

DATASHEET

Imprivata Patient Privacy Intelligence (formerly Imprivata FairWarning) vs. other patient privacy monitoring solutions



Imprivata Patient Privacy Intelligence (formerly Imprivata FairWarning) is the top solution in patient privacy monitoring across all areas within compliance: alerting, investigations, reporting, analytics, and user experience. Our solution helps you comply with confidence, protect the privacy of patient data, and prevent violations. These capabilities aid in the creation of a culture of privacy, while also supporting risk reduction.

Unlike other solutions on the market, Imprivata Patient Privacy Intelligence (PPI) is a complete risk analytics and intelligence solution. PPI supports the most integrations of any platform and can provide you with visibility into more user activity and anomalous behavior. When paired with Imprivata Enterprise Access Management (formerly Imprivata OneSign and Imprivata Confirm ID), PPI delivers a single identity intelligence and monitoring solution for each user across EHRs and applications, a capability the competition cannot offer.

Functionality	The Imprivata difference	Other solutions
Data element flexibility	The Imprivata difference: PPI allows for data elements to be updated within the platform to help decrease false positives. For example, if a staff member moves addresses, the PPI solution can update that address to ensure alerts for neighbor snooping are accurate.	Other solutions: In other solutions, temporal constraints are set, meaning data elements are held forever, impacting alerts such as coworker, neighbor, and same household.
Reactive auditing	PPI allows you to search on every access within the EHR to perform reactive audits. Searches will display accesses ranked by risk, and marked appropriately if the system feels the access is suspicious. With explanations for each access to understand why it is suspicious to start the investigation process.	No other solution on the market can conduct reactive searches and report back with the ranked, suspicious access for review.

Functionality	The Imprivata difference	Other solutions
Proactive auditing	PPI provides explanations for every access within the EHR to detect the 99% of appropriate accesses. Leaving your team with only the 1% of truly suspicious accesses, ranked according to risk, so you can audit and investigate efficiently.	All solutions on the market utilize Artificial Intelligence to identify privacy violations, but none provide the level of detail about each access that PPI brings.
Full incident management capabilities	Health systems can manage the entire process from alerts to investigations within PPI. Select from a library of reports and charts to assist with an audit or internal review. On top of that, all incidents, even those that were auto closed alerts, can be reviewed and logs can be accessed for information. This helps show why an alert was closed even if determined appropriate for potential OCR auditing	Not all solutions offer a full incident management platform, nor do they have robust reporting capabilities. Other solutions that don't alert on incidents due to low risk do not provide the ability for users to go back into those incidents and view the logs to understand why the incident was closed.
Alert volume threshold	PPI enables customers to set a maximum number of alerts to be reviewed that are ranked by risk to allow for better prioritization. Combined with the ability to incorporate machine learning scenarios that provide the ability to configure detailed policies on a high, medium, or low threshold to close access that meet that detailed policy – users have more control over reducing false positives.	Other solutions do offer alert volumes by policy, but closes all other alerts, even if the alert was risky enough to be reviewed. This does not provide as much flexibility and increases the risk of missed anomalous behaviors.
Identity management across application ecosystem	PPI integrates with HR and other enterprise applications. When integrated with Enterprise Access Management as the identity source, users are given a global perspective on a user's digital identity that cannot be matched.	Only PPI integrates with Enterprise Access Management, and other solutions can sometimes have other integration lacks such as not integrating with HR tools.
Managed Services	PPI provides optional compliance and privacy managed services professionals for healthcare systems that may need additional resources to support their efforts.	Some solutions state that managed services are not required. However, they have begun to offer them to meet the needs of their customers who do not want to rely solely on automated alerts or may have resource constraints.



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 1 781 674 2700 or visit us online at www.imprivata.com

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.

DATASHEET

Reducing risk, protecting patients

Patient privacy monitoring with
Patient Privacy Intelligence (formerly
FairWarning)



Imprivata Patient Privacy Intelligence (formerly FairWarning) helps you meet compliance standards through managing the full lifecycle of patient access auditing.

