WHITEPAPER

Patient privacy intelligence: the intersection of compliance, legal and information security

imprivata®

Preface

This whitepaper examines the critical capabilities that patient privacy intelligence solutions should possess in order to meet the business and technical demands of modern care providers for regulatory compliance and information security. Crucial to modern healthcare is the Electronic Health Record (EHR) as well as a wide-range of healthcare applications used in the course of patient care. Since these systems hold vast amounts of patient information, they are a focal point of regulatory enforcement. HIPAA in the United States is just one example. Patient information is also a target of internal and external information security adversaries with a growing list of motivations that include identity theft, tax fraud, medical identity theft, ransom, espionage, and political hacktivism. According to CIO Magazine, the forecast for healthcare security in 2017 is that nation-state attacks will move from espionage to cyberwar. And, healthcare will be the most targeted industry.

First generation solutions which monitor end-user access to patient information held in EHRs and applications are categorized as Patient Privacy Monitoring (PPM). PPM solutions automate batch analysis on EHR and application audit logs to detect potential breaches and conduct audit reports. PPM solutions fell behind in care providers' needs as the healthcare industry evolved and information security threats escalated. Specifically, PPM solutions lack support for cloud, big data, realtime, extreme scale, and advanced identityaware behavioral analytics. PPM solutions are architecturally closed systems, lacking the ability to collaborate with third-party products in multilayer information security strategies. PPM solutions also leave care providers vulnerable to internal and external threats targeting EHRs and applications.

In this whitepaper:

Patient privacy intelligence

Patient privacy intelligence solutions are the industry's latest innovation to address the need for next-generation compliance and information security. These solutions are front and center in multilayer strategies to secure patient data held in EHRs, clinical applications, and **increasingly in cloud** and **big data applications.** Compliance offices use patient privacy intelligence as a foundation for satisfying key provisions of the OCR's **HIPAA Audit protocol**, Meaningful Use attestations, and EPCS certification.

The OCR has dramatically escalated HIPAA enforcement in recent years. Information security offices use patient privacy intelligence to detect and prevent threats such as compromised user credentials, rogue insider attacks, and collaborative insider attacks. They also use patient privacy intelligence to conduct forensic investigations. Information security adversaries recognize applications on premise and in the cloud as a weak link in the information security chain. These and other factors have driven Imprivata Patient Privacy Intelligence (formerly Imprivata FairWarning Patient Privacy Intelligence) into becoming an identity-aware, business critical, real-time capable, predictive, compliance, and information security platform complete with dashboards and governance, forensics, visualization, behavioral analysis, and advanced filtering that is open and collaborative with third-party security solutions.

Foundations – data integrity and governance

Healthcare has become highly specialized and collaborative. This has carried over into Healthcare Information Technology environments which are highly diverse, specialized, and very dynamic. Care providers have dozens or even hundreds of applications containing Patient Health Information (PHI), usually with a core EHR as the center-piece. Although, this can vary especially with merger and acquisition activity resulting in combined entities with different EHRs. Using these applications are dozens, hundreds, or even thousands of clinical and administrative end-users. End-user information is almost always maintained "stove-piped" within the applications with different information held in each. Few care providers have reached nirvana in centralizing all user information into a single provisioning system that is compatible with all of their applications.

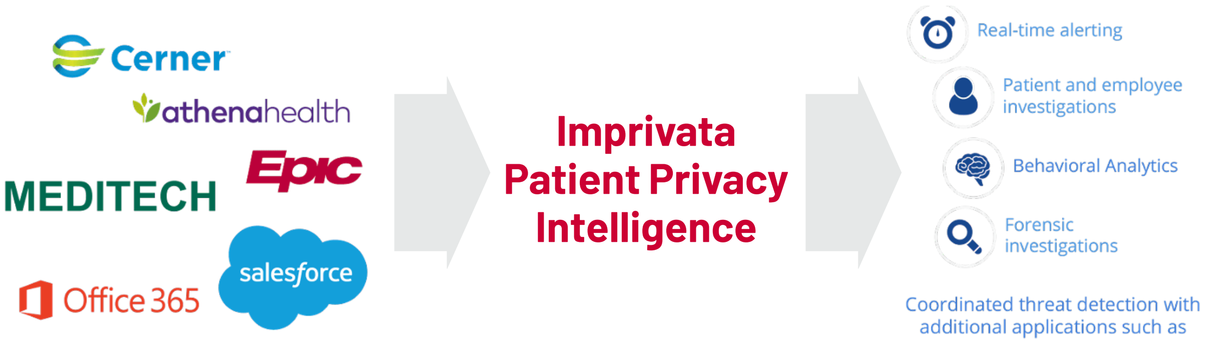
Diverse and dynamic applications containing PHI, each with many dynamic end users, drive three core architectural requirements for a patient privacy intelligence platform.

