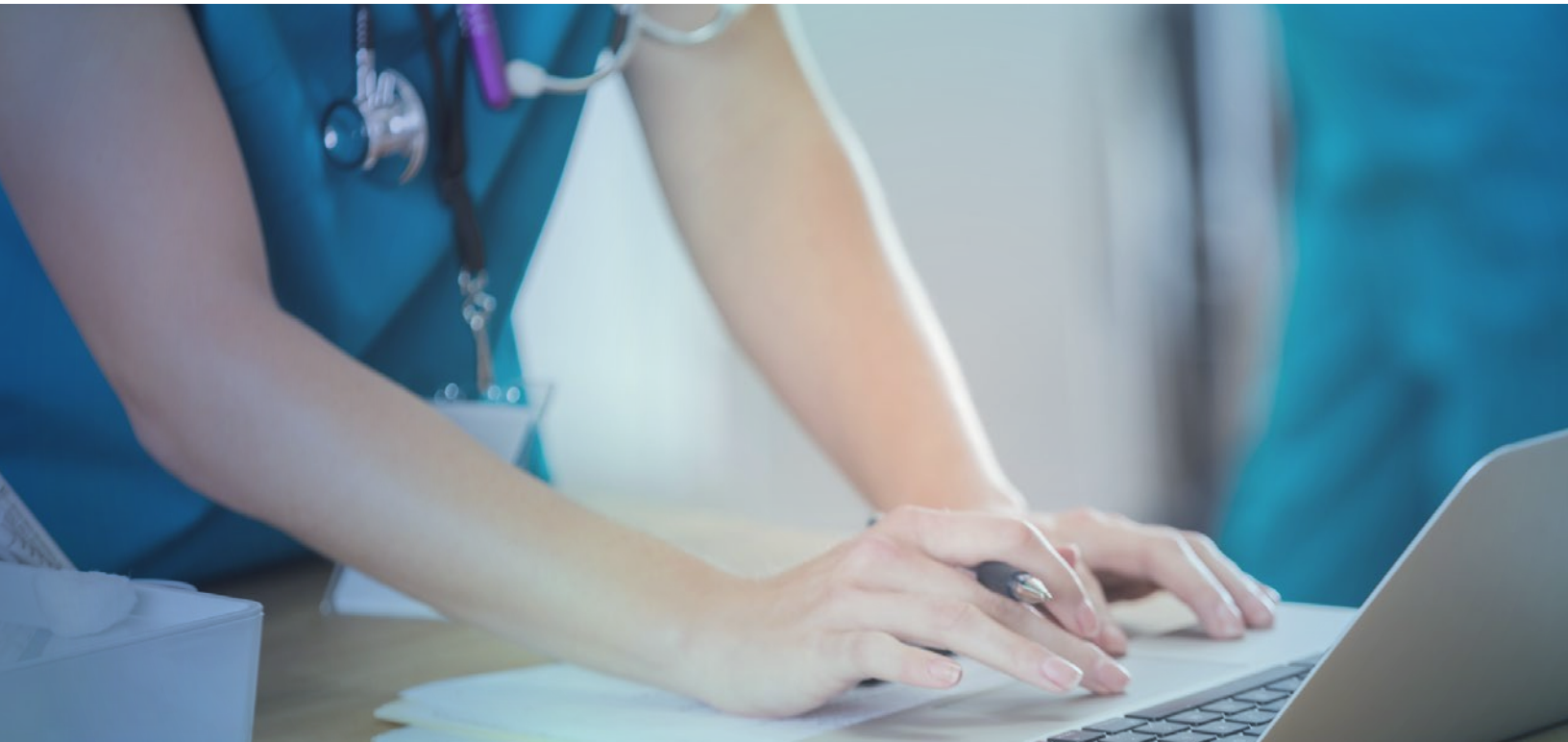
Tausight®

Whitepaper

Identifying and Protecting PHI at the Point of Risk

Provider Protected Health Information (PHI) data breaches are increasing at an alarming and unprecedented rate. While external third-party attacks receive a great deal of the headlines, one of the fundamental reasons for this occurrence is that clinical, IT and business workflows are extremely complex and vulnerable — and this puts PHI at risk. With the shift to remote care and accessing/moving PHI outside an organization's firewall, this risk level becomes even more acute.

