

Strategies for Maximizing the Impact of Your Healthcare Privacy Investments

Accounting of disclosure, privacy breach detection and notification are at the core of new healthcare regulations such as ARRA HITECH and the FTC Red Flags Rule

[A FairWarning® White Paper](#)

[Trust but verify®](#)

Overview

Motivated by patient-citizen damages from a pandemic of healthcare privacy breaches, lawmakers across the United States, Canada, United Kingdom, and Europe have enacted new regulation protecting patient privacy and penalizing those involved. Snooping, identity theft and general inappropriate access of medical records are now explicitly prohibited. Additionally, a patient's right to know who has accessed their records has been expanded. *The new breed of laws such as: ARRA HITECH privacy provisions, FTC Identity Theft Red Flags Rule, California Senate Bill 541 and Assembly Bill 211, Canadian Provincial Privacy Acts and the UK Freedom of Information Act specifically focus on expanded privacy issues such as anti-snooping, prevention of medical identity theft, accounting of disclosures, and a patient's right to know who has accessed their medical information.* In parallel, enforcement has increased at every governmental level. In the U.S., it is well documented that Federal enforcement of HIPAA has increased dramatically. The state of California has already levied fines for violations of brand-new anti-snooping laws, and the Information Commissioner's Office in the United Kingdom has announced a crackdown on NHS Trusts involved in privacy breaches. General security and privacy measures from past regulation such as HIPAA, PIPEDA and the EU Data Protection Directive are table-stakes and are expected to be in-place within healthcare entities.

Every entity maintaining or accessing patient information now faces multiple regulatory risks in an environment of increased enforcement. Healthcare entities should pursue technologies and processes that address multiple elements of new healthcare privacy laws, providing them with the greatest leverage for their compliance investment dollar.



FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Background

This white paper outlines core tenets of new U.S. Federal, local and global healthcare privacy regulations. The white paper goes on to outline how privacy breach detection addresses *multiple* regulatory responsibilities for healthcare entities depending on where the entity operates. Compliance with new healthcare privacy regulation is here to stay, thus; addressing multiple privacy regulations with leveraged investments is essential to ensuring sustainable and efficient compliance operations.

In the Summary section at the end of this white paper, a table by geography is provided which maps FairWarning's privacy breach detection solutions to the new healthcare privacy regulation.

The reader can find more information on new healthcare privacy laws by following the links below:

- U.S. ARRA HITECH privacy provisions, click [here](#)
- U.S. state disclosure laws (45 states), click [here](#)
- FTC Red Flags Rule, effective to healthcare, November 1, 2009 click [here](#)
- U.S. Whistle-Blower Lawsuit, click [here](#)
- California Senate Bill 541, Assembly Bill 211 click [here](#)
- Massachusetts Data Privacy, 201 CMR 17.00, effective January 1, 2010, click [here](#)
- Canadian Provincial Laws, click [here](#)
- Ontario's Freedom of Information and Protection of Privacy Act, click [here](#)
- UK Information Commissioner's Office, click [here](#)
- Less recent, but pertinent privacy laws include: [HIPAA](#), [PIPEDA](#), [UK Data Protection Act](#) and [European Union Data Protection Directive](#)

In a companion [privacy breach detection white paper](#), FairWarning® details why healthcare entities are so vulnerable to privacy breaches such as snooping and identity theft *even after they implement the "check-list" of security technologies such as encryption, authentication, security information management and access controls*. The [privacy breach detection white paper](#) offers insights on why additional privacy legislation was required to address the continued pandemic of healthcare privacy breaches. Additional FairWarning® materials map [privacy breach detection](#) to [ARRA HITECH / HIPAA](#), [FTC Red Flags Rule](#) and [UK / EU privacy laws](#).

Healthcare entities face new anti-snooping, accounting of disclosure, and patient rights to information laws. The new laws stipulate substantive fines for the institutions and individuals involved and further penalize willful neglect. In the U.S., Federal Whistle-Blower laws apply to the willful neglect of obligations to protect patient privacy, early cases are underway and may expose even greater non-compliance risks.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 2

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

Elements of the New Healthcare Privacy Laws

Past regulation such as the U.S.'s HIPAA focused on general privacy and security provisions which are now expected to be in-place. The new breed of privacy regulation such as: U.S. ARRA HITECH privacy provisions, California Senate Bill 541, Assembly Bill 211, Canadian Provincial Privacy Acts, and the UK Freedom of Information Act are specifically focused on:

- I) Detection, reporting and prevention of patient record snooping as well as medical identity theft
- II) Accounting of disclosure and a patient's rights to know who has accessed their medical records
- III) Breach disclosure and notification requirements
- IV) Increased enforcement and penalties

This white paper focuses on the benefits of compliance with the first three (3) elements of the new laws rather than the risks and consequences of the fourth.