1. APPLICATION SECURITY INTELLIGENCE

Healthcare providers have dozens or even hundreds of applications which hold PHI. HIPAA, forensics investigations, and information security analytics drive a clear requirement for patient privacy intelligence platforms to flexibly support this wide-range of applications within one product platform, and a "single-pane-of-glass." HIPAA, for example, mandates the systematic review of all systems which access PHI through the examination of audit trails. It is highly desirable that a single solution fulfill this core requirement for ease and expense purposes alone. Thus, it is highly desirable that a patient privacy intelligence solution have an architecture designed for massive flexibility in application support. Due to this forethought in architecture, our Imprivata Patient Privacy Intelligence solution supports more than 150+ applications in production customer environments.

Vendors like Epic, Cerner, MEDITECH, athenahealth, eClinicalWorks, and others routinely change the content of their audit logs and even the meaning of field values. This has significant implications for the data integrity of patient privacy intelligence platforms. When the meaning of fields or the addition of fields occurs in audit logs, the basic accuracy of forensic investigations, audits, analytics, and filtering changes. This jeopardizes the validity of eDiscovery, HIPAA compliance, information security analytics, and every aspect of a patient privacy intelligence platform.

The implications are that highly attentive and collaborative efforts between the patient privacy intelligence vendors, application vendors and customers must be carried out vigilantly in order to maintain data integrity. We have fulfilled this requirement through our Imprivata Patient Privacy Intelligence Ready program. As part of this effort we collaborate with every EHR vendor of significance on a proactive basis.


Cerner
athenahealth
Epic
MEDITECH
salesforce
Office 365
Imprivata Patient Privacy Intelligence
Real-time alerting
Patient and employee investigations
Behavioral Analytics
Forensic investigations
Coordinated threat detection with additional applications such as

Application security intelligence

A foundational benefit of Imprivata Patient Privacy Intelligence is its ability to correlate fields based on their meaning across all of a healthcare provider's EHRs and applications. Furthermore, we maintain a dedicated team that collaborates with EHR and application vendors in order to coordinate audit log changes. We call this program the Imprivata Patient Privacy Intelligence Ready Program, and we support more than 150 applications. Our application security intelligence architecture, and associated service program with application vendors, ensures care providers receive uninterrupted service and have accurate data in Imprivata Patient Privacy Intelligence. Imprivata holds patents for its approach to application security intelligence.

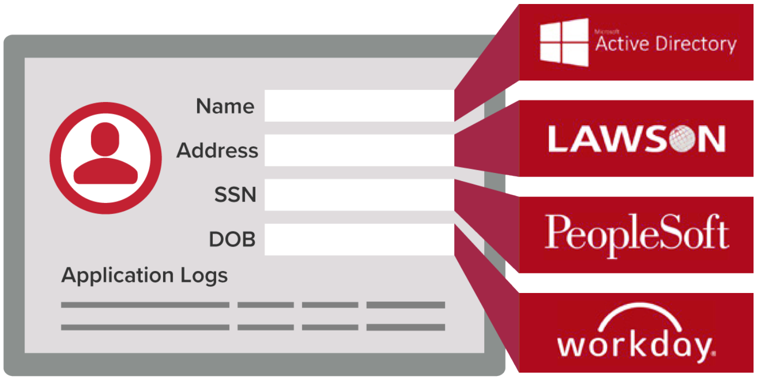
2. CORRELATION OF USER IDENTITY AND DATA ACCURACY

Patient privacy intelligence solutions use end-user information to fulfill forensic investigations on patient complaints, information security investigations, behavioral analytics, algorithms, and filtering. As described above, end-user information is almost always stovepiped within the applications with different information held in each.

End-user information is dynamic, and over time the information becomes inaccurate. Examples of dynamic end-user data include name changes from maiden to married as well as home address, work address, title, and department changes. Even the basic status such as employee, terminated, research only, or contracted may change.