A breakthrough new platform from Tausight combines real-time PHI identification and clinical workflow security to provide healthcare cybersecurity teams with the situational awareness necessary to protect PHI, before or even in the event of a breach. This proactive approach leverages best practices and cybersecurity principles recommended by HHS, NIST and PHE.



Executive Summary

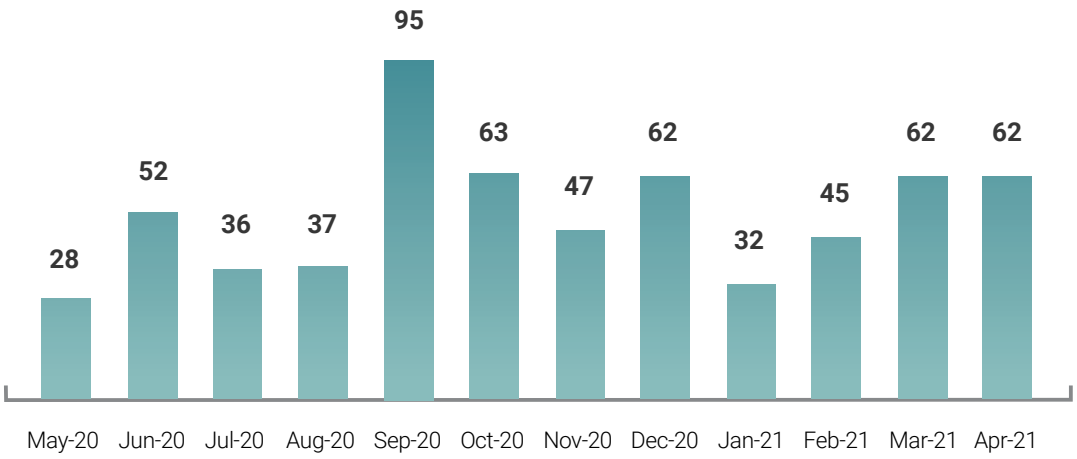
Today, the threat of cyberattacks and breaches has reached the point that most healthcare organizations understand that it's not a matter of whether a breach could occur but rather when it will occur.

It's a view shared by conclusions from the Healthcare Industry Cybersecurity Task Force: instead of recommending that organizations continue to act mainly on perimeter protection efforts, the task force emphasizes a focus on cyber-resilience and business continuity when a breach does occur.

Faced with this inevitability, healthcare organizations must not only establish a complete and comprehensive inventory of all the PHI across their entire environment, but also understand the risk to this PHI based on the endpoints where it resides. Doing so is the only way to avoid the impact to patients, the reputation of the organization, and the financial impact to all parties if a breach did occur.

This whitepaper will highlight the reasons why gaining complete visibility to, and understanding of, PHI across a healthcare organization's entire environment (both inside and outside the firewall) is mandatory in order to manage risk, minimize the possibility of an HHS OCR HIPAA Privacy and Security Rules violation disclosure, and protect patients. Traditional perimeter security tools focused on the technical security requirements of the infrastructure are not addressing this concern. The paper will also describe how breakthrough new solutions can now give healthcare security teams the 24/7 visibility they need to immediately see what is happening and take the most appropriate action to minimize risk and prevent potential PHI data breaches.

U.S. Healthcare Data Breaches in the Past 12 Months



HIPAA Journal 2021

So Many Breaches, So Much PHI Risk

Since 2015, more than 220 million healthcare records have been breached, and unfortunately, the trend will only get worse. In 2020 alone, there were 642 breaches of 500 or more individual patient records, the level that requires reporting to the U.S. Health and Human Services Office for Civil Rights (HHS OCR). Currently 89% of healthcare providers report that they have suffered some type of data breaches within the last two years.

It is not surprising that most healthcare CIOs' and CISOs' top concern — and top priority — is how to avoid a breach. In healthcare, protecting PHI is the cornerstone of patient trust and the very foundation of patient safety. Unfortunately, clinician workflows accessing PHI are extensive and varied and extremely difficult to protect, subjecting healthcare organizations of all sizes to compliance concerns and elevated security risks.

