TRACE3

Artificial Intelligence Solution Design

Case Study: Protecting Patient Data with Machine Learning

This report is targeted for executives, privacy professionals, and analytics leaders looking for better ways to protect patient data and other sensitive information.

This case study combines technical and non-technical perspectives to provide an overview of the client’s challenges, project approach, solution design, and business value.

Disclaimer

This document has been prepared solely for Trace3's internal research purposes without any commitment or responsibility on our part. Trace3 accepts no liability for any direct or consequential loss arising from the transmission of this information to third parties. This report is current at the date of writing only and Trace3 will not be responsible for informing of any future changes in circumstances which may affect the accuracy of the information contained in this report. Trace3 does not offer or hold itself out as offering any advice relating to investment, future performance, or market acceptance.

01 Problem Overview

In recent years, high-profile data breaches and privacy violations in the healthcare industry have garnered significant attention.

Protecting patient data from unauthorized access is crucial for maintaining patient privacy; preventing identity theft, fraud, and legal issues; and safeguarding patients' rights against unfair treatment based on health, insurance, or financial status.

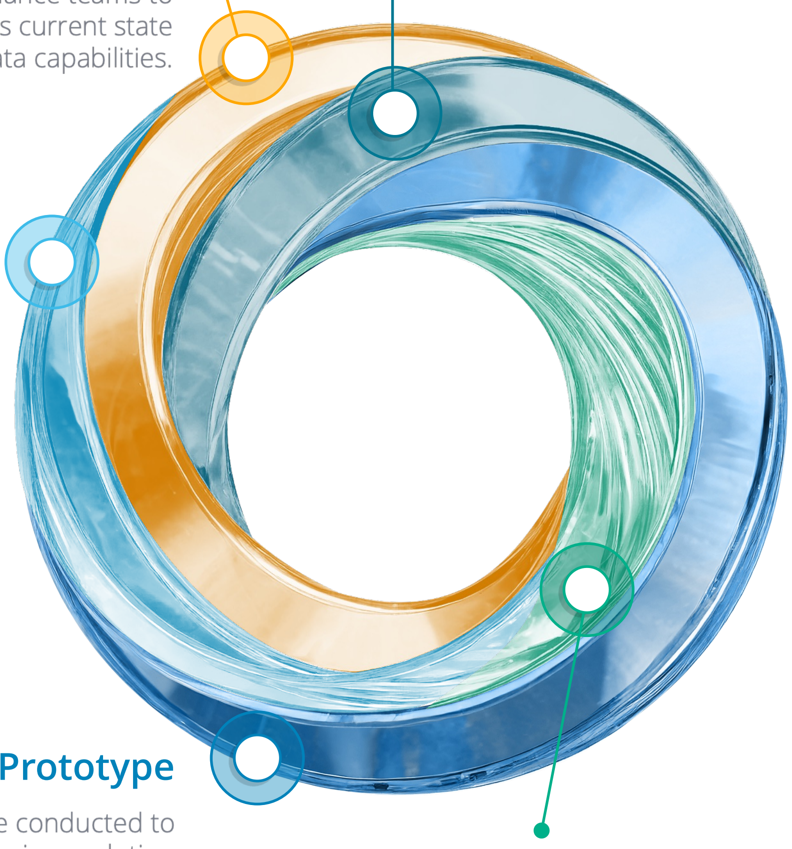
Failure to adequately protect patient data can quickly erode patient/provider trust and damage the brand of an organization.

Several prominent healthcare organizations have faced media scrutiny over the past few years, due to patient records being exposed and shared without permission through unauthorized access. Frequently, these incidents are attributed to errors by employees, negligence, snooping on medical records, data theft by malicious insiders and other reasons. To combat this problem, **more rigorous prevention and detection controls** for technology, processes, people, and policies are needed.

At the same time, frequent false alarms and intrusive investigations can disrupt patient care, increase costs, and damage employee morale. Considering the need for healthcare organizations to serve more patients with fewer resources, the **need for more effective, more accurate detection** strategies has never been more important.

02 Our Approach

The project approach focused on establishing a thorough understanding of the client's problem, business requirements, data and technical capabilities, AI/ML maturity, and culture. To build momentum and establish an environment for successful adoption, Trace3 organized the project in five distinct phases: **Listen**, **Educate**, **Prototype**, **Plan**, and **Buy-in**.



Buy-in

Focus group sessions and educational briefings were conducted to ensure that all stakeholders aligned with the recommended direction.

Listen

Workshops were conducted with end users, product owners, stakeholders, physicians, and compliance teams to understand the client's current state and data capabilities.

Educate

Training sessions were held to educate the team on machine learning fundamentals, industry-leading practices, and the challenges of deploying machine learning solutions.

