DATASHEET

imprivata

Protect patients, stay secure

How our organization works to protect our customer's data in Imprivata FairWarning

We understand the importance of our customers' patient data and trusting our organization as a business partner. That's why we've designed Imprivata FairWarning privacy and security measures to keep this data protected. As an enterprise, we have woven in both Privacy and Security by Design and Default into the enterprise; from product design to contracting - and take into account applicable regulatory standards.

What we do on the inside

OUR TEAMS

We take privacy and security very seriously and have two separate leaders for each, including a Global Head of Security and Compliance, and a Head of Privacy and Compliance. In addition to the aforementioned roles and their respective teams, we have interdisciplinary committees that meet regularly to discuss developments, needs, and actions within each space:

- **Cyber Team:** comprised of senior leadership and executive members who are focused on both our organization and the needs of our customers.
- **Privacy Committee:** leaders from Imprivata business units who discuss initiatives, regulations, procurement, technology, product development, etc.
- **AI Committee:** strategic membership across product design, research, and development, security, privacy, compliance, procurement, and other stakeholders tasked with Responsible AI ("RAI") governance based on Imprivata's core Principles.

SECURITY BY DESIGN

Our information security program is based on ISO27001/27701. While other security frameworks were reviewed, ISO standards are **global** IT security management standards; ISO 27001 focuses on the gap between risk management and security controls. **In addition, ISO certification requires third-party auditors and certifying bodies while other frameworks are voluntary.** These certifications demonstrate our continued commitment to information security at every level to show customers that the security of their data has been prioritized and addressed with measured implemented throughout our organization.

Other ways we strive to properly control the security of customer data include:

- To facilitate identification and authorization to its systems, Imprivata FairWarning requires a password policy of 14 character minimum, and complexity requirements are also enabled.
- Multifactor authentication is enabled for all critical Imprivata FairWarning services and all access controls are mapped to NIST SP 800-63B, and forwarding logs are sent to the Security Information and Event Management (SIEM) system.
- Events are both monitored through Imprivata's Security Operations team and a Managed Detect and Respond Service.

PRIVACY BY DESIGN

Privacy by Design and by Default means privacy seamlessly integrates into our governance and compliance programs whether at the enterprise level or for products, services, and system designs. Utilizing our internal Framework, which is informed by the PMF, NIST, ISO, and other regulatory standards, our organization takes a personal data-driven approach to governance. Focusing on ISO 27701, this standard is geared towards meeting privacy regulations and laws like European Union General Data Protection Regulation (GDPR) and the United States Health Insurance Portability and Accountability Act (HIPAA).

We take a proactive approach to privacy, with policies and accompanying procedures designed to address risk. Data stewardship is at the very core of our governance and compliance functions. We consider things like:

- Minimum necessary data collection, processing, and retention
- Customer control over data collection, processing, and retention
- Least privileged access guidelines, so that those who do not need access to data do not have it
- No live data in testing environments
- Single tenant vs. Multitenant environments
- Federated learning for AI algorithms

CERTIFICATIONS

Imprivata FairWarning is designed as governance and compliance enabler, with HIPAA as the North star. With our proactive approach to privacy and security, we have invested in third party certifications and assessments of the enterprise and of Imprivata FairWarning including:

- SOC 2 Type 2
- ISO 27001
- ISO 27701
- HIPAA Risk Assessments

Some organizations certify a small scope of their enterprise that does not extend to the product level - we scoped in all of Imprivata, Inc.

We are also engaging with specialized experts in AI to plan long-term infrastructure, transparency, and other governance and compliance actions related to the Imprivata FairWarning solution. Some key considerations include:

- Direct and indirect identifier usage for training customer AI models
- Data and context controls for data used in AI models
- Location of AI models during training and production processes (e.g. federated approaches to limit movement of customer data and mixing data across customers)
- Expert determination of reidentification risk

SCOPE OF DATA

As previously stated, we understand the importance of customer patient data and trust in our organization. Accessing organizational systems is a risk, and that is why we are only accessing the level of information needed. The Imprivata FairWarning system does not require access to the entire EMR system, rather, Imprivata FairWarning only needs specific data sets within the event log and other systems:

- Patient data
- User data
- User and Patient Demographic data
- User Work Data
- Patient ADT data
- Application Event Data

HOW WE RECEIVE DATA

The Imprivata FairWarning solution either receives data from the necessary systems through data extraction, or from customers providing this log data before going through the event normalization process across data sources. This data is reviewed for data integrity on a consistent basis to proactively detect and mitigate any data integrity issues. Personal data processed by Imprivata FairWarning is based on what the customer determines is necessary for its use of products and services under its applicable agreement. The extent of what and how much personal data is provided is determined and controlled by the organization. The collection and use of personal data may include the customer's employees, healthcare professionals or administrators, contractors, collaborators, clinicians, suppliers, and subcontractors.

SOLUTION VALUE

EHRs and other applications used are a critical part of patient care, but also hold valuable information that puts them at risk of being targeted by internal and external threats. As such, healthcare is a heavily regulated space. Imprivata FairWarning provides critical capabilities required to meet the business and technical demands of healthcare organizations in today's era of modern healthcare applications and the ever-increasing threat landscape.

Not utilizing a Patient Privacy Intelligence tool can leave an organization open to risk that cannot be mitigated. With Imprivata FairWarning, healthcare organizations are better able to protect themselves.

Equipped with artificial intelligence, machine learning, and behavioral analytics capabilities, Imprivata FairWarning allows compliance teams to:

- Proactively detect inappropriate behaviors, unknowns, and true anomalies that are nearly undetectable
- Deliver reliable data analytics to drive efficiency and effectiveness
- Prevent incidents before they happen to mitigate risk
- Strengthen an organization's compliance posture and meet privacy monitoring goals

Our organization takes the protection of this data seriously. At both the enterprise and product level, we structure our security and privacy guidelines to be risk-based so that we may establish and maintain customer trust. We use strict privacy protocols designed to keep data private and implement security features to protect that information. The combination of both efforts allows us to help our customers feel secure about both their staff and patient data while utilizing Imprivata FairWarning to help meet compliance needs and reduce risk.

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

FW-DS-privacy-security-overview-0123