



Healthcare Privacy Regulatory Compliance in the U.S.

***Market Survey Report Nearly One Year after
ARRA HITECH***

January 27, 2010

Table of Contents

Survey Methodology	3
Executive Overview	5
Report Breakdown	9
Healthcare organizations' awareness and understanding of new privacy laws and concerns surrounding willful neglect and breach notification	
Perceived impact of ARRA HITECH accounting of disclosure requirements	
Healthcare organizations' adoption rate of automated systems and processes that will meet compliance requirements	
Perceptions surrounding government enforcement of the new laws and the likelihood of an audit	
Deployment and effective use of privacy and auditing tools for compliance	
Survey Analysis	20
About FairWarning	22
About New London Consulting	23

Survey Methodology

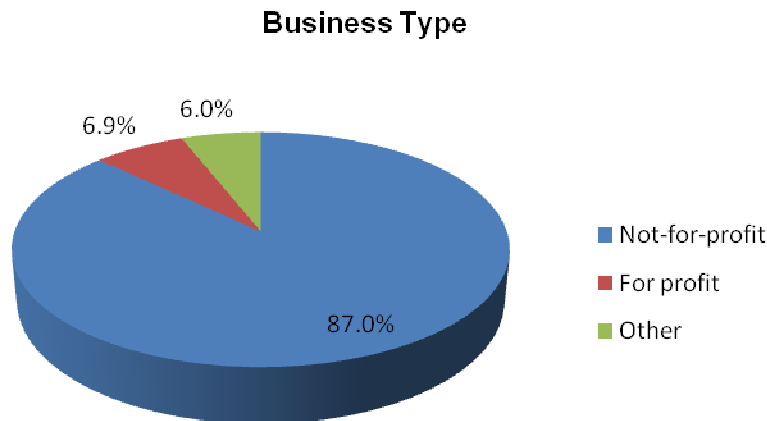
In November 2009, **FairWarning®**, a leading provider of privacy solutions for the healthcare industry, commissioned New London Consulting to develop a survey of healthcare providers. The survey was designed to elicit answers regarding opinions and insights on new healthcare privacy regulations, patient safety, privacy and auditing budgets and information technology risk management.

New London Consulting and **FairWarning®** developed a survey consisting of 26 questions. The survey was conducted using an online platform. Survey invitations were sent to more than 4,000 C-suite executives, compliance, privacy or risk managers, directors and executives, IT managers, non-IT managers, and IT hands-on personnel working within healthcare organizations, specifically hospitals across the United States. The survey invitation resulted in the participation of 216 individuals. The survey was live for approximately 21 days.

The demographics of survey participants are as follows:

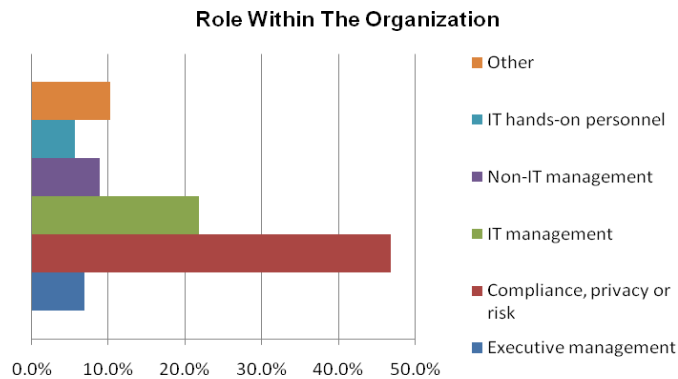
Business Type

Not-for profit	87.1 percent
For profit	6.9 percent
Other	6.0 percent



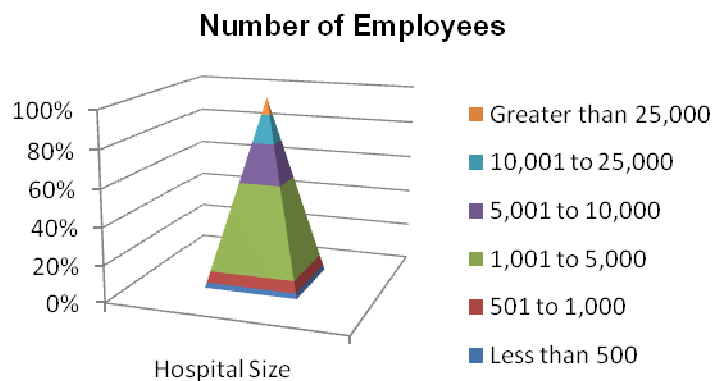
Role within the organization

Executive management	6.9 percent
Compliance, privacy or risk	46.8 percent
IT management	21.8 percent
Non-IT management	8.8 percent
IT hands-on personnel	5.6 percent
Other	10.2 percent



Number of employees

Less than 500	2.8 percent
501 to 1,000	6.0 percent
1,001 to 5,000	46.8 percent
5,001 to 10,000	20.8 percent
10,001 to 25,000	14.8 percent
Greater than 25,000	8.8 percent



States represented

AK, AL, AR, AZ, CA, CO, FL, GA, HI, ID, IL, IN, KS, KY, LA, MA, MD, MI, MN, MO, MS, MT, NC, NE, NJ, NY, OH, OK, ON, PA, RI, SC, SD, TN, TX, UT, VA, VT, WA, WI, WV, WY

Executive Overview

In 2009, several privacy provisions were signed into law impacting the manner in which healthcare organizations must protect and audit patient private data and disclose breaches to the patient, media and government. Most notably, ARRA HITECH privacy provisions were signed into law February 17th, 2009. In 2009, the FTC ruled that the FTC Identity Theft Red Flags Rule, which will be enforced beginning June 1st, 2010, will now cover healthcare providers. These laws and rules require healthcare entities to operate under greater transparency and have expanded privacy issues including anti-snooping, prevention of medical identity theft, accounting of disclosures and a patient's right to know who has externally accessed their medical information. New privacy laws also require breach notification to the media, patients affected and the government.