Equipped with artificial intelligence, machine learning, and behavioral analytics capabilities, our solution helps healthcare organizations strengthen their compliance posture and meet privacy monitoring goals.

Benefits of Patient Privacy Intelligence (PPI)



EFFICIENT INVESTIGATIONS

A full investigation module with navigation to easily move through the investigation process and highlighting of key documentation areas for investigations to help quickly resolve compliance issues.



REACTIVE AUDITING

Respond to patient complaints quickly with the ability to search on all accesses, get instant awareness into what users are doing at the event level, and see what to focus on with indicators and risk scores.



PROACTIVE AUDITING

Receive alerts on suspicious accesses that need to be reviewed and gather insights for investigations with a full view into each access to review what specific actions were taken in the access log.



ROBUST REPORTING

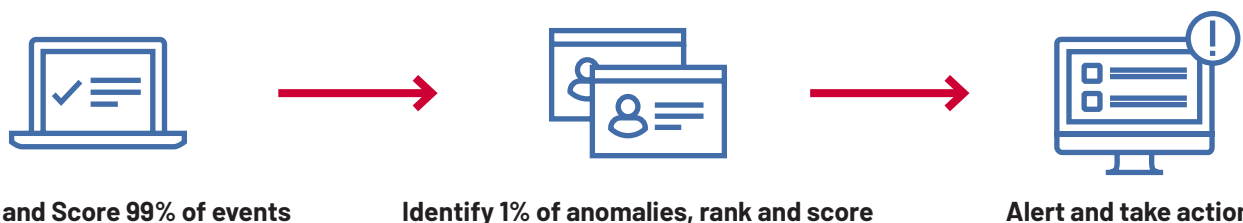
With over 100+ out-of-the-box reports and the ability to produce custom reports, your organization can quickly compile data that meets compliance standards and helps your organization understand user behavior.

Key Capabilities of PPI

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Utilizing artificial intelligence (AI), and machine learning, PPI allows you to proactively detect high-risk activities. By combining the two processes, the system can identify instances of known and unknown anomaly types.

Focus on what needs to be addressed by allowing the solution to review 99% of the access log, presenting you with the 1% of accesses that are truly suspicious. Those accesses are ranked and analyzed for possible violations with PPI Artificial Intelligence Risk scores and access explanations for fast insight into what accesses need to be prioritized for review.



Utilize alert limits to set daily alert thresholds to ensure focus on the highest risk accesses and machine learning scenarios. Identify new risks, reduce overall risk, and save time to focus on additional aspects of your privacy and compliance program.

INTEGRATIONS

PPI is the only patient privacy monitoring solution that integrates with Imprivata Enterprise Access Management (formerly OneSign) to provide a detailed view of anomalous user activity across applications for a full scope of potential user risk. Combined with PPI's One ID and patented Identity Intelligence technology creates one identity for each user in PPI to easily identify high-risk users and gather insights on consistent issues that could be mitigated.

PRIVACY BY DESIGN

We understand the importance of your patient data and trusting our organization as a business partner. That's why PPI solutions take the proper privacy and security measures to keep your data protected. We only collect necessary data, enforce least privileged access, and implement strict policies for the security of personal data. PPI aligns with frameworks such as ISO 27001 and NIST, and has completed both SOC 2 and ISO 27001 certifications.



OPTIONAL FULLY MANAGED APPLICATION:

Imprivata helps organizations with implementation of Imprivata solutions, informs and guides technical change management and strategic business planning. They act as a supplemental IT resource, providing hands-on support, training, and remote administration. Benefits of Services include increased return on investment, reduced complexity, accelerated time-to-value, reduced cyber risks and threats, boosted efficiency, precision, and end user satisfaction.



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 1 781 674 2700 or visit us online at www.imprivata.com

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.