The detection and prevention of inappropriate patient access, as well as the ability to rapidly report on who accessed a patient's records are essential to compliance with new healthcare privacy laws. Entities focused on patient privacy and regulatory compliance will be positioned to avoid the risks of increased enforcement, fines, patient lawsuits as well as the institutional damage of media exposure.

I. Detection, Reporting, Prevention of Patient Record Snooping and Identity Theft

U.S. ARRA HITECH defines privacy breach to explicitly include snooping by expanding the definition of breach. The term "breach" means 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 the information is disclosed would not reasonably have been able to retain such information.

ARRA HITECH also extended how "Business Associates" are covered by Federal privacy laws; thus, snooping is now explicitly prohibited within all entities which maintain or handle PHI.

An additional U.S. Federal consideration is the FTC Red Flags Rule which is effective for healthcare entities as of November 1, 2009. The FTC Red Flags Rule now holds healthcare providers responsible for the detection and prevention of identity theft related activities. As well documented by the U.S. Federal government and media, medical identity theft has become one of the fastest growing information crimes in the world and in most cases involves internal employees or contractors taking advantage of their access to medical records.

California SB 541 and AB 211 also explicitly prohibit medical record snooping and outline reporting and notification responsibilities as well as delineating significant fines. The California state government has already levied [significant fines](#) to entities violating these new laws which

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

went into effect January 1, 2009. A new state law in Massachusetts expands security and privacy requirements and goes into effect January 1, 2010. The [MA Data Privacy Act](#) specifically contains a computer and systems security requirement for "...the monitoring of systems for unauthorized use of or access to personal information". Additional states are expected to follow.

Across Canada, UK and Europe, medical snooping is covered under general country data protection acts. In the UK, hundreds of recent healthcare privacy breaches led to an [ICO Crackdown](#) on patient privacy within NHS Trusts. In [Canada](#) and [Finland](#), healthcare privacy breaches related to identity theft has led to stronger privacy enforcement.

Entities without privacy breach detection technologies and associated processes are fundamentally exposed to government enforcement, financial penalties, patient lawsuits, willful neglect provisions as well as media exposure.

Under new healthcare privacy regulation, inappropriate access to medical records such as snooping and activities related to medical identity theft are illegal. The new laws require the detection, reporting and prevention of inappropriate medical record access. Enforcement is increasing and fines have already occurred.

II. Accounting of Disclosure and a Patient's Rights to Know Who has Accessed their Medical Records

In parallel to new regulation which mandates greater privacy protection for patients, new legislation has been enacted by law-makers which provide patients expanded rights to know who has accessed their medical records.

ARRA HITECH" s Accounting of Disclosure provision provides a patient with the right to receive an Accounting of Disclosure of their medical records up to three (3) year prior to when their inquiry is made. Healthcare entities which have not invested in the technologies and processes to retain and review audit trails of systems which access protected health information are in non-compliance and will not be able to fulfill on their Accounting of Disclosure responsibilities.

Canadian provincial laws, UK Freedom of Information, and EU Data Protection Directives provide patients with similar disclosure rights.

New patient accounting of disclosure laws, mean healthcare entities must now rapidly assess who accessed a patient's records over a multi-year time period. Entities without an established repository for audit trails or with manual processes are sure to be non-compliant and overwhelmed by the most basic of their regulatory responsibilities.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

Page | 4

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

III. Breach Disclosure & Notification Requirements

The U.S., ARRA HITECH [specifies dramatic new responsibilities](#) for healthcare entities when they discover any privacy breach. *The new law defines “Discovery Date” and stipulates that notification will occur within sixty (60) days of the “Discovery Date”.* To ensure entities do not under-report, tiered financial penalties for willful neglect now apply. ARRA HITECH also contains a media and Federal government notification requirement. Additionally, there are now forty-five (45) [states with disclosure laws](#). Entities operating over multiple states are generally required to comply with Federal and multiple state disclosure laws.

The UK Information Commission Office (ICO) has required notification in the case of a privacy breach since 1998 and failure to notify the ICO is a [criminal offense](#). Due to an epidemic of UK privacy breaches in 2008 and 2009, the enforcement of this requirement has dramatically accelerated along with other [ICO enforcement activities](#).

In Canada, [Ontario’s Freedom of Information and Protection of Privacy Act](#) is far-reaching in its protection of patient privacy and has become a model for other provinces. New privacy laws applying to disclosure have been enacted on a [province by province basis](#).

