



Executive Overview of Survey Results on Industry Best Practices for Patient Privacy in Electronic Health Records

Best practices for creating and sustaining a culture of patient privacy for care providers making meaningful use of electronic health records

Research and analysis conducted by New London Consulting, April 15, 2011

Sponsored by



Purpose of the Study and Executive Overview Report

In January 2011, FairWarning®, commissioned New London Consulting to develop and conduct an independent survey of healthcare providers. The survey was designed to elicit answers regarding healthcare professionals' opinions and insights on patient privacy initiatives, breach detection, prevention and remediation. The survey was live for 21 days and resulted in the participation of 340 individuals from care providers across the United States and several Canadian Provinces. Canadian and United States responses have been analyzed separately, and the Canadian report will be issued under separate cover. The full survey methodology is detailed in Appendix I.

The results in this report come exclusively from respondents based in the United States.

A series of 24 questions were posed that sought to reveal the following:

- Industry best practices for creating a culture of patient privacy and best practices adoption rates
- The effectiveness of privacy breach prevention and detection activities
- How care providers are investigating and remediating privacy breaches

The Executive Overview Report highlights several noteworthy trends and reveals new market data detailing the efforts of care providers to more proactively and effectively detect, prevent, investigate and remediate privacy breaches.

Summary of Findings

A wide-chasm has developed in the treatment of patient privacy between best practice care providers and others. Best practice care providers report that they have implemented an automated breach detection tool, conduct on-going privacy training including specifics on appropriate use of electronic health records (EHR), consistently levy sanctions and conduct a timely remediation process.

The survey revealed a dramatic divergence of confidence levels in patient privacy programs between best practices care providers and other care providers:

- Best practice care providers are ninety-seven percent (97%) confident in their breach detection and deterrence capabilities. In contrast all other care providers report they are only forty-four percent (44%) confident.
- Best practice care providers who consistently communicate and levy sanctions are seventy-eight (78%) confident this activity deters breaches. In contrast all other care providers report they are only twenty-two percent (22%) confident that their sanctioning activities are effective in deterring breaches.
- Care providers utilizing an automated in-house developed or commercial breach detection tool report they are one hundred twenty-two percent (122%) more confident than other care providers in detecting and deterring privacy breach.

Finally, survey data reveals while ARRA HITECH has increased a sense of urgency in conducting that virtually all care providers are still in need of coordinating technologies, policies, training and remediation into an entity-wide plan that creates a culture of privacy.

Baseline Definitions

Privacy Breach:

The misuse of access to electronic health records for the purpose of curiosity or malicious activity. Curiosity based breaches include self examination of one's own record, family member snooping, VIP snooping, co-worker snooping, neighbor snooping, and other non-malicious users. Malicious breaches include identity theft, medical identity theft, fraud, using data for personal gain, criminal activities, and other life-altering activities.

Remediation:

The act or process of correcting the damage caused by a breach.

The complete survey findings are detailed on the following pages.

Executive Overview: Key Highlights

Eleven percent (11%) of responding care providers have created a culture of patient privacy through the application of industry best practices.

Care providers identified the following industry **best practices** for creating a culture of patient privacy:

- Use of a commercial automated privacy breach detection tool
- Ongoing privacy training
- Specific training on inappropriate access to EHRs
- Consistent application of sanctions
- Effective and timely remediation

Best practices care providers report their detection activities are effective, and indicated that the more proactive their breach detection, the more effective their privacy program. These respondents state their detection is effective and report high levels of confidence in their ability to deter both curiosity-based and malicious privacy breaches. In contrast, only forty-four percent (44%) of remaining care providers assert that both their detection and deterrence efforts are effective.

In addition, care providers that apply **best practices** report that privacy training and specific training on inappropriate access to EHRs occurs at least once a year. Ninety-seven percent (97%) of best practices respondents in this group state that the care provider consistently communicates sanctions for inappropriate access to EHRs, and one-hundred percent (100%) assert they consistently levy sanctions. In general, these care providers take an aggressive approach to remediating privacy breaches.