3. DATA INTEGRITY MONITORING

Because patient privacy intelligence solutions continually consume data from dynamic application audit logs such as user identity sources as well as dynamic information on patients, they must be monitored for data integrity. As an example, if audit logs or identity information is not delivered due to a network issue or application change, the data integrity of the patient privacy intelligence solution is compromised. Without daily data integrity monitoring, the data goes undelivered. Typically, the problem of missing data is not discovered until an investigation driven by lawsuit, patient complaint, or suspected breach. We've seen this problem in hundreds of deployments.



Identity intelligence

A second foundational component of Imprivata Patient Privacy Intelligence is identity intelligence, which is purpose-built to interface with user management systems such as Lawson, PeopleSoft, WorkDay, Active Directory, and other applications. Identity intelligence correlates user information from all of a care provider's sources in order to centralize the most accurate information available about a user. Correlation and accuracy of user information is essential to legally defensible forensic eDiscovery, behavioral analytics, filtering, and learning algorithms. Additionally, some care providers have successfully implemented user provisioning systems from commercial vendors, or they may have written their own. In these cases, the Imprivata Ready program has an open interface that builds accurate and correlated user identity into the foundation of the platform. Imprivata holds a patent for its identity intelligence approach to producing accurate user-identity information.

Data integrity monitoring

The foundation of regulatory compliance, legal defensibility, and information security. Solutions and vendors without data integrity monitoring put their customers in the position of discovering data integrity issues during forensic investigations of security incidents, patient complaints, and lawsuits, or during cooperation with law enforcement. New patient privacy intelligence vendors tend to spend money on market awareness and sales as well as single product features. Yet, they under-invest in critical service infrastructure. By under-investing in the infrastructure of service and data integrity monitoring, the "solutions" they offer leave their customers open to the risk of discovering data integrity issues when it is too late.

Certifications dependent on data integrity and governance

There are numerous certifications which are business critical to the healthcare industry and rely on data integrity, governance, and information security best practices. These certifications are required of vendors in order for their care provider customers to receive governmental funding for Meaningful Use and operating certain aspects of the care provider's business. Recognized industry certifications from unbiased third parties, along with customer references, also play an important role in evaluating vendor claims.

THIRD PARTY CERTIFICATIONS

We've architected Imprivata Patient Privacy Intelligence with data integrity and governance in mind. And third parties have certified it to meet these standards.

Meaningful Use (MU) — Patient Privacy Intelligence is part of the Electronic Health Record and must be certified in order for care providers to collect MU funds. INFO|GARD performed our certification testing.

Electronic Prescribing Controlled Substances (EPCS) — Patient Privacy Intelligence participates in the prescribing process in certain circumstances and must be certified in a DEA- EPCS Certification Audit.

Office for Civil Rights HIPAA Audits — Because of the scale of our customer base, our care provider customers have been extensively scrutinized by the Office for Civil Rights (OCR) and have successfully demonstrated satisfaction of key HIPAA requirements using our Patient Privacy Intelligence (PPI) platform.

Open Web Application Security Project (OWASP) — On a recurring basis, we conduct OWASP application security testing to detect common vulnerabilities.

Salesforce Cloud Security Certification — Our application is certified by Salesforce's extensive testing for cloud security in order to appear in the AppExchange.

Court cases and lawsuits — Our platform has withstood the extreme scrutiny of countless court cases which required eDiscovery. In each of these cases, data integrity was a crucial consideration. Information security certifications for a Business Associate as well as their technology are crucial for care providers evaluating breach and OCR audit risks.

SOC 2 Type 2 — Our solutions and business have received SOC 2 Type 2 certification. This includes recurring testing such as ZAP Penetration Testing and Nessus Vulnerability Scans of the operating system and application.

Business critical

Patient privacy intelligence platforms without a foundational architecture of data integrity and governance are at high risk of failing to receive third party certifications. In certain circumstances, this jeopardizes their customers' ability to receive MU funding and operate electronic prescription. Furthermore, a lack of third-party certifications and scrutiny are indicative of business associates who are prone to breaches and putting their customers at risk. Their platform may not withstand eDiscovery process associated with wrongful termination and malpractice lawsuits. Finally, platforms without third party certifications, testing, and scrutiny present high risk associated with OCR HIPAA audits which are specifically targeting capabilities associated with patient privacy intelligence.

Healthcare business drivers

With the foundation of data integrity, governance and information security detailed, we can begin to examine the business drivers shaping patient privacy intelligence. There is an important philosophical point to make now. The role of our technology and solutions are to serve our customers' business. All too often, business serves technology resulting in the failure to deliver business value. We examine Imprivata Patient Privacy Intelligence within the context of business drivers our healthcare customers face. Here are six key business drivers for our customers.

