imprivata

DATASHEET

Imprivata Access Compliance solutions: FairWarning Artificial Intelligence Risk Scores

The FairWarning Artificial Intelligence Risk Score (FAIR Score), a built-in function of all Imprivata Access Compliance solutions, is a machine learning-generated confidence score for determining whether the outcome of the alert may result in an investigation. FAIR Scores are available for detail-based enforced policies that generate greater than 30 alerts over a 30-day period. A higher FAIR Score indicates that the system is more confident that the alert will become an investigation.

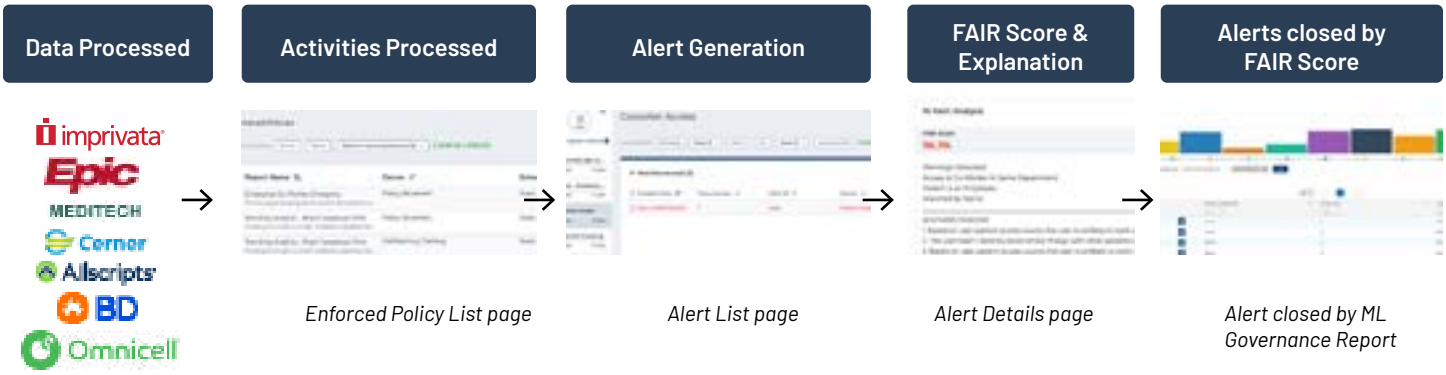
To calculate the FAIR Score, we look at the following to identify which alerts will become investigations and incidents, then we set the closing model threshold to a FAIR Score that produced zero investigations or violations based on historical data.

- Event count analysis for historical alerts and typical user workflow:
  - Event types (print, edit, update, delete)
  - Area of the application (e.g. flowsheets, problems list, reporting) Encounter type
  - Patient departments
- Admission/discharge periods in relation to alert events
- Analysis of similarity between field values for pairs of the following:
  - Patient department, User department, User facility
  - Event type
  - Encounter type (e.g. office visit, inpatient encounter, procedure visit) Application (e.g. flowsheets, problems list, reporting)
  - Report name (e.g. inpatient flowsheet, care plan, etc.)
  - Event name (what was printed, updated, etc.) and the area of the application
  - Encounter service areas

We continuously retrain the machine learning closing model on 30 days of alerts, investigations, and incidents.

Using historical data to continuously retrain models is an incredibly valuable method to ensure models learn from new outcomes, however there are possibilities that a future alert with a low FAIR Score can turn into an investigation. To validate alerts with a lower FAIR Score are accurately scored, we will randomly select 5% of alerts below the closing model threshold and surface these in the Alert List. The outcomes of these alerts are also taken into consideration for adjusting the FAIR Score threshold.

What is the Machine Learning Closing Model process to generate FAIR Scores and close alerts?



What does the FAIR Score look like in the application?

AI ALERT ANALYSIS

FAIR SCORE
68.432%

FAIR Score contributing factors:

Admit Date (FAIR Score weight 59%)

Events for this Event Type are not usually performed with this Application (FAIR Score weight: 21%)

Events for this Event Type are not usually performed with this Encounter Type (FAIR Score weight: 21%

WHAT ARE THE FAIR SCORE WEIGHTS IN THE FAIR SCORE CONTRIBUTING FACTORS?

FAIR Score weights are calculated based on the contributing factors' impact on the FAIR Score. We will show the top contributing factors for each FAIR Score. The higher the FAIR Score weight, the more influence that factor had on the FAIR Score.

AM I ABLE TO CUSTOMIZE MY RISK TOLERANCE TO CLOSE MORE FALSE POSITIVES?

Yes, there are a few options to customize risk tolerance and close more false positives in a way that best suits your organization:

- Machine Learning Scenarios: With Machine Learning Scenarios, the system takes all historical alerts, investigations, or certain alerts that have a custom field associated with them that indicates there was an investigation and creates three (3) different models. Users can select them through one of three scenarios:
    - Low: This scenario will close the fewest alerts and is the most conservative approach.
    - Medium: Closes alerts with a threshold that may contain some previous true positives that had a lower FAIR score, and only shows alerts with a Medium FAIR score or higher.

- High: Closes the most alerts; the least conservative. Do note, a "High" threshold setting closes more alerts and may increase the chance of a potential violation going undetected. Users are advised to select this setting on a limited basis.

AM I ABLE TO CUSTOMIZE MY RISK TOLERANCE TO CLOSE MORE FALSE POSITIVES?

As the threshold increases, so does the number of alerts that will close if they meet the scenario. Machine Learning Scenarios only apply for detailed policies that create alerts by user and patient and have at least 30 alerts within the past six (6) months. If a policy is eligible for applying a Machine Learning Scenario, the level selection drop-down will be available to use.

Closed alerts remain available for auditing what alerts are reviewed and closed by Machine Learning, and reporting is available to review which alerts are closed by Machine Learning.

- **Alert Limits:** This functionality allows users to select a maximum number of alerts to be shown for a specific policy, helping to focus on the highest risk accesses to review.
- **Machine Learning Scenarios combined with Alert Limits**: By combining Machine Learning Scenarios with Alert Limits, the system will only alert users to what needs to be reviewed, up to the set alert limit. For example, if an enforced policy has an alert limit of 10, but the system only finds six accesses to be reviewed, it will only alert users on those six accesses. With this combination, the system can review all accesses and clear alerts that meet the enforced policy.

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

DS-FW-Machine-Learning-Closing_Model_0524