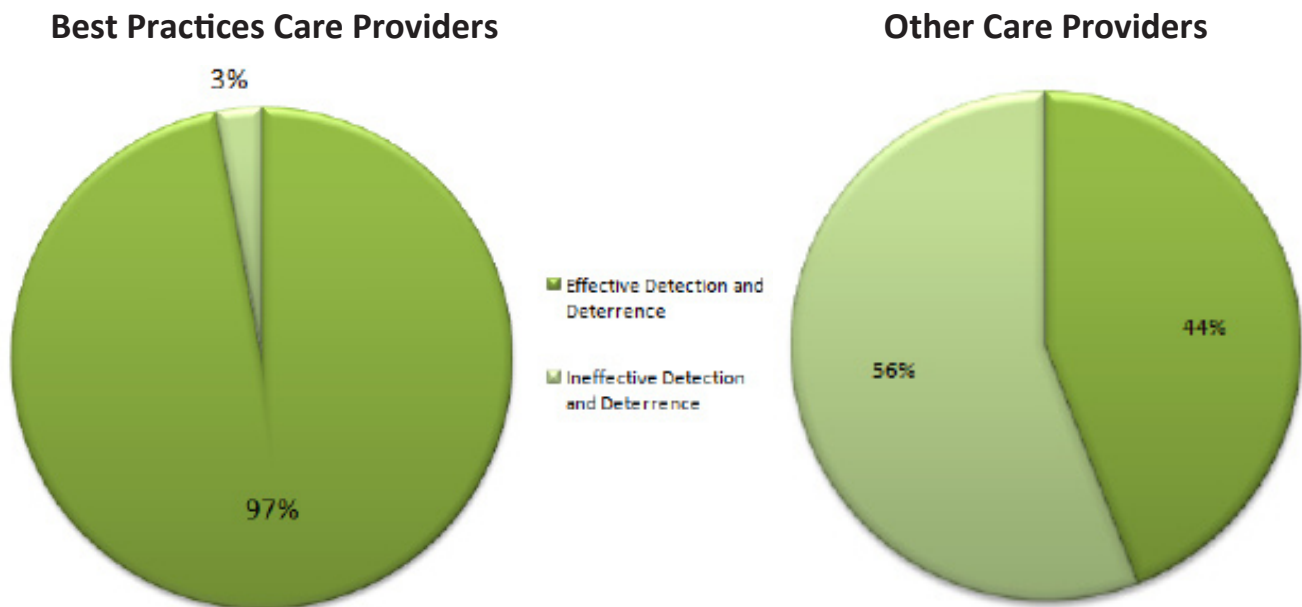


Figure #1: Confidence in Privacy Breach Detection and Deterrence

A Care Provider's Efficacy in Deterring Breaches is Directly Related to its Consistency in Communicating Sanctions and Levying Fines.

Seventy-five percent (75%) of respondents state their organization clearly communicates sanctions for inappropriately accessing patient records while seventy-two percent (72%) report consistency in levying these sanctions. Among care providers that consistently communicate sanctions for inappropriate access and are consistent in levying sanctions, seventy-eight percent (78%) report high levels of efficacy in deterring both curiosity-based and malicious privacy breaches. In comparison, among care providers that report inconsistent communication and levying of sanctions, only twenty-two percent (22%) report high levels of efficacy in deterring privacy breaches.