1. INDUSTRY COMPETITION, MERGERS AND ACQUISITIONS

Merger and Acquisition activity is impacting the thinking of every care provider. There are three basic decisions to make: acquire or merge with other care providers, form local partnerships, or get acquired. This has a dramatic impact on scale, flexibility, availability, and service level strategies for Imprivata Patient Privacy Intelligence.

2. HIPAA ENFORCEMENT, HITECH, STATE LAWS

The impact of increased HIPAA enforcement and associated privacy requirements mandated by HITECH, as well as state laws such as those in California, Florida, Texas, New York, and Massachusetts. Imprivata Patient Privacy Intelligence satisfies core requirements in HIPAA, state, and international security frameworks that mandate the systematic review of systems which access PHI through the examination of audit trails and related information. There were a record 12 Resolution Agreements issued in 2016 alone. And, in 2017 there were already three by February 1st.

3. ESCALATING INFORMATION SECURITY THREATS

Dramatically escalating information security threats that are being perpetrated by new adversaries with motivations never foreseen drive new analytic, visualization, real-time, and filtering requirements Furthermore, the healthcare industry, long a target of lawsuits, is now using audit logs including legally defensible forensics investigations in wrongful termination and malpractice suits. This raises the stakes for patient privacy intelligence.

4. CLOUD AND BIG DATA FOR IMPROVED, AFFORDABLE OUTCOMES

Rapid cloud and big data adoption by care providers is resulting in the propagation of PHI. Information security and governance is immature in these areas for almost all vendors. This results in information security risks and noncompliance for healthcare organizations using these technologies.

5. SKILLS SHORTAGES

Information security and privacy skills shortages are particularly prevalent in healthcare. For a variety of reasons, including mergers and acquisition, attrition, and reduction, experts are in scarce supply. This requires new and flexible staffing strategies as well as improved individual productivity.

6. REIMBURSEMENTS UNCERTAINTY

Uncertain reimbursement models for care providers, with the Affordable Care Act at the focal point, require that care providers have affordable and flexible staffing and operational expense strategies across their business. This includes information security, privacy, and governance.

Solution features and requirements by business driver

1. INDUSTRY COMPETITION, MERGERS AND ACQUISITIONS

The care provider industry is consolidating at an incredibly rapid pace. Mergers and acquisitions show no sign of abating and they are producing healthcare organizations at never before seen size and scale. This has serious ramifications to patient privacy intelligence solutions outlined below:

- **Extreme scale and proactive service monitoring —** Every day, patient privacy intelligence solutions must consume vast amounts of audit data, analyze that data, and prepare that data for users. The enormous volume of this data requires highly-tuned technology. Because patient privacy intelligence is business critical, the platform must be ready for use every day. At this new scale, proactive service levels must be monitored. Also required is a significant investment in technical monitoring and associated infrastructure, dedicated personnel, and processes for resolving small problems, thereby nipping small issues in the bud before they become large problems. Furthermore, disciplined change control and escalation processes are required. Care providers with vast amounts of data cannot function using vendors who have not foreseen service level challenges and operate under a "break-fix" model.

- **Change control and planned maintenance windows —** Care providers operating at scale must have controlled processes in their information technology environment in order to maintain data integrity and satisfy their own governance requirements. Because patient privacy intelligence has become business critical, it is essential that solutions are operated with availability, change control for patches, updates, data changes, and upgrades. Change control is often associated with planned maintenance windows that both vendor and customer agree upon.
- **Extreme flexibility in supporting multiple EHRs and applications —** We have already covered the need for supporting a wide-range of EHRs and applications, and when entities merge. It only highlights this need further. Care providers cannot immediately rationalize into a single EHR and application platform. And, they may need years to execute their "acquisition rationalization" plan. Thus, they need extreme flexibility from their patient privacy intelligence platform.
- **Support for community-based electronic health records —** Some care providers are creating local and regional partnerships which share the investment and operational expense of leading electronic health records — Patient Privacy Intelligence solutions must support these shared models in order to meet the business strategy needs. The most common solutions are Epic Community Connect and Cerner Works.
- **Software as a service (SaaS) and on-premise solutions with service monitoring —** Care providers of all sizes, including those with massive scale, need flexible options for the operations of their regional providers. Or, if their strategy is to immediately rationalize acquisition costs, they need massively scalable technology as discussed above. Regardless of whether the deployment is a small software-as-a-service model, or a massively scalable on-premise solution, it is necessary to have proactive service monitoring and data integrity monitoring.

