



# Best Practice Webinar: Understanding Anomaly Detection Workflows

June 18, 2024

Presenters:

Jennifer Vaquero - Sr. Manager, Managed Privacy Services

Adam Droz - Sr. Customer Success Advisor, Customer Success



# HOUSEKEEPING!

## Email verification coming in 24.8!

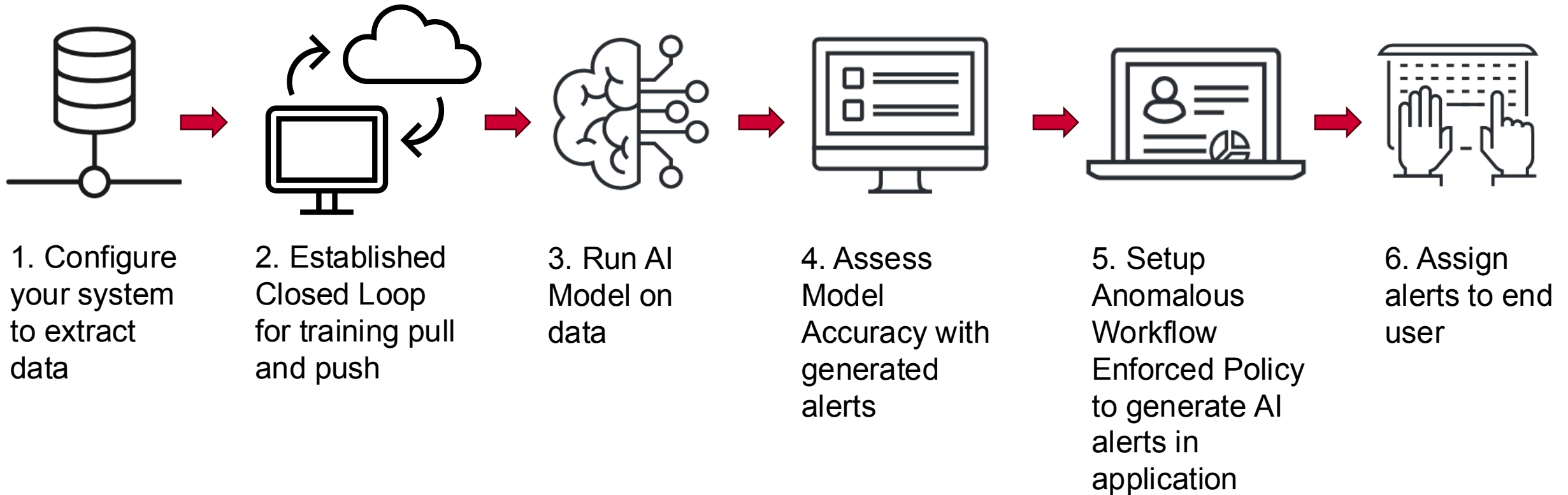
- Customers will need to verify their email domains with their account team
  - Success and support can assist with whitelisting your organization domain
- System Admins work with your end users and account team to ensure each user who has access to your application by having end users...
  - Click on their profile in the top right
  - Click “My Profile”
  - Click the “send verification code” (should take a minute or so)
  - You will receive an EMAIL from [noreply@imprivata.com](mailto:noreply@imprivata.com) with a 5-digit code
  - The user will then need to enter their code into their “My Profile” page
  - Click “Save”
  - Now you’re verified!

Thank you for helping us be a more secure partner!

# AGENDA

- How does the Anomaly Detection work?
- Implementing Anomaly Detection and workflows
- Understanding Risk Scoring
- Stepwise Alert Workflow
- Key Takeaways and Tips
- Q&A

# AI Configuration & Setup: How does it work?



# Implementation: Alerting & Goals

- HR/AU Data not required for AI Alerting but recommended, all users will be monitored
- Implement the policy with 5 to 10 alerts daily
- Alerts are produced based on FAIR Score
  - Alerts with the highest FAIR score will be generated for review
  - Occasionally, an “unscored” alert may come through for review (new activity/user)
- Alert VOLUME can be adjusted based on customer feedback
- Alert QUALITY improves dramatically after 30-90 days
  - Please provide feedback early in the process to your account team!
- AI Alerts typically take more time to analyze and investigate