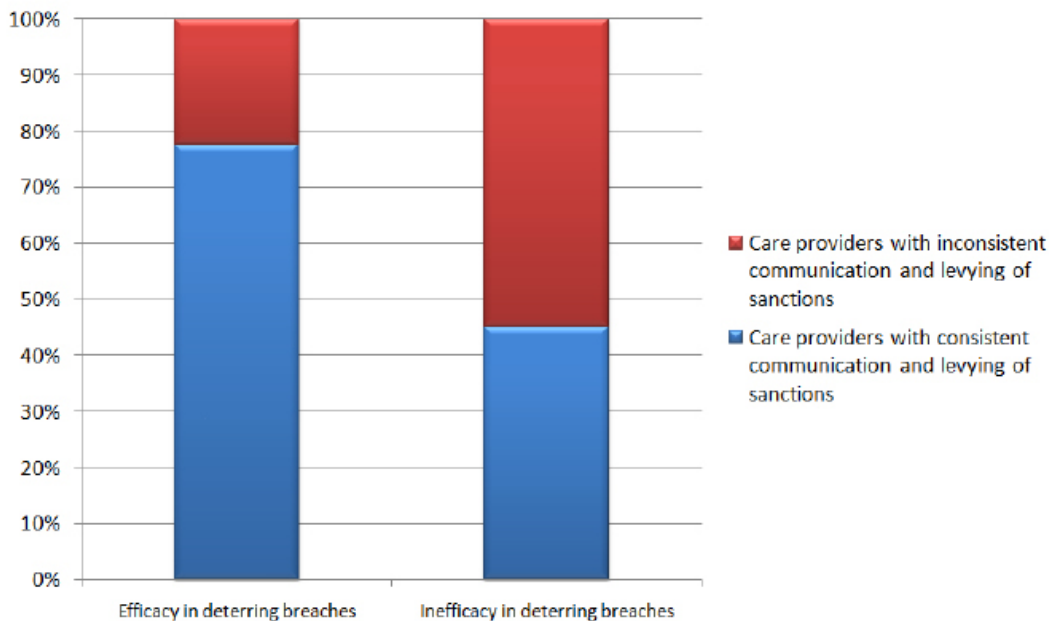


Figure #2: Breach Prevention Efficacy and Sanctions

Care Provider Respondents Indicate Moving to Automated Breach Detection Tools Results in More Efficient and Proactive Detection of Privacy Breaches.

The data demonstrates that care providers still rely heavily on manual and complaint driven detection and most care providers are utilizing several methods for detection. However, care providers that utilize a commercial breach detection tool report significantly less reliance on manual processes as compared to care providers that utilize an internally developed tool. Additionally, care providers that utilize automated breach detection tools, whether internally developed or commercial, are more than twice as likely to report that their detection activities are highly effective. Sixty-nine percent (69%) of care providers that rely on an automated breach detection tool report their detection activities are highly effective, while only thirty-one percent (31%) of care providers that do not use an automated tool report their detection activities are highly effective.

4-out-of-5 care providers with effective detection report effective deterrence of privacy breaches. Comparatively, 1-out-of-2 care providers without effective breach detection report efficacy in deterring privacy breaches.

As demonstrated in the figure below, eighty-three (83%) of the respondents that report the care provider’s detection activities are effective or highly effective also report high levels of efficacy in deterring both curiosity-based and malicious privacy breaches.

The majority of care providers demonstrate a sense of urgency and diligence in investigating suspected privacy breaches. Care providers initiate investigation activities immediately or within 30 days in cases of suspected malicious breaches.

Care providers report that HITECH has changed the way in which they investigate suspected privacy breaches. Eighty-four percent (84%) of respondents state that the organization now has a more formal investigation and remediation process while near seventy-eight percent (77.8%) state there is more urgency in conducting breach investigation. Fifty-eight (58%) of respondents report there are more internal stakeholders and departments involved in the process. Nearly half of respondents note there is more involvement of legal counsel and a greater reliance on the privacy, risk and compliance departments within the organization.

Survey data reveals the healthcare industry is in need of best practices for coordinating technologies, policies, training and remediation into an entity-wide plan that creates a culture of privacy.

Thirty-five percent (35%) of responses indicate the care provider does not have best practices for deterring and remediating privacy breaches. As shown below, care providers state the obstacles to conducting best practices include employee resource constraints, lack of knowledge of best practices, budget constraints, a lack of consistency and lack of or no support from hospital executives or board.

