DATASHEET

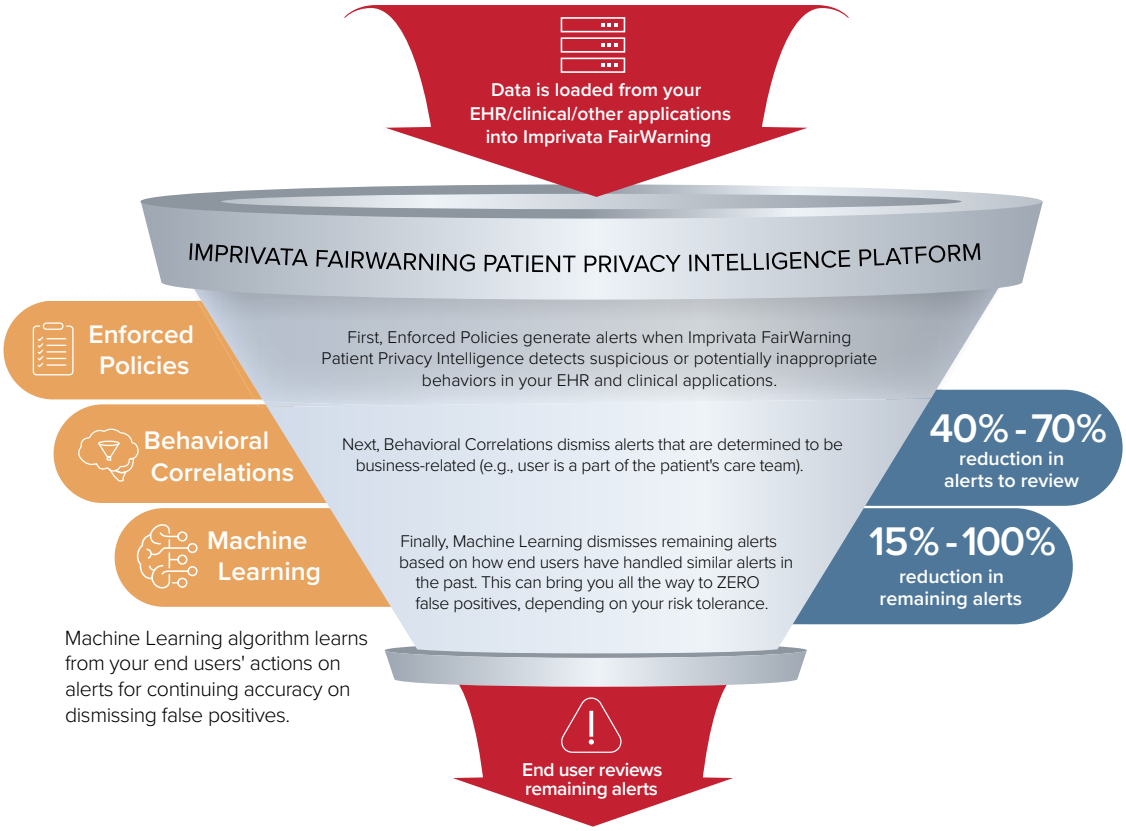
Save Time by Eliminating False Positives

Dealing with false positives can consume precious resources – but are they a necessary evil if you want to catch all possible privacy incidents?

Not necessarily. Imprivata FairWarning Patient Privacy Intelligence customers have found that layering Behavioral Correlations with patented, machine learning-based technology can help them eliminate false positives entirely, giving you time back in your day to focus on additional aspects of your privacy and compliance program – and reducing your overall risk.

BY USING BEHAVIORAL CORRELATIONS IN COMBINATION WITH MACHINE LEARNING:

- Get time back in your day to focus on additional areas of your privacy program.
- Expand your privacy program to monitor for more enforced policies, thanks to the decreased workload from fewer false positives.
- Gain peace of mind knowing the alerts generated are true privacy risks/incidents.
- Maintain your existing end-user workflow (all technology is included in Imprivata FairWarning Patient Privacy Intelligence).