Extreme scale, change control, and governance flexibility

Patient privacy intelligence solution vendors should provide referenceable customers attesting to their products' ability for extreme scale, extreme flexibility in supporting applications, and the vendor's ability to operationalize change control and governance. Even for small and medium sized care providers, investment in solutions from vendors who cannot provide references of scale are suspect. And, in the current M&A environment, they represent a high business risk. This is because care providers making acquisitions view technologies and vendors who cannot scale as a liability in the care provider being acquired. Additionally, as acquiring organizations recognize the necessity of information security, they view vendors and products without a track record as liabilities. Finally, care providers of scale require proactive service monitoring and clear escalation processes because small problems must be addressed quickly before they become large-scale availability issues.

2. HIPAA ENFORCEMENT, HITECH STATE LAWS

The American Recovery and Reinvestment Act of 2009, The Health Information Technology for Economic and Clinical Health Act (HITECH), and the associated Omnibus Rule significantly strengthened HIPAA. These regulations mandated HIPAA enforcement by the OCR as well as new congressional reporting requirements. Additionally, these regulations put into place privacy laws that include impactful mandates in the occurrence of a breach, including:

- Disclosure of a breach to the impacted patients
- Notification of a breach to the Department of Health and Human Services
- Media notification in the event of a breach impacting 500 or more patients
- Pivoting the harm standard to require the care provider to prove a patient's record had not been breached through a "Risk of Compromise" guideline

HITECH also added provisions for greater monetary penalties for care providers suffering breaches and found to be noncompliant with HIPAA. Furthermore, escalated consequences were added for those found to be in willful neglect. Finally, attestation for HITECH MU funding was tied to key HIPAA provisions including those fulfilled by Imprivata Patient Privacy Intelligence.

In recent years, the OCR has conducted record numbers of HIPAA audits. Additionally, in 2016, it issued a record number of Resolution Agreements with associated payments required by care providers. Not surprisingly, the OCR has also issued three Resolution Agreements in January 2017 alone.

Implications of HIPAA and HITECH

The implications for a patient privacy intelligence platform are vast. HITECH transformed HIPAA from a patient-compliant driven system in which patients had very few actual rights, into a framework that requires the proactive detection of potential patient breaches, the assessment of all potential breaches for risk of compromise, conducting and tracking investigations of all potential breaches, notification to the OCR in the event of a breach, notification to the media if greater than 500 patients are impacted, and disclosure of the breach to the affected patients.

These obligations require new capabilities in order to organize, streamline, and report on patient privacy intelligence activities. Especially important is the ability to demonstrate policies and controls of key HIPAA requirements to the OCR and internal auditors.

Some of the important requirements include:

- **Investigation management** – The ability to create automated reports on potential incidents, including open cases, those closed with incident, those closed without incident, patients impacted, notification time period, days open, and more.
- **Risk of compromise assessments** – An automated process for assessing the need to report the potential incident as a breach.
- **Advanced filtering** – Intelligent and multipronge approach in reducing false positives.
- **Workflow enablement** – As potential incidents are discovered they must be tracked and collaboration must be performed with the care provider to determine if a breach has occurred.
- **Governance dashboards** – Dashboards provide the ability to quickly demonstrate fulfillment of key HIPAA requirements through policy, control, and attestation.
- **Security controls** – Because patient privacy intelligence solutions handle PHI, the solution itself is subject to HIPAA requirements and must satisfy authentication, authorization, user provisioning, as well as production and review of audit logs. These and other controls are mandated for MU certification.

All of the above requirements can be found in Imprivata Patient Privacy Intelligence, including our certification under MU. We have dozens of care provider customers who have successfully attested for MU funds with our MU-certified solutions.

REFERENCEABLE ABILITY TO SATISFY HIPAA AUDITS AND ATTEST FOR MU

The OCR's continued HIPAA audits and its issuance of increasingly punitive Resolution Agreements have raised the stakes for care providers. Patient privacy intelligence vendors who have not built in investigation management, risk of compromise assessment, notification, and disclosure workflows into their products put their customers in the position of the spreadsheet nightmare — tracking incidents through Excel. This tracking method is error-prone and does not support "chain of custody" in accurately maintaining information on potential incidents, thus jeopardizing the validity of incident tracking practices in patient complaints, HIPAA, and eDiscovery. Furthermore, vendors who have not built in proper security and data integrity controls may be unable to have their products certified for MU, jeopardizing their customers' ability to attest for MU payments. Finally, vendors should have referenceable customers who can attest to their ability to successfully pass OCR HIPAA audits.