Additionally state legislators are pushing for tougher laws to protect patient privacy. For example, California Senate Bill 541 and Assembly Bill 211 became law January 1st, 2009 and have already been enforced resulting in fines and penalties.

In the past, the healthcare industry was largely unencumbered by patient privacy laws. HIPAA was rarely enforced and "privacy breach" was loosely defined. With the passing of these new laws, the government has detailed a very specific expectation for compliance: a timeline for compliance, a clear definition of a privacy breach, an accounting of disclosure requirement, breach notification requirements, and applicable fines and penalties for institutions and individuals involved in privacy breaches.

With the passing of new laws, the government has detailed a very specific expectation for compliance: a timeline for compliance, a clear definition of a privacy breach, an accounting of disclosure requirement, breach notification requirements, and applicable fines and penalties for institutions and individuals involved in privacy breaches.

In November 2009, [FairWarning®](#), a leading provider of privacy surveillance solutions for Electronic Health Records, commissioned New London Consulting to develop a survey of healthcare providers, specifically hospital personnel. The survey was designed to elicit answers regarding healthcare professionals' opinions and insights on new healthcare privacy regulations such as ARRA HITECH, privacy security and auditing, information technology risk management, and compliance requirements.

New London Consulting and [FairWarning®](#) developed a series of 26 questions that sought to reveal the following:

- Healthcare organizations' awareness and understanding of new privacy laws and concerns surrounding willful neglect and breach notification
- Perceived impact of ARRA HITECH accounting of disclosure requirements
- Healthcare organizations' adoption rate of automated systems and processes that will meet compliance requirements
- Perceptions surrounding government enforcement of the new laws and likelihood of an audit
- Deployment and effective use of privacy and auditing tools for compliance

Survey Findings Overview

The complete survey findings reveal healthcare organizations are:

- Familiar with new healthcare privacy and security regulations, specifically ARRA HITECH and the FTC Red Flags Rule
- Concerned with the reputational impact associated with a breach and breach notification requirements
- Mobilizing to meet compliance requirements and deploying critical technologies to plug security gaps and meet compliance requirements
- Allocating budget to meeting new privacy and security requirements
- Beginning to believe that enforcement of these laws is a government priority and,
- In need of further education to align spending and technology deployments to government expectations

Highlighted Survey Findings

ARRA HITECH was signed into effect in 2009. The FTC Red Flags Rule will take effect in June 2010. These laws provide a more stringent definition of a privacy breach and mandate specific actions that must be taken in an effort to protect patient privacy. ARRA HITECH defines a privacy breach as the “unauthorized access, use or disclosure of protected health information which compromises the security or privacy of such information. Additionally, these laws stipulate specific fines, penalties and notification requirements when a breach occurs. Now that the law clearly defines a breach, the survey indicated that healthcare organizations are very concerned that they must notify and disclose under ARRA HITECH. Or should they choose not to disclose, these organizations must be prepared to defend their decision to the government.

The survey indicated that healthcare organizations are “very concerned” that they must notify and disclose under ARRA HITECH.

This survey revealed that almost all of the respondents were familiar with these federal laws. When asked questions specific to ARRA HITECH, respondents were most concerned about breach notification to the media, patient and the government. Survey respondents’ top three concerns surrounding non-compliance were 1) reputational impact of a failed audit or major privacy breach, 2) financial penalties for non-compliance and 3) media exposure.

Under the new ARRA HITECH legislation patients have a right to request an accounting of who has externally accessed their Electronic Health Record (EHR.) In effect this means that when a healthcare entity shares patient data with any person/entity outside the organization for any purpose including treatment, payment or sharing of clinical data, the patient has a right to request from the healthcare entity an accounting of who this data has been shared with. Healthcare organizations using an EHR are required to account for *any* external access or inappropriate access to the record and disclose this information to the patient upon request. When asked about specific accounting of disclosure requirements set forth in ARRA HITECH, the vast majority, 92.1 percent of survey respondents, stated their organization is aware of the requirements.

92.1% of survey respondents stated that their organization is aware of the specific accounting of disclosure requirements set forth in ARRA HITECH.

Survey respondents report that they are implementing processes, procedures and technologies in an effort to meet compliance requirements. Overall, respondents feel that their organization is appropriately budgeting for compliance activities. Although these organizations are working toward compliance, nearly one-third state that they will not meet compliance deadlines set forth in ARRA HITECH. The survey also reveals that there is a need for market education regarding the need to implement automated systems that will monitor, audit, detect and report patient record access to meet ARRA HITECH accounting of disclosure requirements. Respondents report that nearly 44 percent of organizations have already deployed accounting of disclosure log aggregation and patient privacy auditing solutions.

A majority of respondents stated that they were either concerned or very concerned about being audited for privacy compliance.

Many organizations are employing critical technologies to plug security vulnerabilities. The survey identified seven cornerstone technologies which complement processes and other automated systems designed to meet compliance requirements. These technologies include:

- User privacy monitoring in EHRs
- Accounting of disclosure log aggregation
- Data leakage prevention
- Patient and user privacy auditing
- Single sign on
- Identity management
- Infrastructure log management

The survey revealed that the healthcare industry is mobilizing efforts to implement and integrate these technologies. However, very few organizations have implemented all of them. These leading organizations account for 7 percent of the survey respondents. The most commonly deployed technologies are, respectively: patient and user privacy auditing, identity management and single-sign on. The top three technologies that organizations are planning to deploy are: accounting of disclosure log aggregation, data leakage prevention, and infrastructure log management. More than 4 out of 5 organizations plan to include these technologies in their privacy and security plans.