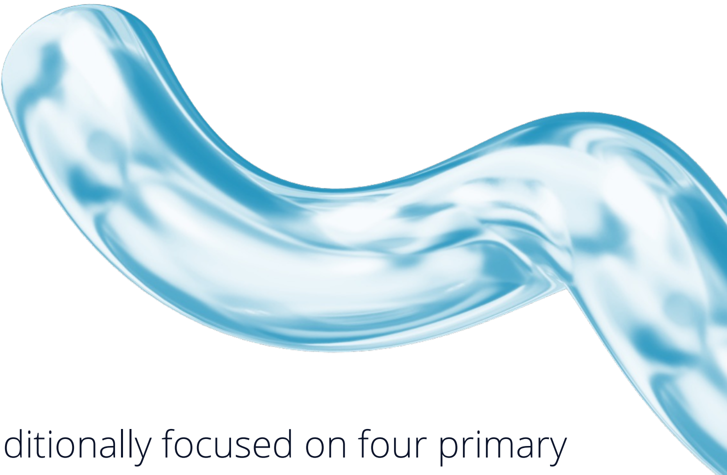
Prototype

Ideation activities were conducted to identify and evaluate various solution options. Mockups were developed to help the client understand the role of machine learning in solving the problem at hand.

Plan

A comprehensive deployment plan and timeline was created, with investment requirements and a business case that the client used to quickly obtain management support.

Trace3 applied design thinking and AI solution design techniques throughout this project: defined the problem, identified impacted personas, and analyzed the client's workflow to determine the best solution for their organization. This approach provided the client with a **better understanding of their current capabilities and the steps needed to implement a sustainable machine learning-based solution**, fostering a culture of accountability, transparency, and data stewardship.

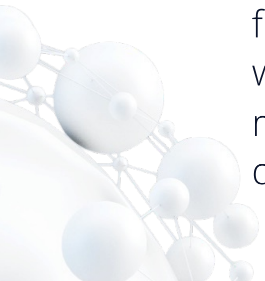


03 Current State

Client monitoring efforts traditionally focused on four primary data vectors: **Same Department**, **Direct Reports**, **Same Household**, and **Same Address**. These vectors each contain subtle characteristics that made it very **difficult to detect inappropriate access situations**.

During the COVID pandemic, for example, registration staff assigned to one specialty department had to supply staffing coverage for another specialty department. As a result, what might appear to be inappropriate access by a staff member would be explainable due to a temporary assignment.

Prior to this project, the client used a monitoring system that combined log data from the electronic medical record with position data from their HR system. This combined dataset was then evaluated against pre-defined criteria using a decision-tree model that considered a limited number of features. Each access event received a score that was filtered for significance. Once the data was combined, the events were then categorized into the four use case groups mentioned above. Identified events were then loaded into queues where they were reviewed by the client's staff.



many **false positives**

incomplete chart coverage

location **impacts** requirements

limited range of use cases

long processing times

early system limitations

Several significant issues exist with this approach that caused the solution to produce sub-optimal effectiveness.

- First, it **lacked precision** and resulted in an inordinately high number of false positives (e.g., more than 90%) and an unknown number of undetected true positives.
- Second, since the monitoring system solely focused on situations where an employee was involved, **unauthorized access** by a family member or person living at the same address **might not be captured.**
- Third, the processing logic was **difficult to tailor to unique circumstances** (e.g., differences in policies) across geographic locations.
- Finally, long processing times often would result in **unnecessary delays** to an investigation.

04 Solution Components

Trace3 utilized a methodology rooted in **listening, educating, and prototyping**. Consultants and data scientists jointly engaged stakeholders across various levels to understand their needs and data capabilities. By conducting workshops and training sessions, Trace3 provided the client with a **foundational knowledge of machine learning fundamentals and industry practices** which facilitated ideation, prototype development, and decision making.

Once the problem was accurately framed and requirements identified, Trace3 and the client explored various deployment options.

The solution needed to **meet the client's requirements** for improving accuracy, flexibility, clarity, performance, and preserving required functionality.

After a thorough analysis, the client selected a solution that complemented existing capabilities with an ensemble method approach that leveraged multiple models instead of using one single model.

This approach offered several advantages:

- it leveraged the client's previous investments,
- was fast to launch, and
- reduced the change impact on the client's staff.

Furthermore, the ensemble method solution aimed at improving the accuracy of models by reducing variances. By harnessing the power of machine learning and refining the monitoring infrastructure, the **solution components enhanced the effectiveness and efficiency** of the client's monitoring efforts.