## ***AI Benchmarking Goal:***

***By 90 day mark, >10% of Alerts produced become Investigations***

***Ex: 35 alerts per week would result in up to 3 alerts becoming investigations***



# Understanding the FAIR score

- The FairWarning Artificial Intelligence Risk Score (FAIR Score)
- Higher FAIR Score indicates that the system is more confident that the alert will become an investigation (80% **RISKY** vs. 10% **Low risk**)
- User scoring “features” compare differences in access for:
  - 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 area
  - 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

## AI Alert Analysis

FAIR Score

**80.037%**

FAIR Score contributing factors:

Events for this Patient Department are not usually performed with this User Department (FAIR Score weight: 45%)

Events on this alert are not usually performed by this user (FAIR Score weight: 29%)

Events on this alert are not usually performed by this user (FAIR Score weight: 24%)

[View Less](#)

# Anomalous Workflow: Alert Review – AI Analysis

Step 1: Review the AI Alert Analysis at the center of the Alert

## AI Alert Analysis

FAIR Score

65.266%

This alert's confidence is 65.26%. This alert is based on 1.0 days of data.

1. The user hasn't recently done similar things with other patients (46% weight).
2. The user hasn't recently worked with other employees who care for this patient (34% weight).
3. The user didn't do similar things with other patients today (18% weight).


[View More](#)

- The machine is telling us that the user does not work in this way with similar patients
- The user has not worked with other employees who are also working on this patient
- On the day in question, this user only acted this way with this patient


# Anomalous Workflow: Alert Review – User/Patient Cards

Step 2: Review the User and Patient cards to pair with the AI insights

**Kassidy Grimes**  
User

Alerts  Investigations

6 0




User ID:	E0000282
User Department:	Pediatrics
User Title:	Patient Service Specialist
User Facility:	Fusion Medical
User Birth Date:	1986-05-05
User Address Line 1:	134 N St, Clearwater, FL 13357
User City:	Clearwater
User State:	Florida
User Postal Code:	13357

[View Less](#)

**John Smithson**  
Patient

Alerts Investigations

3 0



Patient ID:	0000101238
Patient Department:	Surgery
Patient Birth Date:	5/28/1977 12:00:00 AM
Patient Address Line 1:	2240 Janes Ln
Patient City:	Steger
Patient State:	Georgia
Patient Postal Code:	76638

[View Less](#)

- AI Insight #1: “**Pediatrics** user does not work this way with similar **Surgery** patients”
- AI Insight #2: This Pediatrics user does not have peers working on this Surgery patient
- AI Insight #3: On the day in question, this user only acted this way with this patient
- User already has 6 open alerts, they could be a high risk user



# Anomalous Workflow: Alert Review – Alert Details

Step 3: Review the access details provided by the Anomalous Workflow Alert

Alert Events [For Manual Run - How many patients did this user access?](#) + Add Report

1-6 of 6 Display: 250 Columns: 16 Columns Selected Q Attach Events to Investigation CLEAR ALL FILTERS

User Department	User Title	Event Name	Event Type	Patient Department	Patient Birth Date
Pediatrics	Medical Assistant	Chart Review Encounters tab selected	View	Surgery	May 28, 1977
Pediatrics	Medical Assistant	History activity accessed	View	Surgery	May 28, 1977
Pediatrics	Medical Assistant	Encounter viewed in Chart Review	View	Surgery	May 28, 1977
Pediatrics	Medical Assistant	Encounter viewed in Chart Review	View	Surgery	May 28, 1977
Pediatrics	Medical Assistant	Visit diagnoses viewed	View	Surgery	May 28, 1977
Pediatrics	Medical Assistant	Visit diagnoses viewed	View	Surgery	May 28, 1977

- Pediatrics Med Assistant is accessing an Adult Surgery Patient
- Actions are view only and on sensitive areas of the patient's chart