HOW DO BEHAVIORAL CORRELATIONS WORK?

Imprivata FairWarning Patient Privacy Intelligence's Behavioral Correlations will automatically document and dismiss an alert when it determines a user has a business reason for accessing a patient record. The filtering algorithms conduct an analysis to determine these clinical scenarios within the event and user data:

- Has the user modified the patient?
- Has the user modified the patient record in the last month?
- Is the user part of the care team?

Due to the inconsistent use of care team members within the source application, Imprivata FairWarning Patient Privacy Intelligence has found more accurate results by defining “care team” as “two other users from the same department have modified or edited the patient record in the last month.”

HOW DOES MACHINE LEARNING WORK?

Imprivata FairWarning Patient Privacy Intelligence's Machine Learning technology learns how to respond to alerts in your application by prioritizing and scoring each future alert based on how your end users have previously reviewed and closed alerts manually. You can leverage this technology to automatically document and close alerts that meet a certain score or risk tolerance. We start by teaching the technology to score future alerts based on the following data:

- Name of the Enforced Policy
- Patient flagged in the alert
- Event types
- Access types
- User flagged in the alert
- Status of similar alerts
- Event names
- Other attributes

WHAT’S REQUIRED TO BEGIN ELIMINATING FALSE POSITIVES IN IMPRIVATA FAIRWARNING PATIENT PRIVACY INTELLIGENCE?

Imprivata FairWarning Patient Privacy Intelligence eliminates false positives by layering Enforced Policies, Behavioral Correlations, and Machine Learning technologies.

Imprivata FairWarning Patient Privacy Intelligence will apply our latest Behavioral Correlation algorithms, which include clinical context and identification (e.g., existing members of the patient’s care team) to automatically close and document alerts that were business-related. To enable Behavioral Correlations, you must have:

- 10 or more alerts per day
- Epic, Cerner, or Meditech
- Proactive Monitoring (Enforced Policies) enabled or planned for coworker, household, or manager snooping

Machine Learning will automatically document and dismiss alerts based on actions taken by your end users on similar alerts in the past. To enable Machine Learning, you must:

- Have proactive monitoring enabled (Enforced Policies)
- Have three months of alert history to draw upon
- Implement Imprivata FairWarning Behavioral Correlations for at least three months
- Determine your risk tolerance
- Be willing to accept some level of false negatives
- Follow the best practice workflow

HOW DO I GET STARTED?

Imprivata FairWarning Patient Privacy Intelligence Behavioral Correlations and Machine Learning technology has been implemented with over 150 in-production customers. While the results vary based on workflow, applications, and risk tolerance, customers are seeing false positives reduced by 40 to 90 percent. This has allowed them to expand their monitoring programs, save time through efficiencies, and spend more time with staff and patients.

1. Contact your Customer Success Manager or create a support case in the online Community.
2. Review the Enforced Policies on which you would like to reduce the volume of alerts. This review will be performed during a call with our team. Imprivata FairWarning will provide initial recommendations based on best practices.
3. Imprivata FairWarning will implement Behavioral Correlations on the active Enforced Policies. We will review the alert volume change with you and share the resulting Governance Report to track for future use.
4. For those eligible, Imprivata FairWarning will implement Machine Learning technology and begin training the system. This technology learns the difference between appropriate and inappropriate access based on alerts manually reviewed by your end users. FairWarning predicts which alerts should be documented and dismissed as “appropriate access” and review the results with the customer. When an alert is closed, it’s not gone forever, but rather archived in case a record of the alert is ever needed. This will move to production if the customer is satisfied with the results. Imprivata FairWarning will review the learned behaviors every six months, for accuracy.

For more information, please contact us at 1 781 674 2700 or visit us online at www.imprivata.com

FW-DS-save-time-by-eliminating-false-positives-0321