Although these organizations are moving toward deploying these critical technologies, responses indicate there is a continued need for market education regarding what these organizations must demonstrate to meet compliance regulations. Nearly half of the respondents believe their organization is in full compliance with state and federal privacy laws and are audit ready however many of them have yet to deploy the technologies that will meet accounting of disclosure requirements, or audit for patient privacy and monitor for privacy breaches.

Responses indicate that there is a continued need for market education regarding what organizations must demonstrate in order to meet compliance regulations.

The survey suggests that the healthcare industry is just beginning to believe that government enforcement of privacy laws is a state and federal priority. Although the industry is not yet fully convinced that there will be increased audit activity, a majority of respondents stated that they were either concerned or very concerned about being audited for privacy compliance. Slightly more than half of respondents believe enforcement of privacy laws is a government priority; however only one-third of respondents believe that compared to 12 months ago, they stand a greater chance of a state or federal privacy audit.

Responses also indicate healthcare organizations do not know or possibly do not understand what the government will be looking for in an audit scenario. Of the organizations that believe they are in full compliance with the laws, just 51 percent of respondents agree or strongly agree that the government will not find any material shortcomings.

Compliance requires organizations to demonstrate effective use of solutions and technologies should permeate all business units, correspond with business processes and integrate with the business functions of the organization. The survey revealed that healthcare organizations are beginning this process. Just 7 percent of respondents have demonstrated that they have both processes and automated systems in place which incorporate the cornerstone technologies designed to eliminate security and privacy vulnerabilities. Nearly 60 percent of organizations are concerned about the technology challenge of monitoring dozens of healthcare applications. The survey also revealed that many of these organizations plan to leverage key privacy and auditing technologies but have yet to set a deployment date.

Compliance requires organizations to demonstrate effective use of solutions and technologies that permeate all business units, correspond with business processes and integrate with the business functions of the organization.

Complete survey findings are detailed in the following pages.

Healthcare Organizations’ Awareness and Understanding of New Privacy Laws and Concerns Surrounding Willful Neglect and Breach Notification

ARRA HITECH defines a healthcare privacy breach, stipulates accounting of disclosure and details patient notification responsibilities. Additionally, it outlines tiered penalties and increased healthcare privacy audits of healthcare entities.

Nearly all survey respondents stated they are familiar with the new federal privacy and security regulations.

Under the FTC Red Flags Rule, healthcare entities must identify and operationally detect patterns that provide a suspicion of identity theft related activities. The healthcare entity is further obligated to report identity theft when it occurs in their operations and must implement systems and processes that prevent identity theft in their operations. The FTC implemented this ruling because of an epidemic of well documented identity theft incidents during 2007 and 2008.

Healthcare entities which turn a blind-eye to, or “willfully neglect”, patient privacy rights and the curtailment of privacy breaches now face serious business repercussions which include; media exposure and associated public relation damages, patient visibility and associated lawsuit risks, Federal government fines as well non-compliance with the U.S. Health and Human Services Office of Civil Rights, the U.S. Federal Trade Commission and state law.

This section of the survey was designed to measure healthcare organizations’ familiarity with the new Federal laws. Additionally the survey sought to reveal healthcare organizations’ primary concerns relative to non-compliance.

Nearly all survey respondents stated they are familiar with the new federal privacy and security regulations.

- 92.1 percent of survey respondents stated they are familiar with ARRA HITECH
- 90.7 percent of survey respondents stated they are familiar with the FTC Red Flags Rule

Survey respondents’ top three concerns surrounding non-compliance are 1) reputational impact of a failed audit or major privacy breach, 2) financial penalties for non-compliance and 3) media exposure.

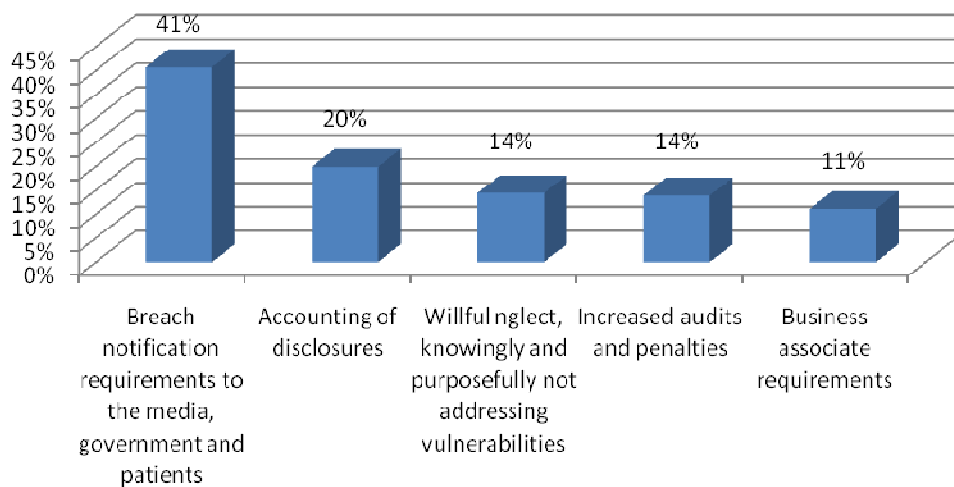
- 66.7 percent of survey participants ranked “reputational impact if my organization fails an audit or suffers a major privacy breach” as their first or second concern. 40.3 percent of survey participants ranked “reputational impact if my organization fails an audit or suffers a major privacy breach” as their number one concern.
- 57.8 percent of survey participants ranked “media exposure relative to non-compliance or a privacy incident” as their first or second concern. 22.2 percent ranked it as their primary concern.