Shadow IT - 80% of employees say they use applications on the job that aren't approved by IT.

Guidelines such as the NIST Cybersecurity Framework and the HIPAA Safe Harbor Law provide baseline recommendations and best practices to help safeguard PHI. They present valuable guidelines related to an organization's overall security efforts, such as the need to inventory assets critical to protecting patient information, and to identify vulnerabilities presented by IT systems, users, devices, and endpoints.

But protecting PHI is extremely difficult. Even with a hard-to-hire team of cybersecurity professionals utilizing a range of disparate security tools a significant amount of an organization's PHI is still unseen and unaccounted for.

Shadow IT is a well understood concept in cybersecurity circles. 80% of employees say they use applications on the job that aren't approved by IT. In healthcare the problem is worse. When employees and staff install and use unauthorized IT applications, they further compromise health providers' security by creating and spreading "Shadow PHI."

Shadow PHI is patient protected information (PHI) that resides within or is now moving toward a position of hidden vulnerability. Shadow PHI is created in numerous ways, including workers placing PHI on removable devices (e.g., USB drives), leaving shared workstations unattended, including PHI in personal email systems, and in third-party clouds associated with many device apps. Shadow PHI is continually created and spread throughout a provider's environment, from acute care settings out to the edge.

Identifying and tracking Shadow PHI is a tall order. At worst, it's nearly impossible, for a number of major reasons:

1. While multi-industry perimeter, network, and endpoint security-focused tools play an important role in a healthcare organization's security stack, they simply weren't designed to provide continuous, real-time visibility and insight into the PHI stored and used at each endpoint and at the point-of-care.

2. Evolving healthcare delivery models — accelerated by the COVID-19 pandemic — now mean PHI is being sent and accessed outside firewalls and other traditional controls. As the industry shifts to more decentralized healthcare models and a growing number of remote clinical employees, more PHI data is being accessed, shared, and used beyond perimeter security tools.

3. The rapid growth of network-connected medical devices (IoMT) has dramatically expanded the footprint where PHI can be stored and accessed. Including these in a comprehensive "landscape" of where PHI exists has become mandatory.

Shadow PHI - Over 80% of healthcare patient data is unstructured!

All these add up to the need to secure clinical PHI-related workflows by gaining clear visibility to an organization's entire PHI landscape, and then understanding the risk of this Shadow PHI based on endpoint security, movement, and access — all this on a 24/7 real-time automated basis.

Why is Securing PHI so Difficult?

Faced with an explosion in endpoint devices and the need to manage a growing population of remote clinical employees, healthcare organizations are confronted with more concerns and questions than answers.

Most healthcare organizations are unable to address the following fundamental questions necessary for securing PHI workflows:

- Where is *all* of my PHI?
- Who and what is accessing it and where is it going (inside and outside the firewall)?
- How do I know the PHI on my endpoints is secure? Can I prove it?
- Where is all of my Shadow IT and where is the Shadow PHI in my environment?
- What is the extent of my risk in the event of a potential breach?
- If I did have a breach, would it be an HHS OCR reportable disclosure?
- Where are the gaps in my PHI security – especially with so much remote work?
- What actions can I take now to help reduce the risk of a breach? Where do I start?

Existing Cybersecurity Tools Can't Secure PHI Workflows

Cross-industry perimeter focused cybersecurity solutions available today have not been adequately designed to meet all of the uniquely complex needs of our healthcare systems. Largely adopted from other industries, cybersecurity methods are focused primarily on identifying network devices, traffic, and defending against perimeter attacks. These "Defense in Depth" solutions are not focused on identifying and managing a specific threat's risk to PHI.

