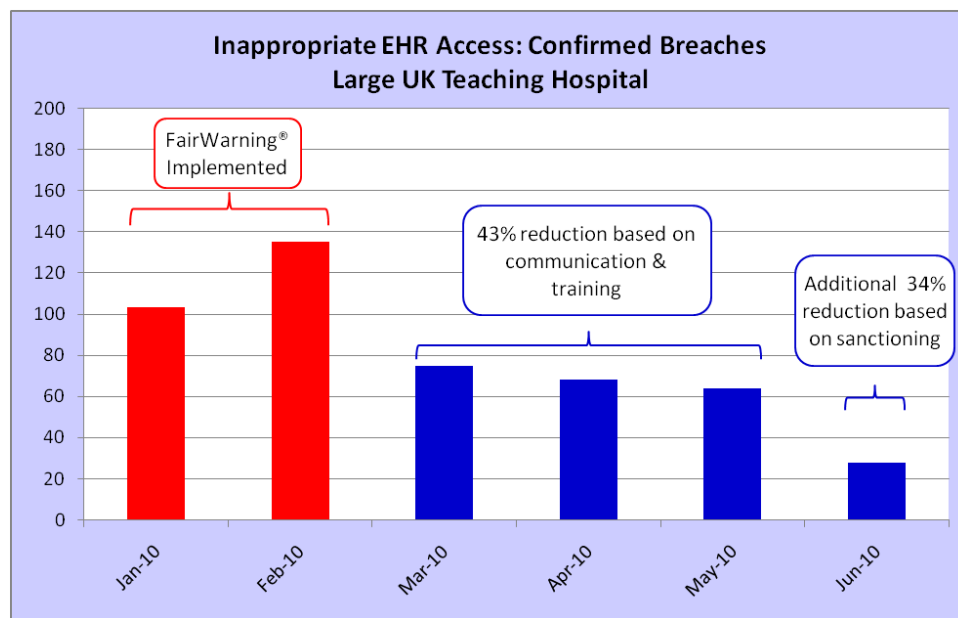


Figure 4. Privacy Breach Rates of Large UK Based Teaching Hospital

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 14

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

The Risk and Potential Damages of Inaction

Care providers who do not address their regulatory responsibilities of detecting, mitigating and appropriately reporting patient privacy breaches have new and growing risk considerations. New patient privacy laws now carry fines, executive exposure, patient disclosure, media notification, lost productivity, reputational damages, compliance reviews (audits), as well as long term resolution agreements or consent decrees with the Federal government.

Estimating Damages of a Visible Privacy Incident

Historically, many care providers have not prioritized privacy and security on par with facility expansion and other financial investments. Industry sentiment has been “why invest in privacy and security when associated regulation such as HIPAA is not enforced and has no teeth?”

However, [ARRA HITECH of 2009](#) as well as newly enacted or modified state healthcare privacy laws have significantly escalated the potential damages resulting from patient privacy breaches.

Based on firsthand experiences with its customers, the FairWarning® **Privacy Incident Damages Estimator** (available by emailing: Solutions@FairWarningAudit.com) takes into consideration newly enacted legislature. This estimator is freely available and has been vetted with customers as well as other constituents who have experienced firsthand a privacy incident that resulted in unwanted media attention, as well as a governmental audit (Compliance Review) and Resolution Agreement.

Escalation of Damages Resulting from a High-Profile Patient Privacy Incident

Damages resulting from a high-profile patient privacy incident escalate in accordance with a care provider’s legal responsibility to promptly respond to a suspected incident, mitigate the potential damages, disclose the incident to the patients involved, sanction employees and report the incident to the federal government and media. The Department of Health and Human Services Office of Civil Rights has made it clear that high-profile privacy breaches will most likely result in a Compliance Review and if the care provider is found willfully negligent, a Resolution Agreement may be required. According to interviews conducted with care providers who have experienced high-profile incidents, if the care provider is found grossly negligent, the FTC may also get involved.