Survey respondents’ top three concerns surrounding non-compliance are 1) reputational impact of a failed audit or major privacy breach, 2) financial penalties for non-compliance and 3) media exposure.

- 49.5 percent of survey participants ranked “financial penalties for non-compliance” as their first or second concern. 25.9 percent of survey respondents ranked it as their first concern.
- Only 26 percent of survey respondents ranked “possibility of a long-term resolution agreement with the Federal government” as their first or second concern.

Specific to ARRA HITECH regulations, respondents are most concerned about breach notification requirements to the media, government and patients.

Respondents Were Most Concerned About:



- When asked to rank what is the most concern to a respondent’s organization, breach notification requirements to the media, government and patients was the highest ranked concern. 40.7 percent of respondents ranked this as their number one concern.
- Accounting of disclosures ranked as the second highest concern (19.9 percent) followed respectively by: willful neglect, knowingly and purposefully not addressing vulnerabilities (14.4 percent); increased audits and penalties (13.9 percent); and lastly, business associate requirements (11.1 percent).

40.7% ranked breach notification as their number one concern.

Perceived impact of ARRA HITECH Accounting of Disclosures Requirements

The new ARRA HITECH legislation states that patients have a right to know who has externally accessed their personal health information (PHI). Healthcare organizations are required to account for any access to the record and disclose this information to the patient upon request. ARRA HITECH poses several logistical challenges including ensuring that every external touch of a patient's PHI is logged and auditable. This requires healthcare entities to monitor access by the healthcare entities' employees including doctors, nurses, billing and insurance personnel, and external business associates such as visiting physicians, insurance company employees and other partners.

The survey consisted of a series of questions designed to uncover the perceived impact of ARRA HITECH accounting of disclosure requirements. These questions addressed planning issues including: meeting compliance timelines, setting budgets and addressing technical considerations for meeting the accounting of disclosure requirements. Additionally, the survey was designed to uncover which technologies these healthcare organizations were employing to assist in the automation of their accounting of disclosure responsibilities.

When asked about specific requirements set forth in ARRA HITECH, the vast majority of survey respondents stated their organization is aware of the requirements.

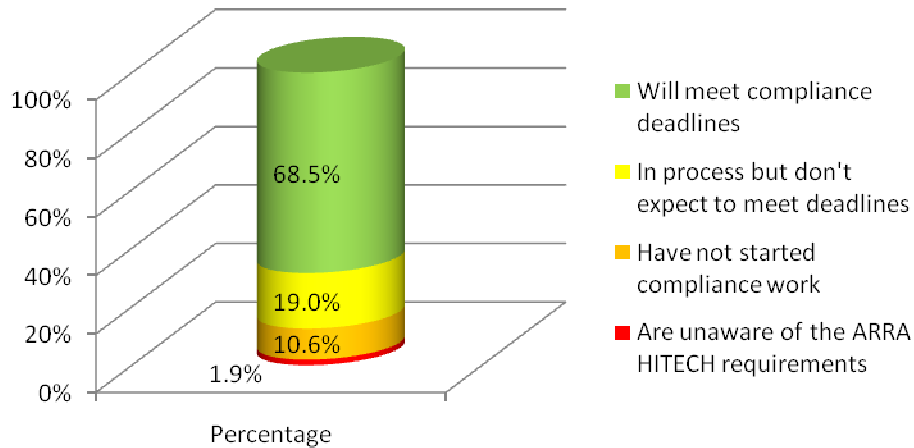
- 92.1 percent of survey respondents stated their organization is aware of the accounting of disclosure requirements as specified in ARRA HITECH

Survey responses demonstrate that healthcare organizations may not realize or understand the need for implementing and integrating automated systems to monitor, audit, detect and report patient records access in an effort to be ARRA HITECH compliant and meet accounting of disclosure requirements.

- Of the 43 percent of organizations that stated they have automated systems in place to meet the accounting of disclosure responsibilities of ARRA HITECH, less than half of those organizations (37) have deployed accounting of disclosure log aggregation and patient and privacy auditing solutions.
- 44.9 percent of respondents stated that their organization does not plan to deploy, or has yet to determine a deployment date for an accounting of disclosure log aggregation solution.

Nearly one-third of survey respondents stated they will not be compliant with ARRA HITECH requirements by the set deadlines.

ARRA HITECH Compliance Readiness



- 19 percent of survey respondents are in the process of performing ARRA HITECH compliance work but don't expect to be completed by the deadline.
- 10.6 percent of survey respondents have not started to perform significant ARRA HITECH work.
- 1.9 percent of survey respondents state that they are unaware of the ARRA HITECH Act and its requirements.
- 40.3 percent of survey respondents report that they have an automated system to meet the accounting of disclosure responsibilities of ARRA HITECH.

68.5% feel they will meet compliance deadlines.

Majority of respondents report that their organization is allocating budgets to meet new privacy and auditing requirements.

- Only 24.6 percent of respondents feel that their organization is not appropriately budgeting to meet privacy and auditing requirements.
- 28.2 percent of respondents agree or strongly agree that their organization has appropriately budgeted for meeting new privacy and auditing regulations.
- 37.5 percent of respondents agree or strongly agree their organization is adequately allocating budget to achieve the priority of ensuring patient privacy.
- 21.8 percent of respondents feel that their organization is not appropriately budgeting to achieve the priority of ensuring patient privacy.

