CASE STUDY

Memorial Healthcare System's privacy and security comeback: from reported breach to patient privacy excellence

imprivata®

ORGANIZATION SNAPSHOT

Memorial Healthcare System

LOCATION
Florida

EMPLOYEES
13,000

INDUSTRY
Healthcare

CHALLENGE

MHS was dealing with more than 10 patient record access alerts per week, creating too much data to investigate properly. Further challenges included ensuring Epic Care Connect access compliance for affiliated healthcare providers and ACO affiliate patient privacy adherence.

SOLUTION

- Imprivata FairWarning Patient Privacy Intelligence
- Managed Privacy Services

RESULTS

- 90% reduction in specific security alerts
- Equivalent time savings equal to two FTEs
- Manage the full life cycle of a security incident
- Stellar privacy compliance audits

Memorial Healthcare System

Richard Leon
Chief Information Security Officer
at Memorial Healthcare System

Memorial Healthcare System (MHS) is one of the largest public health systems in the country with 13,000 employees, 2,500 physicians, countless other non-employee physicians across six hospitals, and numerous ancillary healthcare facilities and physician practices. The award-winning healthcare system serves a patient population of millions of people across southern Florida.

Memorial Healthcare System's growth and success in patient care and outcomes had left them with a robust volume of data and therefore increased costs and effort to properly investigate access to PHI. The Imprivata FairWarning Patient Privacy Intelligence Platform and Managed Privacy Services team reduced specific security alerts from ten a week to just one a week through access visibility and patient privacy policy design. This saved the time equivalent of two full time employees (FTEs) for alert investigations, while enterprise-wide training built a culture of true patient privacy excellence.

Overview

Achieving patient privacy excellence is an ongoing journey in healthcare settings that must begin with that proverbial first step. For Memorial Healthcare System (MHS), benchmark-setting patient outcome improvements had gone hand in hand with steady growth. But growing pains and enterprise-wide policies were producing too much data for MHS to properly review access to PHI. Just one year later, they had come a long way in their journey to achieve a complete privacy and security transformation.

The privacy pain points that prompted MHS's first steps are representative of where many healthcare systems are today—an inability to fully detect, investigate, mitigate, and re-mediate security incidents. **MHS's journey to achieving those goals can be a roadmap that guides others to proactive risk mitigation built on strong policies and a culture of patient privacy.** For MHS, the foundation of their success is driven by the Imprivata FairWarning Patient Privacy Intelligence Platform and Managed Privacy Services.

> **"We needed a new approach to privacy investigation technology, privacy and security policies and workforce education that would ensure complete PHI access transparency."**

As one of the largest public health systems in the country, MHS serves all of southern Florida's population. The award-winning healthcare system has more than 1,800 beds, 13,000 employees, 2,500 physicians on staff, and hundreds of affiliate physicians across six hospitals and numerous ancillary healthcare facilities and physician practices.

The challenge of privacy access visibility

Like most growing healthcare organizations, MHS's existing enterprise-wide privacy policies created an influx of data without the resources and expertise to investigate each incident. This led to a privacy incident that resulted in a significant HIPAA-related settlement.

> **"Tracking access to our integrated Epic EHR by employed and affiliated physicians, as well as outside case reviewers and third parties, was essential, and we knew it would require more than just looking at logs for true cross-system transparency."**

The privacy incident became the rallying point for the creation of a detailed plan that would improve their security culture, strengthen their privacy and compliance posture, and ultimately enable them to provide even better care. Developing that plan would first require pinpointing the gaps in their security culture that led to the breach. Richard Leon, Chief Information Security Officer at MHS, summed up the situation at the time:

"We had a disconnect between implemented security technologies, privacy policies and staff education across disparate locations. Although we had robust security components, we needed a new approach to privacy investigation technology, privacy and security policies and workforce education that would ensure complete PHI access transparency."

While MHS had a privacy department, corporate compliance, regulatory policies, and log reviews, they realized they would need greater granularity and transparency for effective privacy and security.

MHS determined that addressing all of the privacy and access issues would require **a comprehensive PPM platform that could aid in managing the full lifecycle of a security incident.** "Tracking access to our integrated Epic EHR by employed and affiliated physicians, as well as outside case reviewers and third parties, was essential, and we knew it would require more than just looking at logs for true cross-system transparency," explained Richard.

Like many healthcare systems, MHS security and privacy teams worked in silos, but they determined that Imprivata FairWarning would be the ideal solution to change that ingrained approach. “Imprivata FairWarning would allow the two teams to work in tandem as opposed to separate process cultures, which was due to the lack of a holistic system for communication, collaboration and investigation,” explained Richard.

“Imprivata FairWarning provided the data to understand workflows, pinpoint workforce data access and privacy challenges, and guide training.”