The damages estimate summary below is based on a patient privacy incident which receives media attention and escalates into a Compliance Review and into a three year Resolution Agreement. These estimated damages were developed with the help of care providers and vested entities with firsthand experience with similar incidents. A general discussion of the damages and their escalation follows.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 15

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

Damage Category	Dollar Impact
Forensic investigation	\$ 517,000
Corporate Incident Management	\$ 309,000
Employee dismissal, rehiring and training	\$ 308,000
Patient disclosure and credit monitoring services	\$ 13,000
Federal and state fines	\$ 1,500,000
Federal Audit Management Time ("Compliance Review")	\$ 1,069,000
Federal Resolution Management Time ("Resolution Agreement")	\$ 4,389,000
Reputational Damage	\$ 0 to \$ 9,000,000
Total	\$ 8,105,000 to \$ 17,105,000

Table 3. Example Damages from High Profile Patient Privacy Incident

Additional detailed materials on privacy incident damages can be downloaded without registration from:

<http://www.fairwarningaudit.com/documents/2010-FAIRWARNING-DAMAGES-WEBINAR.pdf>

Forensic Investigation

An investigation can easily result in thousands of hours of productivity loss and directly impacts the information security, privacy teams, EHR vendors, IT and other consultants. The privacy and information security teams of care providers bear the burden of researching by whatever means available a privacy incident. These may have been discovered by an employee, reported by a patient or disclosed in the media. When the misuse of access to a patient's electronic health record is involved, this means investigating audit logs from the past. If there are no automated tools in place, this is a manual process that can take as little as a day or as much as six months to complete. The impact of a forensic investigation escalates with the number of patients, users and medical record systems involved. Additionally, to validate and assist in the investigation of a high profile patient privacy incident forensic specialists will likely become necessary.

In July 2010, after an unencrypted hard drive containing 27.7 million pages of medical records was either lost or stolen, Health Net was fined \$250,000 and entered into a Corrective Action Plan that requires, among other things, improved employee training, a variety of technologies for the protection of PHI, and submission of status reports for at least six years. Health Net described its costs to investigate the incident as exceeding \$7 million, not including the costs to implement the Corrective Action Plan

Corporate Management

Visible patient privacy breaches require hundreds of hours of attention from corporate management including: the most senior executive leadership, internal legal counsel, internal public relations, compliance, audit, privacy, information security, HIM and IT leadership. For a

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

newly discovered high profile patient privacy incident, there is a period of weeks in which team members, including executive leadership may spend as much as 30 to 50 percent of their time. Once the incident has been understood and initially evaluated, the privacy incident status remains on the weekly agenda of the team, usually for a period of several months.

Employee Dismissal and Replacement

High profile patient privacy incidents often results in dismissal of staff involved with an egregious incident. Generally dismissals involve as few as one employee and as many as several dozen. The cost of hiring temporary workers, recruiting and hiring permanent replacements as well as training replacements is modeled into the estimate.

Patient Notification and Credit Monitoring

New federal guidelines under ARRA HITECH require patient disclosure for all privacy breaches and media notification for breaches which involve 500 or more patients. The expenses associated with patient disclosure escalate directly with the number of patients involved. As a risk-mitigating precaution, care providers suffering from a visible privacy incident offer credit monitoring services to patients involved. The expenses associated with disclosure and credit monitoring are well established and modeled into the damages estimator.

Fines

Famously, ARRA HITECH escalates the fines associated with HIPAA non-compliance. Under HIPAA, the maximum yearly fine was \$250,000. Under HITECH, the maximum annual fine *per violation category* is \$1.5 million. This means that an entity could potentially be fined up to the maximum \$1.5 million several times in a given year, for different categories of violation.³

Violation Category	Fine Per Violation	Maximum Fine Per Year
Did Not Know	\$100 - \$50,000	\$1,500,000
Reasonable Cause	\$1,000 - \$50,000	\$1,500,000
Willful Neglect, Corrected	\$10,000 - \$50,000	\$1,500,000
Willful Neglect, Not Corrected	\$50,000	\$1,500,000

States such as California with AB 211 and SB 541 have levied significant financial penalties against care providers associated with patient privacy breaches. AB 211 and SB 541 imposed fines of up to \$25,000 per patient affected, as well as \$100 per day that an incident goes unreported.

Additionally, under ARRA HITECH, state Attorney General's offices can bring suit against the offending care provider resulting in further financial penalty. In July 2010, the Connecticut Attorney General's office became the first to enforce HIPAA violations. In the Health Net incident referenced above, the state Attorney General assessed a fine of \$250,000.