Only 24.6 percent of respondents feel that their organization is not appropriately budgeting to meet privacy and auditing requirements.

Adoption Rate of Entity-Wide Automated Systems and Processes for Compliance

With new healthcare privacy legislation, and an increased Federal focus on patient privacy and compliance, healthcare organizations are working to institute entity-wide privacy and security plans as well as safeguards against inappropriate access to physical records. These laws require that healthcare entities operationalize their privacy and security plans into technologies and business processes in order to avoid the consequences of material shortcomings. In the majority of cases, these security plans involve the implementation of foundational technologies and processes relating to authentication, firewalls, and encryption as well as secure remote access. However, these technologies alone do not meet compliance requirements.

Foundational technologies and processes, such as authentication, firewalls, encryption, and secure remote access are not sufficient to meet compliance requirements.

Additional technologies which are critical to organizational security include: user privacy monitoring in EHRs, accounting of disclosure log aggregation, data leakage protection, patient and user privacy auditing single sign-on, identity management and infrastructure log management. Of these technologies, user privacy monitoring in EHRs, accounting of disclosure log aggregation, patient and user privacy auditing, identity management and infrastructure log management is thought to be the minimum required to meet compliance requirements.

This section of the survey was designed to gauge healthcare organizations' use of such technologies, deployment status and ability to demonstrate effective use, integration and a substantial presence and use of these solutions across the healthcare enterprise.

Healthcare organizations are planning to deploy critical technologies.

A substantial percentage of respondents have *not yet* deployed critical technologies designed to fill security vulnerabilities.

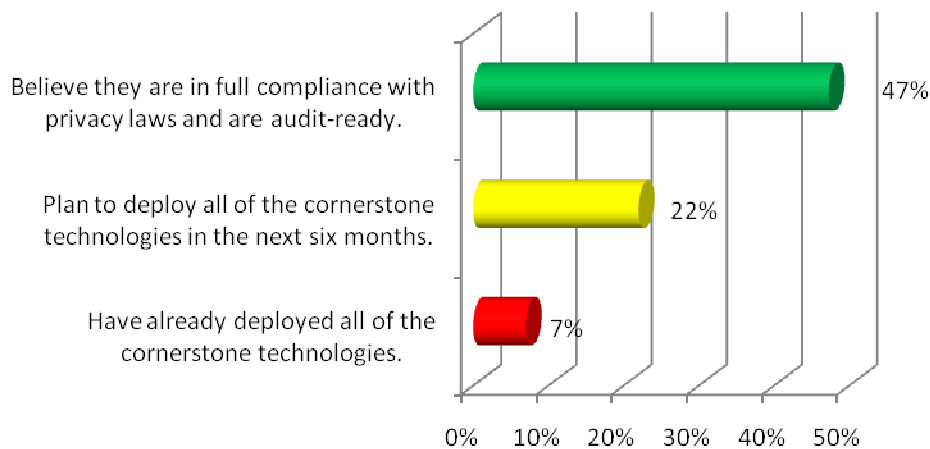
Technology solution	Respondent organizations that <i>have not deployed</i>
User privacy monitoring in EHRs	56.9 percent
Accounting of disclosure log aggregation	63.9 percent
Data leakage prevention	68.5 percent
Patient and user privacy auditing	42.1 percent
Single sign-on	55.1 percent
Identity management	53.7 percent
Infrastructure log monitoring	57.9 percent

Responses indicate healthcare organizations are *planning to deploy* critical technologies.

Technology solution	Respondent organizations that plan to deploy	Respondent organizations that have already deployed
User privacy monitoring in EHRs	46.3 percent	43.1 percent
Accounting of disclosure log aggregation	52.3 percent	36.1 percent
Data leakage prevention	53.7 percent	31.5 percent
Patient and user privacy auditing	35.2 percent	57.9 percent
Single sign-on	37.0 percent	44.9 percent
Identity management	43.5 percent	46.3 percent
Infrastructure log monitoring	46.8 percent	42.1 percent

Responses indicate there is a continued need for market education regarding what healthcare organizations must demonstrate to meet compliance regulations.

Compliance Readiness



- Only 7 percent of the respondents have deployed all of the cornerstone technologies.
- 22 percent of respondents stated their organization has automated systems in place *and* believes they are audit ready. Of these respondents only 32 percent have deployed or expect to deploy the following technologies in the next six months: user privacy monitoring in EHRs, accounting of disclosure log aggregation, patient and user privacy auditing, identity management and infrastructure log management.
- 47.3 percent of organizations believe that they are in full compliance with state and federal privacy laws and are audit ready. However, only 22 percent of these organizations have already deployed all of the following technology solutions: user privacy monitoring, accounting of disclosure log aggregation and patient and user privacy auditing.

- Of the remaining respondents that believe they are in full compliance, 22 percent of the respondent organizations plan to have the following technology solutions deployed in the next six months: user privacy monitoring, accounting of disclosure log aggregation and patient and user privacy auditing.
- 51.4 percent of respondents stated that their organization has automated systems in place to detect report and prevent inappropriate access to patient records in their electronic health records. However, less than 72 percent of these respondents state that they have deployed a patient and user privacy auditing tool. Only 59 percent have deployed user privacy monitoring in EHRs.
- 68.5 percent of participants stated that they have completed or in the process of performing ARRA HITECH compliance work and expect to meet compliance deadlines. However, only 48 percent of these organizations agree or strongly agree that the government **will not** find material shortcomings in an audit of their organization.
- 48 percent of respondents that report they are audit ready are compliance, privacy or risk personnel, 24 percent are IT management or hands-on personnel, 19 percent are non-IT management and 14 percent are executive management.