ESCALATING INFORMATION SECURITY THREATS

Patient privacy intelligence is still useful in detecting, "snooping," and complying with core HIPAA requirements. However, healthcare has been besieged with escalated threats including:

- Financial identity theft of patients and employees, including physician credentials
- Financial identity theft of children, the elderly, and the vulnerable
- Medical identity theft, including large-scale fraud spread by leveraging stolen PHI and physician information
- IRS tax fraud using patient and employee information to submit false income tax returns
- Organized crime saw the ease and scale of theft that could be perpetrated and targeted healthcare
- Nation-states and hacktivists have successfully sought to gain access to sensitive PHI for political embarrassment and espionage purposes
- Ransom-based attacks aimed at server or data hostage for money has become prevalent

In addition to the financial, emotional, spiritual, and professional damage to patients and employees, care providers have suffered reputation damage, civil lawsuits, and the scrutiny of the OCR.

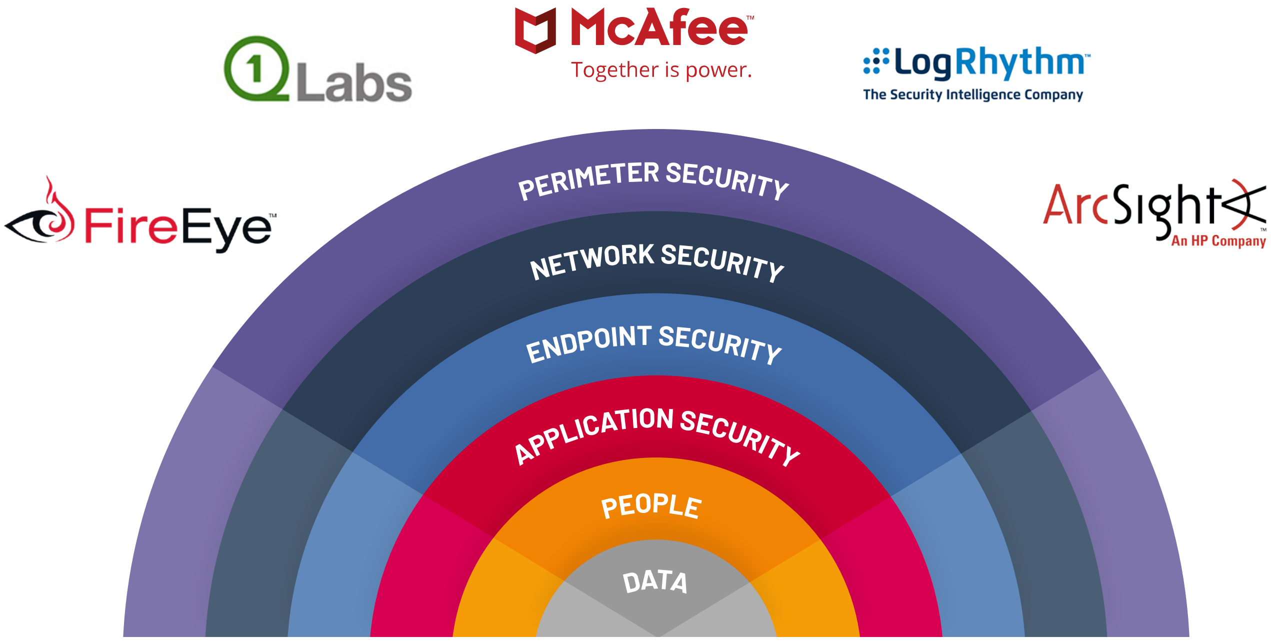
Leading chief information security officers (CISOs) have taken a multilayered security approach to perimeter security as well as security measures for applications. This approach requires a broad set of capabilities for patient privacy intelligence platforms as well as overlap and open cooperation with third party information security solutions through API integration. The capabilities in Imprivata Patient Privacy Intelligence anticipated these demands and are used in parallel to proactively discover users with compromised credentials, or to detect rogue employee attacks or collaborative attacks on EHRs and applications.