# Anomalous Workflow: Alert Review – Deep Dive

Step 4: Compile additional information or use AIR reports for deeper analysis

[What activities did this user do on this patient?](#) ×

[What departments accessed this Patient?](#) ×

[What actions are normally performed by User?](#) ×

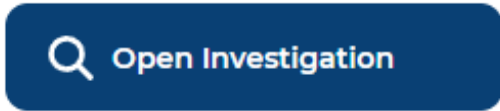
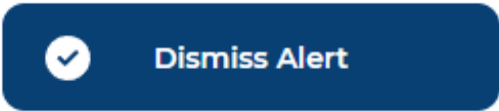

[How many patients did this user access?](#) ×

- Every alert can be configured with AIR reports, think of these as an analysis checklist:
  - What activities did this user do on this patient? (shows access back 30-90 days for comparison)
  - What departments accessed this patient? (shows departmental access for different users back 1-2 weeks)
  - What actions are normally performed by this user? (shows the user's history for the past 1-2 weeks)
  - How many patients did this user access? (shows the other unique patients the user accessed summarized by day)
  - **It is highly recommended to run a full report on the User's Access for that day / week / month if you cannot decide from the standard AIR reports alone**

These reports are completely configurable if one does not suit your workflow or another “commonly asked question” comes to mind as you analyze these alerts, they can be built with the report builder or by contacting your analyst, your success team, or [success@imprivata.com](mailto:success@imprivata.com)

# Anomalous Workflow: Alert Review – Alert Determination

Step 5: Select if the Alert should be DISMISSED or INVESTIGATED

Open an Investigation if you agree with the risk

Alert Review

You've chosen to open an investigation. Complete the fields below.

Open Investigation

Attach this alert to an existing investigation or create a new one below.

- Attach to an existing investigation  
Select One  
Choose an investigation from the list.
- Attach to a new investigation  
Coworker Access  
Name your Investigation.
- Do not attach to Investigation but update the Alert status

Add a note:

Enter your notes here...

Dismiss the Alert if you think the access is appropriate

Alert Review

You've chosen to dismiss this alert. Complete the fields below.

Dismiss Alert

**User-determined outcomes are important for feedback!**

**You do NOT need to fully investigate for the feedback!**

# Anomalous Workflow: Alert Review – Investigation Process

Step 6: Aggregate the Alert, Additional Reports, and Notes into Investigations and send QAM

## Questionable Access Memorandum

To: Manager Name (Manager's Email)  
Cc: Contact 1  
Cc: Contact 2

June 5, 2024

Subj: Questionable Access Memorandum – Anomalous Workflow

Manager Name,

On Friday, July 13, 2018, User Name (User ID) accessed the electronic health records of **Patient Name** (MRN XXX), in **Epic** in environment (**environment**). A review of audit logs failed to identify a work related reason for the access. User Name accessed (list Events accessed in Epic). User Name does not appear to follow a normal workflow for accessing this patient, or appear to be part of the patient's recent care team. User Name is the only user from (User Department) to access this patient in the past month. User Name does not access (list Events) for any other patients on the date in question. Additionally, User Name (provide any additional reasoning for suspicion).

You are identified as User Name's Supervisor. I need your assistance to determine if there was a work related reason for the access. Please reply to all within **3 business days** and indicate if there is a work related reason for the access or not.

No – There is no business reason for the access

Yes – There is a legitimate business reason for the access. **(Please explain reason)**



## Key Takeaways & Analysis Tips

- Anomalous Workflow will require more effort to analyze! There is also a higher chance that the access is appropriate as the user may not be breaking a defined “rule”.
- Lean on the side of caution, if you THINK it may be an investigation – open the alert into one.
- Define your internal processes on investigating potentially suspicious AI, use the QAM template and be collaborative with manager and leadership team members on workflows.
- Use the AI Insights to guide a deeper analysis of the alert details
- If your AIR reports do not have your organizations “analysis checklist” ask us to customize
- Always choose a “yes” or “no” outcome on the alert! User-feedback is very important!
- If you do not understand (or agree) with an alert, please notify us by emailing support or success.
- Alert quality will improve in time as the system learns and receives end-user feedback.

# Questions?

Contact us!

Email your account team, [success@imprivata.com](mailto:success@imprivata.com), or [support@imprivata.com](mailto:support@imprivata.com) if you have more questions or concerns.

E-mail Verification coming in August, are you prepared?



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:

**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 © 2024 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.