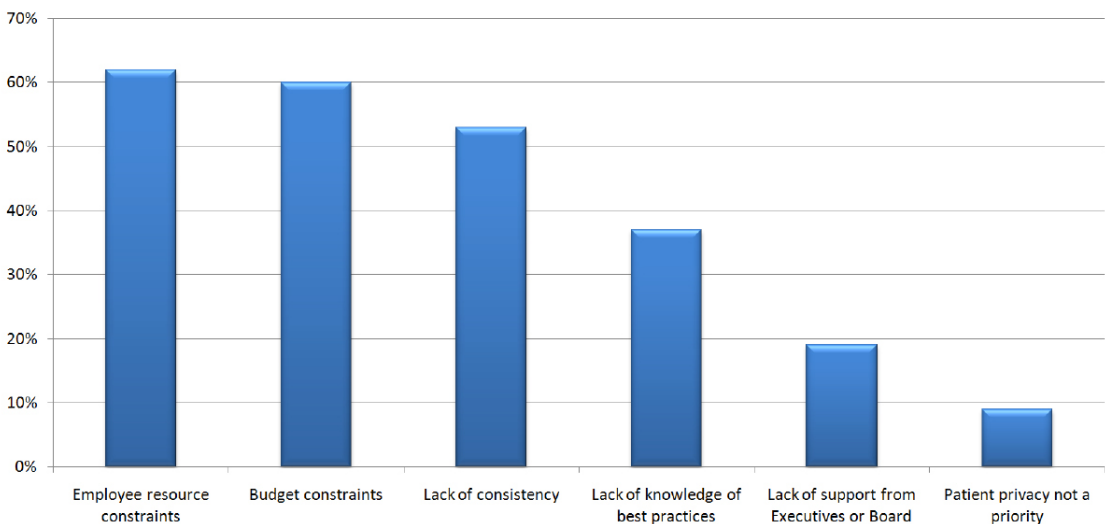


Figure #3:
Obstacles to Application
of Best Practices

Summary

In conclusion, care providers are becoming more astute in respect to the importance of privacy breach detection to mitigate risks which could impede growth and meaningful use of EHRs. As this survey demonstrates, care providers committed to delivering the highest level of patient care are integrating critical patient privacy protections. These care providers demonstrate that patient care and patient privacy are interdependent.

The survey also reveals that there is a distinct chasm developing between the treatment of patient privacy at care providers applying best practices and the rest of the market. As detailed in the report, best practices organizations are more than twice as likely than other care providers to report they are effective at detecting and deterring breaches. Similarly, care providers that consistently communicate sanctions and levy sanctions for inappropriate access are four times more likely than care providers that report inconsistent communication and levying of sanction to report effective deterrence of privacy breaches.

This data suggests that the healthcare industry is in need of best practices for an entity-wide plan for integrating technologies, developing and communicating privacy policies, executing training and carrying out remediation to create a culture of privacy.

Appendix 1: Survey Methodology

In January 2011, FairWarning, a leading provider of privacy solutions for the healthcare industry, commissioned New London Consulting to develop a survey of healthcare providers in the US and Canada. The survey was designed to elicit answers and insights on how these providers detect and remediate privacy breaches. Additionally, the survey sought to identify organizational behaviors which support the protection of patient privacy.

New London Consulting and FairWarning developed a survey consisting of 24 questions. The survey was conducted using an online platform. Survey invitations were sent to more than 10,000 C-suite executives, human resource managers, in-house legal counsel, compliance, privacy or risk managers, directors and executives, IT managers, non-IT managers, and IT hands-on personnel working within healthcare organizations, specifically in hospitals, clinics and other facilities in the US and Canada. The survey invitation resulted in participation of 340 individuals. The survey was live for approximately 21 days.

The demographics of survey participants are as follows:

Business Type

Not-for-profit	86.2 percent	
For profit	9.1 percent	
Other*	4.7 percent	* Includes government healthcare agencies, public hospitals and county-owned healthcare providers.

Role within the organization

Executive management	8 percent
Compliance, privacy or risk	57 percent
IT management	16 percent
Non-IT management	4 percent
IT hands-on personnel	7 percent
Other	8 percent

Number of employees

Less than 1,000	13 percent
1,001 to 5,000	47 percent
5,001 to 10,000	19 percent
10,001 to 25,000	15 percent
Greater than 25,000	6 percent

Composition of healthcare organizations

Hospitals	89 percent
Clinics	73 percent
Other facilities	54 percent

US states represented

AK, AL, AR, AZ, CA, CO, CT, DC, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MA, MD, MI, MN, MO, MS, NC, ND, NE, NJ, NM, NY, NV, OH, OK, OR, PA, RI, SC, SD, TN, TX, UT, VA, WA, WI, WY

Canadian provinces represented

British Columbia, Manitoba, Nova Scotia, Ontario, Quebec, Saskatchewan

* Due to differing laws and compliance requirements, Canadian and United States responses were analyzed separately.

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

© 2011 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.

For more information, please contact:

Sadie Peterson
Director of Corporate & Software Product Marketing
FairWarning, Inc.
727 576 6700 x119
sadie@fairwarningaudit.com

FAIRWARNING®

FairWarning's mission



is to continue to be
the world's leading
supplier of solutions
which monitor and
protect patient
privacy in Electronic
Health Records.

FairWarning, Inc.
9500 Koger Boulevard, Suite 219
St. Petersburg, Florida 33702
www.fairwarningaudit.com