Imprivata Patient Privacy Intelligence is proven for the following:

- Forensic investigations tested through eDiscovery in lawsuits and cooperation with law enforcement
- Both standard and ad-hoc visualization for any report
- Behavioral analytics on users including trending, statistical analysis, and algorithms
- Monitoring and alerting
- Predictive
- Advanced filtering leveraging data integrity capabilities
- Real-time incident detection capabilities
- Open API collaboration with third-party information security vendors

“All of the above” information security capabilities

Leading CISOs are taking a new approach to securing the care provider environment. They are assuming they have been breached and spend the day proving that their systems, including their EHR and important clinical applications, are “clean.” This paradigm change has come about from the success of phishing attacks that focus on end users. The attacks target systems holding protected health information (and employee data) such as EHRs, clinical applications, and enterprise management applications. The hacktivist group Anonymous has taken this approach in breaching care providers with intent of embarrassing government officials by disclosing sensitive patient information. In these types of events, forensics investigations must be used to prove or disprove a breach. With heightening stakes, patient privacy intelligence platforms must have the real-time capability to respond instantaneously to potential threats so the potential damage can be quickly mitigated. Imprivata Patient Privacy Intelligence helps CISOs with an “all of the above approach” through API integration with leading information security vendors. Vendors focusing on a single technique are taking a single-layer of security approach and open their customers up to potential breaches. Furthermore, vendors without open API coordination with leading information security vendors are an important indicator of an immature solution offering.



CLOUD AND BIG DATA FOR IMPROVED AND AFFORDABLE OUTCOMES

The healthcare industry is rapidly adopting cloud solutions in order to reduce operational and capital expenditures while delivering improved information technology service levels. Cloud solutions range from entire health record suites and clinical applications to cloud-based productivity applications like Office 365, Salesforce, Health Cloud, and others. In all cases, it is highly likely that PHI is being transferred and stored in “the cloud.” The cloud is powerful. However, it is still subject to auditing requirements specified by HIPAA as well as information security risks. A Forbes article reported that 83% of care providers are using cloud services. And, the number is growing.

Big data applications like Hadoop and its derivatives are also being rapidly adopted to improve clinical outcomes. In a recent article, McKinsey & Company called this phenomenon "The Big Data Revolution in US Healthcare: Accelerating Value and Innovation." These technologies, whether used on premise or in the cloud, use "horizontal scaling" and propagate PHI across the connected network. Big data applications hold PHI and are also subject to the auditing requirements by HIPAA.

Imprivata Patient Privacy Intelligence enables simultaneous support for traditional EHRs, clinical applications, cloud-based applications, as well as big data applications in a single instance and in a single user interface. This reduces operational and personnel costs and positions our customers for any future they choose.

Cloud and big data in healthcare

Healthcare is putting **PHI** and **big data applications** in the Cloud at an accelerated pace. Cloud and big data solutions which hold PHI are subject to HIPAA requirements in the same way as on premise solutions. Simultaneously, care providers are maintaining some of their applications, and perhaps their EHR, on premise. Our Patient Privacy Intelligence solution enables our customer to support all of these options in a single instance, thereby reducing costs and creating massive flexibility. Patient Privacy Intelligence vendors whose technologies are immature cannot offer this flexibility. And, they are unable to offer flexible options to their customers in the future. Vendors make many claims during the sales cycle. Be sure to talk to referenceable customers. And, ask for as many case studies as possible in which the customer is named and can be contacted.

SKILLS SHORTAGES

The healthcare industry is suffering from a skills shortage in the area of operating their information security and privacy programs. Compounding this is reduction of staff due to either consolidation strategiesor attrition as healthcare providers contemplate their future creating uncertainty for their staff. For information security and privacy professionals, it is easy to change industries from healthcare to finance where there is also a skills shortage. However, the pay is generally more aggressive.

The implications are that care providers need options that are flexible and provide affordability of operations. These options include:

- The ability to hire previously certified patient privacy intelligence experts
- Affordable training and certification programs for developing their own personnel
- Free of charge basic training and best practices
- Outsourced staffing models providing experts at rates below what they could hire comparable staff
- We have operated Imprivata certified training and have graduated over 400 privacy and security professionals

Risks and threats in times of uncertainty

Information security, regulatory risks, and threat of lawsuits do not go away during times of uncertainty. In fact, care providers underinvesting in compliance, privacy, and information security are putting themselves at greater risk than ever. That's because they may be unable to withstand a failed audit or civil lawsuits that may result from an information security breach. These are all liabilities within the context of Merger and Acquisition activity as well. Care providers should partner with expert vendors who provide options and affordability in regards to operating security and governance programs.