47.3% of organizations believe that they are in full compliance with state and federal privacy laws, and are audit ready.

However, only 22% of these organizations have already deployed all of the following technologies:

- User privacy monitoring***
- Accounting of disclosure log aggregation***
- Patient and user privacy auditing***

68.5% of participants have completed or are in the process of performing ARRA HITECH compliance work.

However, only 48% feel that the government will not find material shortcomings in an audit of their organization.

Perceptions Surrounding Government Enforcement of the New Privacy Laws and Likelihood of an Audit

The unannounced HIPAA audit at Piedmont Hospital in March of 2007 was an early signal to healthcare providers that the government was working to change the climate of compliance enforcement. Prior to this well publicized audit, HIPAA was rarely enforced. Healthcare entities were in large part self-monitoring for compliance.

With the passage of ARRA HITECH and other privacy mandates, the government has again signaled to healthcare organizations that systematic enforcement and periodic congressional reporting of privacy and security rules compliance will occur. ARRA HITECH additionally specifies fines which escalate as a healthcare entity demonstrates willful neglect. Under the FTC Red Flags Rule healthcare entities must identify and operationally detect patterns that provide a suspicion of identity theft related activities. The healthcare entity is further obligated to report identity theft when it occurs and must implement systems and processes that prevent identity theft in their operations.

Nearly half of healthcare organizations believe they are compliant with federal privacy laws, and are audit ready.

This section of the survey was designed to measure healthcare organizations' perceptions on the likelihood of being audited by the government under the new laws and risk mitigation. Additionally, respondents were asked to assess their likelihood of passing an audit without material shortcomings.

Nearly half of healthcare organizations believe their organization is compliant with federal privacy laws and is audit ready.

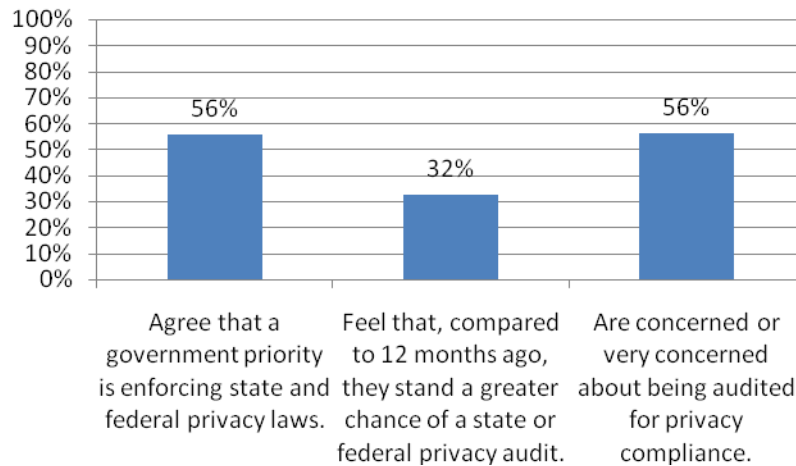
- 47.3 percent of respondents agree or strongly agree that their organization meets state and federal privacy compliance requirements and is audit ready.

Leading healthcare organizations are implementing security and privacy plans to meet compliance however responses indicate the healthcare industry is not yet fully convinced that there will be increased audit activity.

- Only slightly more than half of participants, 55.6 percent, agreed or strongly agreed that a government priority is enforcing state and federal privacy laws.
- Only 32.4 percent of participants believe that compared to 12 months ago they stand a greater chance of a state or federal privacy audit. Only 56 percent of participants stated they were concerned or very concerned about being audited for privacy compliance.

32.4% of participants believe that, compared to 12 months ago, they stand a greater chance of a state or federal privacy audit.

% of Respondents:



The industry in large part is not using third-party experts to help mitigate risk.

- 19.9 percent (43) of survey participants have been audited by a governmental body for compliance of privacy and security regulations in the past 12 months.
- Of those 19.9 percent (43) only 39 percent (17) hired a third-party organization to conduct a privacy and regulatory risk assessment.
- Overall, only 23.1 percent of participants hired a third-party organization to conduct a privacy and regulatory risk assessment.

56% of respondents agree that a government priority is enforcing state and federal privacy laws.

Responses indicate healthcare organizations do not know or possibly do not understand what the government will be looking for in an audit scenario.

- 50 percent of the respondents that agree that their organization meets state and federal privacy compliance requirements, only 50 percent (51) believe that the government **will not** find any material shortcomings.
- Previously audited organizations feel more confident than those that have not been audited, that if audited, the government will not find material shortcomings. Of the audited organizations, only 51 percent (22) agree or strongly agree that the government **will not** find material shortcomings in an audit of their organization.
- Of the organizations that have not been through a government audit (173), only 47.3 percent (82) agree or strongly agree that the government will not find material shortcomings in an audit of their organization.

Of organizations that have already been audited, only 51% feel that the government will not find material shortcomings during another audit.

Deployment and Effective Use of Privacy and Auditing Tools for Compliance

Privacy and auditing tools are essential in building a comprehensive privacy and security plan. Compliance oriented organizations are creating a culture of patient privacy compliance by employing privacy and auditing tools combined with processes and procedures that pervade the organization. Deploying fundamental technologies is a cornerstone of compliance work as it enables the organization to automate their accounting of disclosure responsibilities, detect healthcare privacy breaches and leverage their training and sanctioning processes.