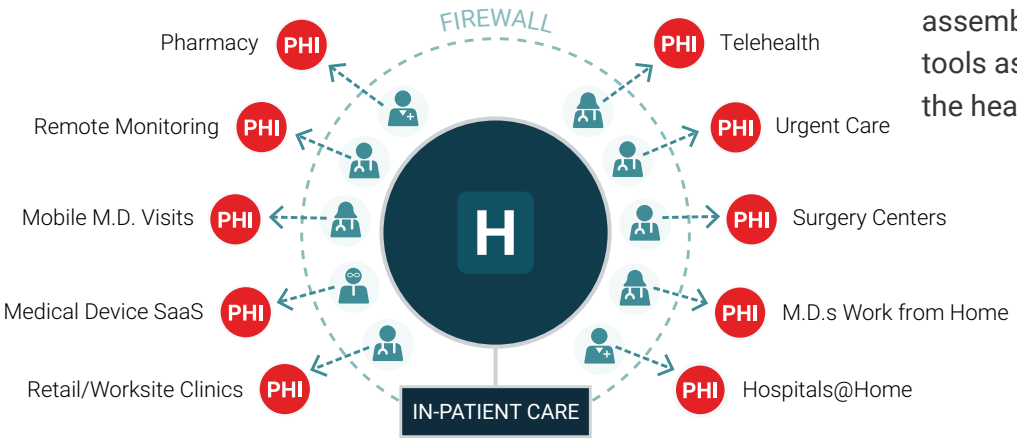
Endpoint security addresses that the computing health and integrity of endpoints are all parts of the overall chain of protection. The real need lies in combining these with an understanding of the data requirements associated with the workflow involved in delivering care.

While Data Loss Prevention (DLP) tools are often considered for use in the healthcare industry, they fail due to the need for well-structured content. DLP requires extensive pattern matching, custom policy rules creation, and ongoing management and rescanning due to the dynamic non-structured types of content generated by clinicians. What works in highly regulated industries like finance simply does not work when it comes to dealing with PHI data. The intelligence needed to identify whether content contains PHI requires intelligence beyond simple regular expressions, rules and even simple use of word statistics.

These are important distinctions because success requires the ability to accurately locate all of an organization's PHI, report on how the data is secured, and work outwards to understanding the security status of all the endpoints in use within an organization – both inside the firewall and externally – and do this on a 24/7 basis. In addition, security teams must also establish the integrity and availability of all the applications used by clinicians to understand the potential risk they might present as they access the PHI data.

Establishing a complete inventory of PHI (including hidden, orphaned, abandoned and in transit data), identifying workflow vulnerability, and assessing the overall risk to patient lives is extremely challenging and requires a purpose-built solution designed for healthcare. This isn't something to be assembled from a collection of security tools as it needs to address the nuances of the healthcare workflow.

Cybersecurity is not designed to protect PHI within clinical workflow or at the edge of decentralized, virtual healthcare.



Perimeter Approaches to Cybersecurity Cannot Defend Against Common Clinical Workflows and IT/Infrastructure Limitations

- Credential sharing issues
- Unattended, open desktops
- Overprivileged clinical users
- Decentralized IT with various security standards
- Shortage of IT security staff
- Remote/traveling staff take PHI with them
- IoT medical devices
- Legacy infrastructure and systems
- Explosion of virtual endpoints
- Inadequate physical computer security