REIMBURSEMENTS UNCERTAINTY

The political climate has created reimbursements uncertainty for some care providers. In these circumstances, care providers need flexibility and affordability in the continued operations of their compliance, privacy, and information security programs. It is highly unlikely they will be able to initiate a major information security initiative within the context of uncertainty.

Critical capabilities overview

Below is a critical capabilities overview of patient privacy intelligence solutions from the care provider perspective:

COMPLIANCE

Care Providers leverage patient privacy intelligence as a foundation of HIPAA compliance asboutlined in the HIPAA audit protocol as well as MU and EPCS. Patient privacy intelligence solutions must have crucial capabilities driven by HITECH and the associated Omnibus Rule as out-of-the-box features to meet the challenges of increased OCR HIPAA enforcement as well as meeting MU and EPCS requirements.

INFORMATION SECURITY

Patient privacy intelligence is now critical to multi-layer information security strategies and must have an open architecture based on APIs and standards in order to interface with third-party vendors. Patient privacy intelligence solutions should have a rich feature set out-of-the-box that includes forensics, visualization, behavioral analytics, advanced filtering, real-time capability, and predictive learning. An "all of the above" information security strategy must be supported as adversaries have constantly changing tactics in an industry besieged by growing threats. PHI is the last layer of defense against phishing attacks.

LEGAL, RISK AND LAW ENFORCEMENT

The examination of audits trails has long been used in wrongful termination suits. Now they are increasingly being used in malpractice lawsuits. A critical implication for patient privacy intelligence solutions is that the assurance of data integrity is now a critical capability more than ever patient privacy intelligence solutions should have a track record of withstanding eDiscovery in lawsuits and law enforcement investigations.

PROACTIVE DATA MONITORING

Patient privacy intelligence solutions are now foundational to regulatory compliance, information security, certifications tied to MU funding, and business operations certifications such as EPCS, and legal defensibility. As such, patient privacy intelligence solutions are business critical to care providers. That makes proactive data integrity monitoring a very important capability. Mature availability, change control, maintenance, and upgrade capabilities and processes are essential to uninterrupted operations.

FLEXIBILITY

Massive flexibility for EHR and application support is essential. That's because cloud and big data are both growing at exponential pace within care provider environments as they maintain their traditional EHRs and clinical applications. Patient privacy intelligence solutions should have a specific architecture capable of resolving the fact that care provider end user information is stove-piped across applications and is dynamic, thus jeopardizing data integrity.

SUPPORT FOR BUSINESS GOALS INCLUDING CARE PROVIDER M&A STRATEGIES

Patient privacy intelligence solutions should also be architected to serve care providers' business goals which include their merger and acquisition strategy. Capabilities which are critical include extreme scale evidenced by customer references, broad application and EHR support, monitoring of data integrity, change control processes and proactive service monitoring, as well as availability of certified professionals and flexible training programs. Flexible staffing options, which reduce cost and increase expertise in times of reimbursement uncertainty, are a plus.

VERIFIABLE SECURITY PRACTICES AND CERTIFICATIONS

Because patient privacy intelligence solutions manage vast amounts of patient information, the information security practices and certifications of patient privacy intelligence vendors should be highly scrutinized. That's because poor application security or business security could result in a care provider breach. Formal certifications and third-party evidence should be required in all business associate claims on information security.

Vendor claims should be validated by third party certifications such as SOC 2 Type 2, MU certification, formal application security testing, and EPCS certification. Claims should also be validated in case studies which cite customer names and direct references to care providers using the vendor's solution in a production environment.

The importance of sound patient privacy intelligence

Patient privacy intelligence has become a business-critical platform for modern care providers because it is used for regulatory compliance, information security, and lawsuits. As OCR escalated HIPAA enforcement and information security threats to the healthcare industry are heightened, the importance and usage of patient privacy intelligence has dramatically increased in order to comply with HIPAA and protect the vast amounts of patient information held in EHRs and applications. Organized crime and adversaries with wide ranging motivations continue to target patient information for use in identity theft, tax fraud, medical identity theft, ransom, espionage to political hacktivism. All signals are that the health care industry will continue to be besieged with attacks escalating the stakes for all involved.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

Copyright © 2024 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.