imprivata

DATASHEET

Imprivata Access Compliance AI and Machine Learning FAQ

This FAQ covers multiple questions around how Imprivata Access Compliance (AC) utilizes AI and machine learning.

DOES IMPRIVATA ACCESS COMPLIANCE (AC) UTILIZE AI?

Yes, Imprivata utilizes AI within the application in two ways:

- The Imprivata Patient Privacy Intelligence (formerly Imprivata FairWarning Patient Privacy Intelligence) machine-learning-powered alert closing model begins with a generically trained model and learns from customer-specific workflows and outcomes.
- The Imprivata Patient Privacy Intelligence (PPI) behavioral anomaly detection model is uniquely fit to each customers data and workflows. The model continues to learn from the customer's events and outcomes data, improving accuracy and reducing false positives.

This AI is what is known as traditional AI, taking data to analyze and report on findings, unlike generative AI which creates new data similar to its training data.

WHAT IS IMPRIVATA ACCESS COMPLIANCE DOING WITH AI/MACHINE LEARNING?

Imprivata Access Compliance utilizes AI and machine learning within the PPI solution in three ways:

- First, our machine learning closing model, which automatically reviews and closes alerts while providing confidence scoring and explanations. The software reviews open alerts daily and assigns a confidence-of-investigation score based on multiple factors, which includes type of policy, user and patient interactions, custom fields – appropriate / inappropriate. This confidence score is used by machine learning to then determine if an alert should be labeled as appropriate behavior based on customer risk threshold configurations and closed. Closed alerts remain available for customers to audit. Logs of alerts closed by machine learning and reporting are available to view by the customer at any time.
- Second, workflow for detecting anomalous user patient interactions. For eligible data sources, all user-patient interactions are reviewed, scored, and explained. Interactions with the highest confidence score are provided to the customer daily. The anomalous workflow detection system considers a range of features to identify normal versus anomalous behavior including:
    - The types of actions a user performs on a patient's chart;
    - The care team accessing the chart along with the user;
    - The number of actions performed on a chart; and
    - The location of the patient in relation to the user.

- For each feature, the system compares the user's behavior today when acting on a specific patient, with the user's behavior today for other patients, as well as the user's behavior on previous days. As privacy auditors (and managed service professionals) investigate potential anomalous activity, the weighting of these features is updated to prioritize anomalous behavior that is likely to produce an investigation.
- Third, our Explanation Based Auditing Solution (EBAS), a machine-learning algorithm that provides explanations at the access level, prior to an alert being generated. With this algorithm, data around clinical context is gathered and reviewed to understand how each access fits into treatment, payment, and operational workflows. The EBAS system works with your organization's data and policies finds connections between your organization's patients and employees for clinical context, learning employee collaboration networks to fill in missing connections, and ranking the abnormal behavior within the 1% of suspicious accesses. The EBAS system is then combined with the machine learning closing model to take the ranked 1% of accesses and analyze possible violations with risk scores and access explanations.

All models are customer-specific and trained on customer data for at least 30 days and will extend as far back as possible. If model quality is poor after bespoke training (the model does not meet threshold during cross validation), a generic model is used. Models continue to learn based on the outcomes provided in alert feedback.

HOW FREQUENTLY DO YOU UPDATE ALGORITHMS AND/OR RELEASE NEW ALGORITHMS?

- Imprivata consistently delivers new product features and enhancements in point releases, PPI is updated monthly. The machine learning closing model and anomalous workflow model leverage updated data (alert outcomes) and retrain regularly.

IS MY DATA MIXED WITH OTHER CUSTOMERS' DATA?

- No, our model is trained on the customer's data only and is not mixed with other customers data.
- Single tenant customer environments are deployed and on our dedicated SaaS solution.
- Customer environments are segregated from corporate environments and data.

WHAT DATA IS THE AI MODEL TRAINED ON?

- The PPI machine-learning-powered alert closing model begins with a generically trained model and learns from customer-specific workflows and outcomes.
- The PPI behavioral anomaly detection model is uniquely fit to each customer's data and workflows. The model continues to learn from the customer's events and outcomes data, improving accuracy and reducing false positives.

HOW DO YOU ACCESS OUR ENVIRONMENT?

Access to customer environments occurs via IP Whitelisting or site-to-site VPN between customer network and the SaaS platform.

IS MY DATA SENT OR SHARED WITH THIRD PARTIES?

No, our AI models are built in-house and derived from known algorithms and packages and hosted in the customer tenant.

HOW DOES IMPRIVATA RECEIVE MY DATA?

The Imprivata solution either receives data from the necessary systems through data extraction, or directly from customers' log data before going through the event normalization process across data sources. This data is consistently reviewed for integrity to detect and mitigate any issues. Personal data processed by the Imprivata solution 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, collaborators, clinicians, suppliers, and subcontractors.

WHAT PRIVACY AND SECURITY CERTIFICATIONS DO YOU HAVE?

With our proactive approach to privacy and security, we have invested in third party certifications and assessments of the enterprise and of Imprivata Access Compliance, including:

- SOC 2 Type 2
- ISO 27001
- ISO 27701

DOES IMPRIVATA LEVERAGE ANY THIRD-PARTY AI TOOLS?

Imprivata does utilize third-party AI tooling, such as GitHub Copilot, in areas where it has been reviewed and approved by our AI Governance Committee. Customer data is not pushed into a third-party AI model.

All AI models are built in-house, and we do not use any third-party AI models.

DOES IMPRIVATA EMPLOY AN AI RISK MANAGEMENT FRAMEWORK?

Yes. Imprivata has deployed an AI risk management strategy that includes, but is not limited to:

- The Software Development Lifecycle
- Third Party Risk Assessments

All AI uses at Imprivata must be vetted through these frameworks and signed off by the Imprivata AI Risk Management Committee.

HOW DOES IMPRIVATA VALIDATE AND TEST ITS AI MODELS TO AVOID HARMFUL BIASES AND INACCURACIES?

Imprivata utilizes multiple methods to help avoid harmful biases and inaccuracies with its AI models:

1. Imprivata only brings in the necessary data to provide results.
2. Imprivata keeps humans in the loop, as it allows customers to see the right information to investigate and act on if needed.
3. Imprivata utilizes model explainability techniques, allowing users to comprehend results with text-based explanations from the models that contribute to each prediction.

4. Imprivata tunes predication thresholds according to specific circumstances to ensure something does not go unnoticed. For example, Imprivata sets lower thresholds for problems where the cost of a false negative (which can cause something to be overlooked) is high.

HOW IS THE AI MODEL CUSTOMIZED FOR INDIVIDUAL CUSTOMERS?

Imprivata Patient Privacy Intelligence machine-learning-powered alert closing model begins with a generically trained model and learns from customer specific workflows and outcomes. Our behavioral anomaly detection model is uniquely fit to each customer's data and workflows. The model continues to learn from the customer's events and outcomes data, improving accuracy and reducing false positives, thereby customizing to their organization's workflows.

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 **imprivata.com**