Designing the Patient Privacy Roadmap

As the first step in the MHS privacy and security journey, Richard developed a **multipronged strategy framework that was built on a foundation of administrative policy controls and awareness training.** “Imprivata FairWarning provided the data to understand workflows, pinpoint workforce data access and privacy challenges, and guide training,” explained Richard.

According to Richard, this approach led to their first targeted use of Imprivata FairWarning for dealing with alerts for security incidents. Although the security and privacy teams had a strong security incident awareness, they had no visibility into their pervasiveness and nature throughout the organization.

“With the true picture of workflows provided by Imprivata FairWarning, we could identify the reasons behind records snooping and differentiate between legitimate and illegitimate reasons for PHI access,” explained Richard. That enables us to develop the training programs that guided people on what was and wasn’t acceptable and what they needed to be conscious of when accessing records.”

Education and collaboration for privacy and security

Richard and the combined security and privacy teams instituted a zero-tolerance policy that made it clear that employment would be terminated for any access violations. With a true understanding of end-user behaviors and process modifications needed to stop policy violations, the team then developed training campaigns and videos. “We personally provided personalized training to the thousands of employee and affiliated office staff people,” said Richard.

While the policy implementations and training encountered a bit of resistance to ingrained legacy processes changes, the real challenge, according to Richard, was balancing security measures with the need to ensure smooth workflows. “It was imperative that we not make the workflows cumbersome in ways that could negatively impact patient care,” he said.

Like many hospitals where security and privacy teams operate in silos, it was a combination of necessity and a desire to do the right thing for patient populations that led to the MHS transformation. The OCR corrective plan requirement following the breach had certainly made the transformation process a necessity. **But it was a common desire to do the right thing for patients and personnel that prompted the collaboration on developing privacy and security innovations.**

“Imprivata FairWarning enabled our security teams to load the logs and make sure that the data was available and working with IT, which enabled the privacy team to have information access through a single pane of glass,” explained Richard. This allowed MHS to proactively detect, investigate, mitigate, and remediate security incidents in a streamlined process.

Results of a 360-degree privacy view

It was a short time after implementation and training that MHS began to see **real results from their Imprivata FairWarning platform and the associated policies.** The health system now gets detailed reporting when PHI information is accessed and printed, as well as the reasons behind who, what, and why. Richard explained the real-world, tangible benefits of 360-degree view of PHI access:

“Imprivata FairWarning has reduced the snooping alerts from one a day to one a week with all of them being benign occurrences. It’s helped us to change our organizational culture around security and privacy so that risks have been decreased to near zero with the occasional benign snooping event. Furthermore, the 90% reduction in false positive alerts through the use of Imprivata FairWarning's Managed Privacy Services have saved us the time equivalent of two more FTEs to handle the past quantity of false alerts.

The teams have entered a deep analysis phase facilitated by workflow understanding in terms of data distribution involving third party vendors. According to Richard, recent OCR audits have all gone well and met the stringent corrective action plan mandates regarding their systems, policies, and monitoring.

"Imprivata FairWarning gave us a 360-degree understanding of potential risks and the ability to build privacy rules around them, which positions us for future implementation uses of the platform," said Richard. "Equally important is that we now have the technology, policies and processes to effectively handle the full lifecycle of a breach."

> **"The 90% reduction in false positive alerts through the use of Imprivata FairWarning's Managed Privacy Services have saved us the time equivalent of two more FTEs to handle the past quantity of false alerts."**

Proactive patient privacy

Since patient data privacy and security is a never-ending road, MHS has a vision for expanding their use of Imprivata FairWarning moving forward. This includes an emphasis on monitoring discharged and deceased patient records that can be accessed for illegal uses.

"We've had some law enforcement activity around the deceased patient records issue in the state, so we want to be proactive in monitoring access to these records for nefarious reasons," explained Richard.

In addition, MHS is also making plans for Imprivata FairWarning expansion around accountable care organization (ACO) activities. "We're currently working with two ACOs in fairly new arrangements," explained Richard. "ACOs don't necessarily have definitive patient populations, so we'll need to make sure that all PHI access is authorized and above board without any patient pilfering attempts, which is a major concern for us."

Another upcoming use of the Imprivata FairWarning platform is focused on MHS's integrated Epic EHR and its Community Connect service that allows other organizations to leverage their Epic environment.

"Imprivata FairWarning can provide the insights for guiding alert designs that ensure care connect organizations and ACOs are using the system appropriately, which is also a big challenge," said Richard.

> **"Imprivata FairWarning gave us a 360-degree understanding of potential risks and the ability to build privacy rules around them, which positions us for future implementation uses of the platform."**

Today, the MHS journey to continually improve patient care and privacy goes on. **With the agility and flexibility of the Imprivata FairWarning Patient Privacy Platform and Managed Privacy Services as a foundation, they have designed a roadmap for proactively mitigating risks and continually developing a culture dedicated to patient privacy.** This will enable them to continue to improve patient care as their organization continues to grow.

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

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

FW-CS-MemorialHealthSuccessStory-0321