

# Imprivata Patient Privacy Intelligence (PPI) vs. Oracle Health Sentinel (formerly P2Sentinel)

Imprivata Patient Privacy Intelligence (PPI) is the leading solution in patient privacy monitoring across all areas within compliance: alerting, investigations, reporting, analytics, and user experience. Our AI-powered solution helps you comply with confidence, protect the privacy of patient data, and prevent violations. With intelligent automation and advanced analytics, PPI empowers your organization with greater efficiency, accuracy, and proactive risk reduction.

Imprivata PPI is a complete risk analytics and intelligence solution that has replaced Oracle Health Sentinel (formerly known as P2Sentinel) in over 50 healthcare systems. Imprivata PPI supports hundreds of integrations across EHR, HR, and other identity systems, and can provide you with visibility into more user activity and anomalous behavior. When integrated with Imprivata Enterprise Access Management (EAM), Imprivata PPI enables a single view of user identity and activity across EHRs and applications, providing a level of visibility that other privacy monitoring solutions simply can't achieve.

Functionality	The Imprivata difference	Oracle Health Sentinel
<b>Identity management across application ecosystem</b>	Imprivata PPI works with 500+ applications, including Oracle Health, PACS, OB-GYN, HR, and other enterprise applications. When integrated with Imprivata Enterprise Access Management (EAM) as the identity source, teams are given a global perspective on a user's digital identity that cannot be matched.	Sentinel only works with the Oracle Health EHR system within the organization and does not bring in HR data, a critical piece in understanding workflow and decreasing false positives.
<b>Proactive alerts and auditing</b>	The advanced AI capabilities of Imprivata PPI provide explanations for every access within the EHR, filtering out the appropriate accesses and alerting you only to those that need to be reviewed. Suspicious accesses are ranked based on risk score to prioritize those that present the most risk to your organization.	Sentinel does provide proactive alerting on potential access violations, but they do not rank alerts based on risk scores or provide explanation behind why the access has been marked as suspicious.
<b>Reactive auditing</b>	Imprivata PPI allows you to search on every access within the EHR to perform reactive audits. Searches display accesses ranked by risk and flagged if the system identifies them as suspicious, with explanations provided to help investigators understand why it was flagged and begin the review process.	Sentinel does not allow for reactive searches that report back with ranked, suspicious access for review, requiring users to manually sift through all results during time-sensitive investigations.

Functionality	The Imprivata difference	Oracle Health Sentinel
<b>Reporting</b>	Imprivata PPI has 250+ out-of-the-box reports built based on our extensive experience in the privacy monitoring space. Our solution also allows users to create custom reports based on what is best for their organization.	While Sentinel does have reporting capabilities, the ability to build highly detailed custom reports is lacking. It is also common for customers to incur fees when requesting assistance in Sentinel report setups.
<b>Alert volume threshold</b>	Imprivata PPI enables customers to set a maximum number of alerts to review, ranked by risk for better prioritization. With machine learning scenarios and configurable high, medium, or low policy thresholds, users gain greater control and can significantly reduce false positives.	Sentinel does offer alert volume thresholds, 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.
<b>Full incident management capabilities</b>	Health systems can manage the entire process from alerts to investigations within Imprivata PPI. Select from a library of reports and charts to assist with an audit or internal review and utilize Governance reporting templates that inform on the efficacy of your privacy program to help satisfy HHS OCR guidelines.	Sentinel does not offer a full incident management platform, requiring users to implement another solution for incident management.
<b>Managed Services</b>	Imprivata PPI provides a team of optional compliance and privacy managed services professionals for healthcare systems that may need additional resources to support their efforts.	Sentinel does not provide managed services, causing issues for customers who have resource constraints or would like an experienced collaborator to work with on their auditing program.



Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

**Global headquarters USA**  
Waltham, MA  
**Phone:** +1 877 663 7446  
[www.imprivata.com](http://www.imprivata.com)

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

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

**Australia**  
Melbourne  
**Phone:** +61 3 8844 5533

Copyright © 2025 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.