³ <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf>

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

HHS Compliance Review

The U.S. Department of Health and Human Services, Office of Civil Rights has publically stated that care providers involved in major patient privacy incidents are likely to be subject to a Compliance Review which amounts to a privacy and security HIPAA audit. The lost productivity of staff and hard consulting and legal expenses associated with a compliance review escalate. Senior executive management, compliance, audit, legal as well as information security and privacy are all impacted. As a Compliance Review is conducted it becomes increasingly likely that external legal counsel will be required to reach a settlement. It is reported that the expense of legal counsel alone may reach \$1 million.

As follow-on to the Compliance Review the care provider is now responsible for demonstrating that the privacy and security gaps identified and have been addressed. This results in additional hard-cost expense of deploying appropriate technologies as well as the productivity loss of the continuing Compliance review. These technologies may include but are not limited to encryption, data leakage protection and identity management.

HHS Resolution Agreement

Based on the level of willful neglect found in care providers' practices, the Office of Civil Rights uses a tool referred to as a Resolution Agreement. In a Resolution Agreement, the care provider pays a settlement fee and agrees to have its practices reviewed periodically by the federal government over a multi-year time period. Additionally, a Resolution Agreement will likely include a significant revamp and redesign of privacy and security practices and training. Senior executive management, compliance, audit, legal as well as information security and privacy resources are all impacted. In negotiating the Resolution Agreement with the federal government, it is reported that the expense of external legal counsel reaches into the multi-millions of dollars. Additionally, the productivity loss of fulfilling the Resolution Agreement reaches into the millions.

The [UK Information Commissioner's Office](#) lists 128 investigations and enforcement notices, requiring similar actions to the HHS Resolution Agreements.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 18

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

Examples of High Profile Privacy Incidents⁴

Health Net Fined by Connecticut Attorney General

- In July 2010, the Connecticut Attorney General's office became the first to enforce HIPAA violations since HITECH authorized independent enforcement at the state level. After a portable hard drive containing 27.7 million pages of PHI was lost, Health Net was fined \$250,000 and entered into a Corrective Action Plan that requires, among other things, improved employee training, a variety of technologies for the protection of PHI, and submission of status reports for at least six years. Health Net described its costs to investigate the incident as exceeding \$7 million.

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 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.

Rite Aid Resolution Agreement and FTC Consent Decree

- In June 2010, after the media discovered inappropriate disposal of personal health information in dumpsters, Rite Aid was investigated and ultimately paid a \$1 million settlement for HIPAA privacy violations. Under the Resolution Agreement, Rite Aid must strengthen policies and procedures, improve training, internal monitoring, and sanctioning. Rite Aid also settled with the FTC for violations of the FTC Act.

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, including tabloids offering employees cash payouts to provide Woods' medical records. Several employees were terminated.

⁴ <http://www.phiprivacy.net>

University Medical Center in Las Vegas

- Between January and November 2009, UMC employee Richard W. Charette allegedly 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.

Kaiser Permanente in California

- In January 2009, Nadya Suleman (Octomom) checked into Bellflower Medical Center and gave birth to octuplets. 21 employees and 2 doctors inappropriately accessed her records. In all, 15 employees were fired, and 8 were sanctioned. Kaiser Permanente was fined \$250,000, the first fine under state privacy regulations AB 541 and SB 211.

CVS Pharmacy Resolution Agreement

- In January 2009, CVS Pharmacy paid \$2.25 million in a HIPAA settlement after media revealed that patient information was being disposed of in dumpsters. Under the Resolution Agreement, CVS must strengthen disposal policies, sanction workers violating the policies, and improve training. They must also conduct monitoring and regularly provide reports to Health & Human Services for three years.

Providence Health & Services Resolution Agreement

- In July 2008, Providence Health & Services paid \$100,000 to settle HIPAA violations, and entered into a Resolution Agreement which requires training and appropriate safeguards for patient information. These were a result of data losses during 2005 and 2006 that included lost backup files and laptops.

New York – Presbyterian Hospital Identity Theft

- From 2006 through 2008, Dwight McPherson, an admissions employee at New York-Presbyterian Hospital in Manhattan, sold nearly 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.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 20

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

International Privacy Incidents

NHS in Yorkshire, England

- In September 2010, Dale Trever, a data quality manager for the NHS in Yorkshire, plead guilty to illegally accessing 431 women's records. He is awaiting sentencing.

University Health Network in Ontario, Canada

- In August 2010, CBC News reported that 763 patient files had been stolen. The Information and Privacy Commissioner is reviewing, and patients were notified.

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 former United Kingdom Prime Minister Gordon Brown, several BBC journalists, and others.

