Tausight®

Protecting PHI at the Point of Risk

Healthcare is at high risk of PHI breach due to the hidden vulnerabilities and Shadow IT that exist within clinical workflow. Healthcare decentralization and the rapid expansion of virtual care further expose PHI and PII to increasingly unsecured and unseen vulnerability.

CISOs and their risk teams are increasingly asked, how can you better detect "Shadow IT" and protect and de-risk the “Shadow PHI” that exists alongside your hidden vulnerabilities?

A breakthrough new platform from Tausight overcomes previously insurmountable PHI identification and clinical workflow security issues and provides the real-time visibility healthcare cybersecurity teams need to protect PHI, before or even in the event of a breach.

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 questions than answers. Most healthcare organizations are unable to answer the following questions related to 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 secure are the endpoints where my PHI is residing?
- What is my risk of a potential breach exposure?
- If I did have a breach, would it be an HHS OCR reportable disclosure?
- What actions can I take now to help reduce the risk of a breach?

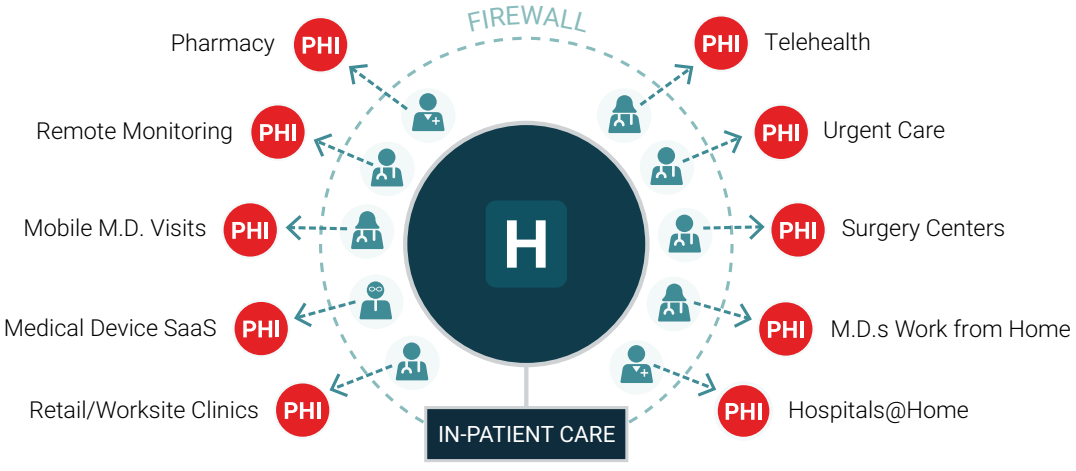
Cybersecurity Is Not Designed To Protect PHI Within Clinical Workflow or at the Edge of Decentralized, Virtual Healthcare

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.

Success requires the ability to first locate all of an organization’s PHI, report on the security status of the endpoints where it resides and determine the potential risk if it is exposed—all in real-time on a 24/7 basis.
Security teams must also establish the integrity and availability of applications used by clinicians and understand the risk to those devices where data may be stored.

Establishing a complete inventory of PHI (including hidden, orphaned and abandoned data), identifying workflow vulnerability, and assessing the overall risk to patient lives is extremely challenging and requires a purpose-built solution.

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 security for computers

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."*

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.

To learn more, please visit www.tausight.com.

Clinical Workflow Vulnerabilities