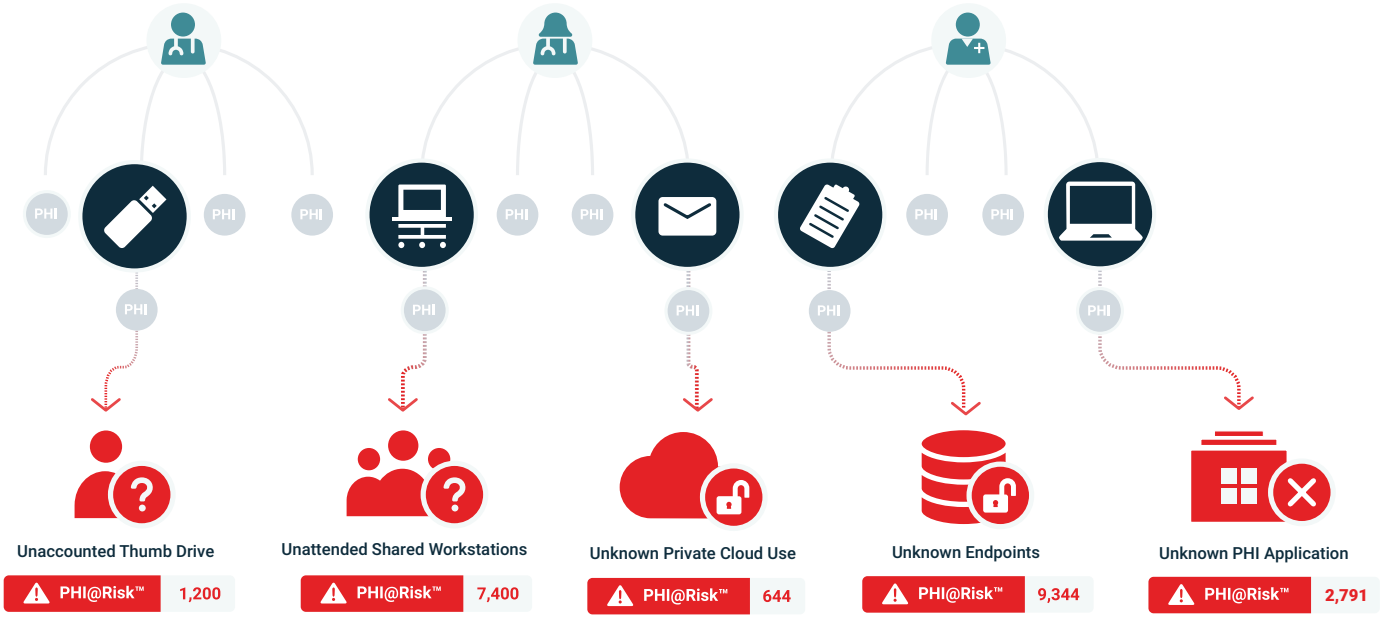
Tausight®: Different by Design

Imagine if healthcare organizations could take advantage of a new approach that enabled them to easily identify and inventory all the PHI spread across their organization, understand the vulnerabilities of the endpoint devices where it resides, and access the risk of incurring an OCR disclosure based on knowing the exact number of unique patient lives potentially impacted.

Now all of this is possible. The Tausight Clinical Workflow Security platform enables identification of real-time actionable PHI at the point-of-care. It provides complete visibility of the entire PHI landscape (inside/outside the firewall, hidden/orphaned/abandoned PHI), its movement, and user access on all endpoints.

Tausight helps change the conversation from *"an ePHI incident happened,"* to *"an incident is happening or could happen."*