behavioral anomaly model

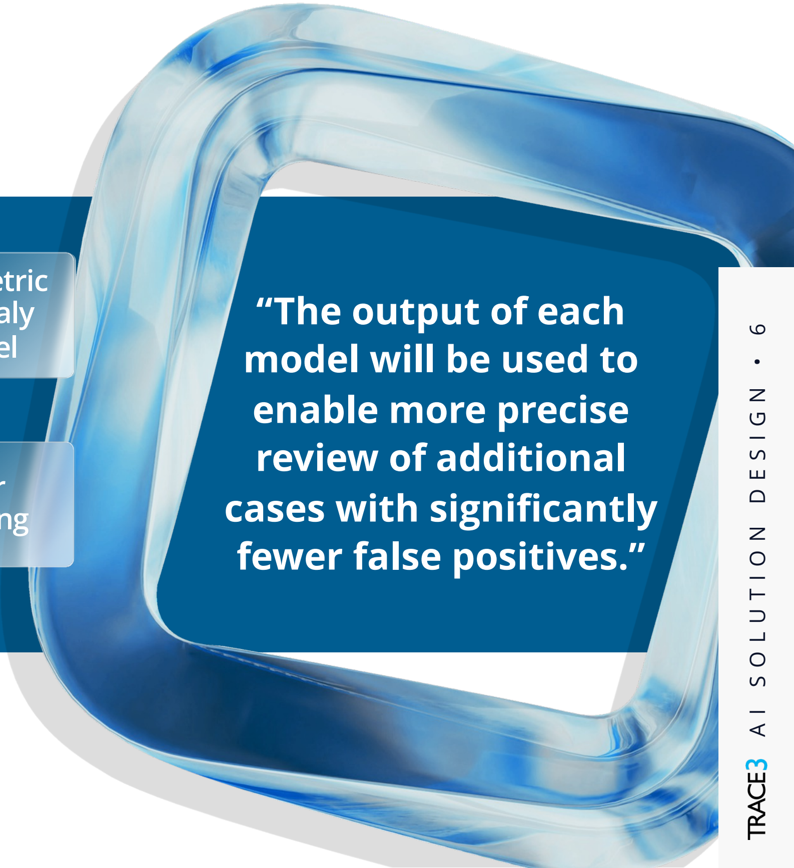
false positive models

volumetric anomaly model

ML platform

enhanced user interface

user training



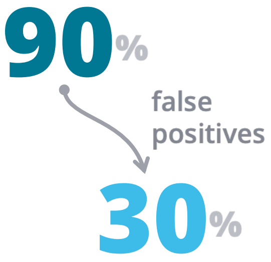
"The output of each model will be used to enable more precise review of additional cases with significantly fewer false positives."

Ultimately, the approved solution contained six key components (illustrated above). Three **machine algorithms** were used to **minimize false positives** by evaluating more features, **detecting volumetric anomalies** when the number of chart access events would exceed expectations for a normal user, and **detecting behavioral anomalies** for activities that would not be normally expected in a person's role. The improved user interface conveyed previously unknown insights generated by the models. These capabilities were supported by targeted **end user training**, **enhanced user interface**, and additional storage and compute resources.

By combining the strengths of current features with the transformative potential of new machine learning capabilities, the enhanced solution is transforming the client's approach to mitigating inappropriate access to medical records, fostering a culture of security, compliance, and trust within their healthcare organization.

05 Business Impact

In terms of efficiency, the use of advanced machine learning capabilities is projected to significantly **reduce the number of false positives** from approximately 90% to approximately 30%. Once the solution is deployed, the models will be refined to reduce false positives even further.



This reduction will streamline the investigative process, freeing up resources, and leading to increased investigator productivity. Moreover, more accurate event detection will help **reduce the risk of HIPAA violations** and potentially **minimize costs** related to penalties, legal proceedings, remediation, and insurance.

By **enhancing effectiveness**, the ensemble method solution extends the scope of access oversight, enabling a more comprehensive monitoring of chart access and accommodating new use cases. Broadened oversight ensures a proactive approach to security, identifies anomalous access patterns across diverse scenarios and strengthens overall defense against potential breaches. Leveraging historical incident data, the new system facilitates a faster response to security incidents, speeds up the resolution of access anomalies, and ensures a more resilient and responsive security posture.

Finally, the solution **promotes scalability**, allowing the system to handle rapidly increasing data volumes, essential for maintaining **optimal performance and effectiveness** in the face of evolving business needs and expanding datasets.

In Conclusion,

this project represents an important demonstration of Trace3's commitment and contributions to the client's efforts to safeguard access to sensitive data. Through collaborative engagement with stakeholders and end users, Trace3 consultants meticulously identified pain points and opportunities to improve the customer experience.

Consequently, Trace3 proposed an innovative machine learning solution marked by enhanced efficiency and security, underpinned by a comprehensive deployment plan and stakeholder buy-in. The ensemble method provides the client a buildable foundation that extends beyond current use cases to proactively address future scenarios.

Organizations looking for more effective ways to protect sensitive patient data should consider the many advantages a machine learning approach provides when compared to legacy monitoring solutions.

At the same time, it is important to consider both data and the human factors to promote adoption and address concerns about privacy, bias, and ethics.

Trace3's AI solution design methodology uses leading practices from design thinking, data sciences, security, and AI governance to deliver AI products that meet and organization's current and future needs.

For more information on how machine learning can improve your organization's ability to monitor access of sensitive data or Trace3's AI Solution Design capabilities, please contact the **Trace3 Center of AI** at centerofai@trace3.com

Trace3 would like to extend a special thanks to Mike Brooks, Jaisen Patel, Erin O'Neill and Andy Bernard for their contributions to this publication