Finland

- In September 2010, the Helsinki Times reported that there have been 20 cases reported to the Office of Data Protection Ombudsman involving illegal access of personal health records and the cases are being investigated
- In July 2008, the European Court of Human Rights fined the Finnish government €34,000, after a hospital employee's HIV status became public knowledge.

FairWarning® Privacy Incident Damages Estimator

Taking into consideration the expenses detailed here, the FairWarning® **Privacy Incident Damages Estimator** enables healthcare organizations to financially estimate the potential cost of a reportable breach. The damages estimator was developed with the input of FairWarning® customers and constituents who have been involved firsthand with privacy incidents which have been reported to the media, HHS Compliance Reviews and HHS Resolution Agreements.

The Damages Estimator is available by emailing, Solutions@FairWarningAudit.com

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 21

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

Summary

Wide-scale inappropriate access to patient records is a potentially costly issue every care provider will need to address regardless of size or geographic location. As existing laws are enforced and additional privacy laws enacted, mandates will continue to require organizations to establish effective safeguards to eliminate the risks of patient privacy breaches. Governments both in the US and abroad continually demonstrate that enforcement of these laws is becoming a priority. As EHR adoption increases, privacy and security will continue to elevate on the priority list of legislators and enforcers.

Currently, as reported in the media and within FairWarning®'s benchmarking research, patient privacy breaches are wide-scale and rampant. A no action approach lands an organization squarely on a powder keg of exposure with well documented hard financial costs and significant reputational damages. Costs of a reportable breach can easily reach into the millions of dollars.

FairWarning®'s benchmarking research further demonstrates that care providers without a privacy breach monitoring solution will likely experience more than one reportable breach per year. Breach examples noted in this document reveal fines in excess of \$2.25 million, with internal breach management costs likely to range from \$6.5 million to \$15 million for a breach which receives media attention and escalates.

When weighing the cost of a breach solution against the potential cost and reputational damages of a reportable breach, it becomes apparent that the cost of a privacy breach monitoring solution is negligible when compared to the cost of a breach. Patient privacy breaches are preventable with moderately priced, off-the-shelf technology combined with well-understood refinements to care provider awareness training, incident remediation and sanctioning processes.

FairWarning® customers who have implemented patient privacy monitoring are experiencing an 85 to 99 percent reduction in privacy breaches. On average, this shift occurs within six months when coupled with effective privacy training and education, awareness and well-communicated sanctions. More importantly, through the implementation and use of a patient privacy breach detection and monitoring solution, healthcare leaders are able to significantly reduce institutional risk associated with reportable breaches.

Leading care providers have already implemented FairWarning® to:

FairWarning® customers who have implemented patient privacy monitoring are experiencing an 85 to 99 percent reduction in privacy breaches. On average, this shift occurs within six months when coupled with effective privacy training and education, awareness and well-communicated sanctions.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 22

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

- Automate privacy auditing reporting across all of their healthcare applications which access PHI
- Stamp out inappropriate access to patient records by automating the proactive detection of privacy breaches related to identity theft, medical identity theft, employee-patient snooping, as well as VIP, friends, family and neighbor snooping
- Streamline investigations of suspect activities
- Dramatically reduce and mitigate risks which result from the misuse of access to EHRs

Care providers today have an opportunity to leverage FairWarning®'s experience with more than 300 customers globally and its FairWarning® privacy breach detection and monitoring solution to create a culture of privacy and compliance which provides strong deterrents for privacy breaches.

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 | 23

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

Additional Resources

United States: ARRA HITECH Privacy Breach Reporting Web Site

Under HITECH, the Office of Civil Rights publishes a list of reported patient privacy breaches that affect 500 or more patients. The list is available at

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>

KLAS Research on Privacy Breach Monitoring

In June 2010, KLAS Research initiated customer research on FairWarning®, published its first FairWarning® and privacy breach monitoring results in July 2010. More information can be found at <http://www.klasresearch.com>.

Canada: Information & Privacy Commissioner of Alberta

For more information on recent amendments to Alberta's Health Information Act, and related regulations, please visit <http://www.oipc.ab.ca/pages/HIA/AboutAct.aspx>.

Canada: Information & Privacy Commissioner of Ontario, and Privacy by Design

For more information on Privacy by Design and the Ontario IPC, please visit <http://www.privacybydesign.ca/>.

United Kingdom: Information Commissioner's Office

More information on activities by the UK ICO can be found at http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com Page | 24

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