Clinical Workflow Vulnerabilities

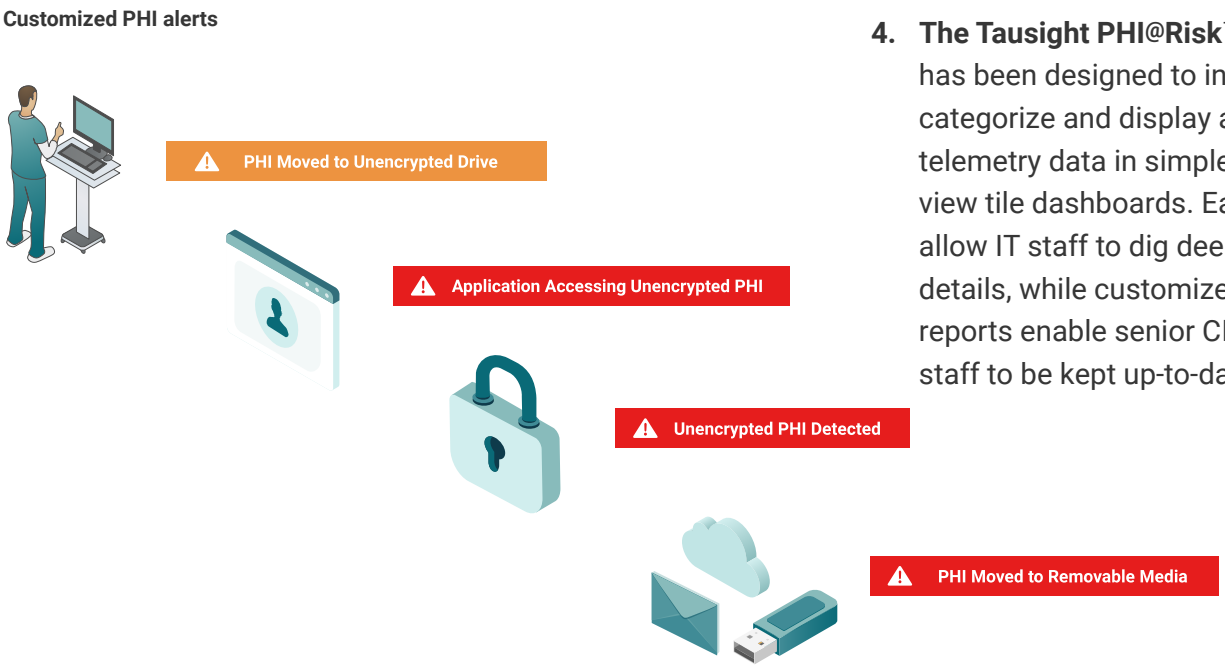


Designed on a modern cloud-based infrastructure and provided as a SaaS service, the Tausight Clinical Workflow Security platform utilizes leading-edge IoT and NLP/ML technologies to achieve up to a 95%+ PHI identification level, well above historical industry levels. Its Smart Differencing™ listening fidelity ensures exactly what PHI data to identify and track. Because it is a healthcare-specific solution, it supports all critical PHI clinical access workflows, while ensuring no impact on systems, performance or users.

Tausight's first product, Tausight PHI@Risk™, is part of the Tausight Clinical Workflow Security platform.

Tausight PHI@Risk™ consists of four major components:

1. **The TauOne® Service** is a smart telemetry agent that is deployed on endpoints. As the heart of the overall Tausight platform, this agent uses two separate machine learning-driven engines that actively learn, sense and monitor vulnerabilities across the entire IT system to detect and classify PHI on a continuous, real-time basis. Once deployed, the agent is invisible and self-updating. There is no need for system downtime or reboots.
2. **The TauOne® Server,** a private, cloud-based server that leverages the Google Cloud Platform and serves as the brain of Tausight PHI@Risk™. It utilizes Google Cloud Analytics and Tausight's proprietary, ML-driven Risk Prioritization engine that creates and prioritizes risk and threat scenarios from the raw telemetry vulnerability metadata generated by the TauOne® agent.
3. **The TauOne® Telemetry Transport Framework,** which is an IoT-based transport system that collects and delivers raw IT system vulnerability data to the TauOne® Service and the TauOne® Server with minimal effect on CPU usage, bandwidth, and connectivity
4. **The Tausight PHI@Risk™ User Interface,** has been designed to instantly categorize and display all the critical telemetry data in simple and easy-to-view tile dashboards. Easy drill downs allow IT staff to dig deep into specific details, while customized alerts and reports enable senior CIO and CISO staff to be kept up-to-date.



Complete Visibility, Complete Control

Tausight provides complete situational awareness of real-time actionable PHI telemetry at point-of-care across deployed endpoints inside and outside the firewall, while identifying the number of unique patients on each endpoint.

This has become critical for real-world healthcare challenges and use cases such as:

- Identifying unencrypted PHI on shared workstations
- Identifying unauthorized access or usage of PHI
- Identifying unsecured PHI data left on a wide range of devices
- Identification of PHI data exfiltrated outside the organization
- Classifying data retention risk presented by stale, orphaned, or expired PHI stored on a wide variety of devices

Summary: The Future of Clinical Workflow Security Starts Now

Today's healthcare environment is under constant cybersecurity attack, identifying and protecting PHI has become a mandatory requirement. CIOs and CISOs require purpose-built solutions for this need that operate on a 24/7 continuous real-time basis. Tausight provides this critical visibility into PHI at risk by combining PHI identification with insight to the vulnerabilities of the endpoints where it is stored and how it is being accessed, including: unencrypted files, unauthorized permissions, unpatched devices and unknown applications. Tausight provides the insight to enable healthcare security teams to take action before a potential breach can occur.

To learn more, visit www.tausight.com.

Tausight®

Identifying and Protecting PHI at the Point of Risk.

www.tausight.com