Deploying technologies does not ensure compliance. A patient privacy and security plan must demonstrate effective use within the organization and permeate all business units, correspond with business processes and integrate with the business functions of the organization. Key indicators of an effective privacy and auditing plan include all of the following:

- Centralizing the audit logs of the electronic health record systems as well as all core applications that access PHI
- Fulfilling their accounting of accounting of disclosure responsibilities by automating privacy auditing reporting across the applications which access PHI
- Proactively detecting privacy breaches related to identity theft, medical identity theft, employee-patient snooping, as well as VIP, friends, family and neighbor snooping
- Ongoing mapping of training and sanctioning processes to achieve compliance

A patient privacy and security plan must demonstrate effective use within the organization and permeate all business units, correspond with business processes and integrate with the business functions of the organization.

This section of the survey was designed to determine if healthcare organizations are employing privacy and auditing tools for compliance in conjunction with establishing processes and procedures that demonstrate effective use throughout the organization and what challenges they face.

Leading healthcare organizations have already deployed key cornerstone privacy and security technologies.

- 7 percent of organizations have already deployed the following technologies: user privacy monitoring in EHRs, accounting of disclosure log aggregation, data leakage protection, patient and user privacy auditing, single sign-on, identity management and infrastructure log monitoring

A minority of surveyed healthcare organizations are demonstrating effective use of key privacy and auditing tools.

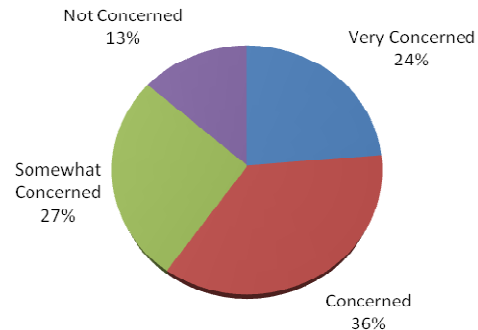
- Exactly half of the organizations surveyed stated they have *both* processes and systems in place to detect, report and prevent inappropriate access to patient records.

- Of the 108 organizations that stated they have *both* processes and systems in place to detect, report and prevent inappropriate access to patient records, only 23 percent of respondents have deployed the key privacy and auditing tools:
 - user privacy monitoring in EHRs
 - accounting of disclosure log aggregation
 - patient and privacy auditing and infrastructure log monitoring
- Of the remaining 83 organizations that state they have *both* processes and systems in place to detect, report and prevent inappropriate access to patient records, 15 have already deployed or expect to deploy user privacy monitoring in EHRs, accounting of disclosure log aggregation, patient and privacy auditing and infrastructure log monitoring within the next 6 months.

Organizations are concerned about the technology challenge of monitoring dozens of healthcare applications.

- 59.7 percent of respondents stated they were concerned or very concerned about overcoming the technology challenge of monitoring dozens of healthcare applications

Level of Concern Regarding the Technology Challenge of Monitoring Dozens of Healthcare Applications

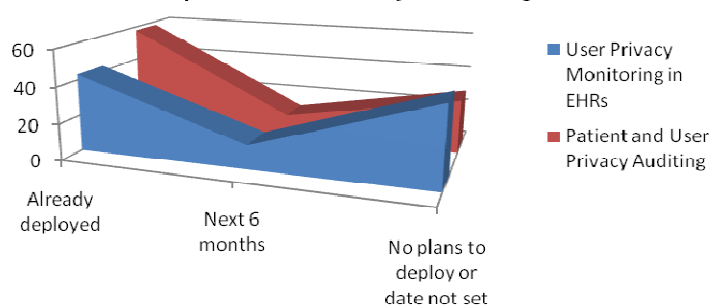


A substantial percentage of organizations have not yet leveraged key privacy and auditing technologies.

- 43.9 percent of respondents stated that their organization does not plan to deploy, or has yet to determine a deployment date for user privacy monitoring in EHRs.
- 29.6 percent of respondents stated that their organization does not plan to deploy, or has yet to determine a deployment date for patient and user privacy auditing.

59.7% of respondents stated they were concerned or very concerned about the technology challenge of monitoring dozens of healthcare applications.

Implementation of Key Technologies



Survey Analysis

Upon analysis, the survey revealed six key themes. Using cross-tabulation of answers to specific questions, the following assertions were evident.

Healthcare organizations are familiar with new healthcare privacy and security regulations, specifically ARRA HITECH and the FTC Red Flags Rule.

More than 90 percent of respondents stated they were familiar with the new laws. Respondents were able to answer questions about the laws; specific requirements detailed within the laws and rules, and were aware of the penalties associated with non-compliance.

Healthcare organizations are concerned with the reputational impact associated with a breach and breach notification requirements.

Several survey questions were developed to measure respondents' top concerns surrounding new legislation. When asked about top concerns relative to non-compliance, respondents overwhelmingly ranked scenarios that would negatively impact their organization's reputation at the top of the list. These concerns were greater than those associated with financial penalties or the possibility of a long-term resolution agreement with the government. Additionally, respondents were greatly concerned with having to notify patients, the media and the government should a breach occur. More respondents were concerned about the breach notification requirement than about being audited for compliance.

The healthcare industry is mobilizing to meet compliance requirements. Healthcare organizations have, are in process, or are planning to implement processes, procedures and critical technologies to meet compliance.