New notification and breach disclosure laws mean healthcare entities must now rapidly assess how many and which patients have been impacted by a privacy breach. Entities performing assessments through manual efforts have found research time usually measures in months. ARRA HITECH disclosure laws as outlined above renders this approach obsolete.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

Summary

Depending on their scope of operations, healthcare entities are bound by multiple new healthcare privacy laws. [FairWarning® privacy breach detection](#) solutions address required privacy components of these new laws such as ARRA HITECH. Addressing components of multiple laws with a single investment maximizes the impact of a healthcare entity's compliance investment and provides for sustainable and efficient compliance operations. FairWarning® privacy breach detection identifies, reports on, and deters privacy breaches from ever occurring. Privacy breach detection consolidates healthcare application audit trails to analyze for patterns associated with snooping and medical identity theft. Privacy breach detection technologies and processes are leveraged to facilitate rapid Accounting of Disclosure and notification responses.

The table below provides a summary of legislation to which FairWarning®'s privacy breach detection solutions apply.






REQUIRED PRIVACY PROVISIONS IN NEW LAWS	FairWarning® Features 	U.S. Federal & State 	Canada & Provinces 	UK & Country Regulation 	EU Countries 
<p>Detect, report and prevent snooping</p> <p>Detect, report and prevent identity theft</p>	<p>Proactive privacy breach detection with over 100 snooping & identity theft scenarios</p> <p>Results used with sanctioning & training as well as other business processes like dissemination of information</p>	<p>ARRA HITECH definition of breach – Applies to <i>all U.S. healthcare</i></p> <p>FTC Red Flags Rule for Healthcare (identity theft prevention) – Applies to all U.S. healthcare</p> <p>CA SB 541 & AB 211 – All California healthcare</p>	<p>Ontario's Freedom of Information and Protection of Privacy</p>	<p>UK Data Protection Act</p>	<p>EU Data Protection Directive, Country by country directives</p>
<p>Notification</p> <p>Disclosure</p> <p>Freedom of Information</p>	<p>Global patient and user investigation</p> <p>Save Ad Hoc</p> <p>Forensically sound repository</p>	<p>ARRA HITECH ACCOUNTING OF DISCLOSURE, others – <i>All U.S. healthcare</i></p> <p>45 U.S. state Disclosure laws</p>	<p>Ontario's Freedom of Information and Protection of Privacy</p>	<p>UK Freedom of Information</p> <p>Caldicott Guardian</p>	<p>EU Data Protection Directive, Country by country directives</p>
<p>General Healthcare Privacy & Security</p>	<p>Proactive review & audit of all systems which access protected health information</p>	<p>HIPAA</p>	<p>PIPEDA</p>	<p>UK & EU Data Protection Directive</p>	<p>EU Data Protection Directive, Country by country directives</p>

Table 1. Privacy Breach Detection & Auditing Regulatory Impact

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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

For More information on Privacy Breach Detection Solutions

- Customer case studies: Patient.Privacy@FairWarningAudit.com
- U.S. and Canada webinar on privacy: [Click here](#)
- UK webinar on privacy breach detection: [Click here](#)
- Privacy Breach Detection White Paper: [Click here](#)
- FairWarning® integration with SIEM solutions: [Click here](#)
- Return on investment calculator: Patient.Privacy@FairWarningAudit.com
- Comparison and evaluation forms: Patient.Privacy@FairWarningAudit.com
- Planning and deployment guides: Patient.Privacy@FairWarningAudit.com

About FairWarning®

FairWarning®'s mission is to be the world's leading supplier of privacy breach detection solutions for Electronic Health Records. Healthcare's privacy leaders have already deployed FairWarning® privacy breach detection solutions:

- FairWarning® customers represent nearly 200 hospitals and over 700 clinics in the United States, Canada and United Kingdom. This is an increase from 90 hospitals at the start of 2009
- 49 % of FairWarning®'s customers are national award winners having been recognized by 100 Most Wired, Verispan 100, U.S. Business Week and Malcolm Baldrige.
- FairWarning®'s production customers *range in size from 1,500 to 50,000 direct employees*. Our turn-key solutions audit privacy for every major electronic health record system and over one-hundred (100) applications, including: *AGFA, Allscripts, Cerner, Eclipsys, Epic, GE, McKesson, MEDITECH, Siemens, others - as well as applications used in the business of healthcare such as Lawson and PeopleSoft.*
- Eighty-three percent (83 %) of FairWarning®'s customers reported having avoided the costs and exposure of privacy breaches by using FairWarning® privacy breach detection to detect and deter breaches from ever occurring
- Fifty-seven percent (57 %) indicated they have been involved in a legal proceeding or court case in which they utilized FairWarning® privacy auditing and investigative capabilities.

FairWarning® patient privacy auditing and monitoring is essential to complying with recent privacy regulations such as ARRA HITECH / Accounting of Disclosures, FTC Red Flags Rule, HIPAA, California SB 541 & AB 211, as well as UK & EU Data Protection Acts and Canadian Provincial laws.

Visit www.FairWarningAudit.com or email solutions@FairWarningAudit.com for more information.

FairWarning, Inc.

Email: solutions@FairWarningAudit.com

Web: www.FairWarningAudit.com

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