The survey reveals that healthcare organizations are spending money to implement technology solutions that will meet compliance requirements and fill critical security gaps. Patient and user privacy auditing had the highest deployment rate at 57.9 percent. Data leakage prevention and accounting of disclosure log aggregation were the least commonly deployed technologies, deployed in less than one third of the organizations. Consequently, these two technologies were expected to be deployed in 53.7 percent and 52.3 percent of organizations respectively. The survey also revealed that in many cases healthcare organizations are implementing several of the key technologies but not all, leaving a substantial security gap and a possible risk for non-compliance.

The majority of respondents, 94 percent, stated that they have processes in place to detect, report and prevent inappropriate access to patient records. Fifty-one percent of respondents stated they had automated systems in place to detect, report and prevent inappropriate access to patient records. Less than half of the respondents have both automated systems and processes.

Healthcare organizations are allocating budget to meet new privacy and security requirements.

Respondents report that their organizations are allocating budgets for compliance work and to achieve the priority of ensuring patient privacy. Less than 24 percent believe their organization has inappropriately budgeted to meet these two objectives.

The healthcare industry is beginning to believe that enforcement of these laws is a government priority.

Prior to the passage of ARRA HITECH and the expansion of the FTC Red Flags Rule to the healthcare industry, HIPAA was the primary healthcare privacy law. Until 2007, the government did little in the way of enforcement or audits. The Piedmont hospital audit marked a shift in the government's priority and interest in enforcement of patient privacy laws.

The survey reveals that the healthcare industry is beginning to believe that the government is now serious about enforcing healthcare privacy laws. Nearly one out of five of the respondents' organizations have already been audited by a state or federal entity. One-third of respondents believe that compared to 12 months ago, they have a greater chance of a state or federal privacy audit. More than half of the respondents are concerned about being audited for compliance. These numbers demonstrate that the government has begun to shift perceptions in the healthcare market regarding enforcement.

The healthcare industry is in need of further education to align spending and technology deployments to government expectations around compliance.

The survey reveals that healthcare organizations are mobilizing to meet compliance regulations. However, when respondents answer questions about specific technology deployments and processes to detect, prevent, report and monitor for privacy incidents, the answers reveal that the majority of these organizations are unclear of the government's expectations around compliance.

Specific to ARRA HITECH, survey responses demonstrate that healthcare organizations may not be aware of the need to implement and integrate automated systems to monitor audit and detect patient record access in an effort to meet accounting of disclosure requirements. Only 17 percent of respondents have deployed an accounting of disclosure log aggregation and patient and privacy auditing solution. Less than half of the respondents state they have both automated systems and processes to detect and prevent security and privacy issues. Although they are implementing critical technologies, a substantial percentage of these organizations have not yet demonstrated effective use or leveraged an integrated approach which combines processes and systems to detect and prevent security incidents.

Only 7 percent of respondents have deployed all seven critical technologies designed to close security gaps. Of the respondents that stated they believe they were in full compliance and audit ready, only 22 percent have deployed user privacy monitoring, accounting of disclosure log aggregation, and patient and user privacy auditing. These statistics demonstrate confusion in the industry about technologies and processes including internal training and sanctioning, necessary for a comprehensive privacy and security solution that will meet compliance requirements.

About FairWarning

FairWarning® is a leading supplier of privacy surveillance solutions for Electronic Health Records. **FairWarning®** patient privacy auditing and monitoring is essential for complying with recent privacy regulations such as ARRA HITECH / accounting of disclosures, FTC Red Flags Rule, HIPAA, California SB 541 & AB 211 and other State Laws, as well as UK & EU Data Protection Acts, NHS IGT guidelines and Canadian Provincial laws. Healthcare's leading organizations have deployed **FairWarning®** privacy surveillance solutions.

FairWarning® customers represent nearly 300 hospitals and over 1,000 clinics in the United States, Canada and United Kingdom. Customers include: Columbus Regional Hospital, Cookeville Regional Medical Center, Halifax Regional Health System, MemorialCare®, Memorial Healthcare System, Mercy Health Partners Hackley Campus, Meridian Health, NHS Lothian, St. Luke's Episcopal Hospital, Saint Luke's Health System, St. Dominic's Hospital, Swedish Health Services, University of Pittsburgh Medical Center (UPMC), University of California San Diego Medical Center and University of Minnesota Physicians, Weill Cornell Medical College.

FairWarning®'s production customers range in size from 1,000 to 70,000 users. The company's 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.

Forty-nine percent (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. Eighty-three percent (83 %) of FairWarning®'s customers reported having avoided the costs and exposure of privacy breaches by using **FairWarning®** privacy surveillance 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, Inc. was founded in 2005 based on the idea of delivering industry's first turn-key software solution for the proactive privacy auditing of Electronic Health Records, this idea is reflected in the company's mission today.

Kurt Long
CEO and Founder
 727-576-6700 x. 101
Kurt@FairWarningAudit.com

Sadie Peterson
Corporate & Product Marketing Manager
 727-576-6700 x. 119
Sadie@FairWarningAudit.com

Shane Whitlatch
Senior V.P. of Global Alliances & Sales Operations
 727-576-6700 x. 115
Shane@FairWarningAudit.com

Valerie Blount
Vice President of Customer & Product Operations
 727-576-6700 x. 114
Valerie@FairWarningAudit.com

About New London Consulting

New London Consulting is a research and strategy company. We are a consortium of senior executives who have come from frenetic mid-sized research and public relations boutiques and big-name global firms. Our work is customer driven and implemented according to the needs of each individual business partner. New London Consulting delivers a full spectrum of award-winning research, marketing and communications programs. Our clients span multiple industries including: technology, healthcare, beauty and communications. NLC is based in the Washington DC metropolitan area and has been in business since 2003.

Jennifer Stansbury

President

703-395-2888

JStansbury@NewLondonConsulting.com