Tausight®

Situational ePHI Awareness™ for Reducing Risk and Aligning with 405d Healthcare Industry Cybersecurity Practices (HICP)

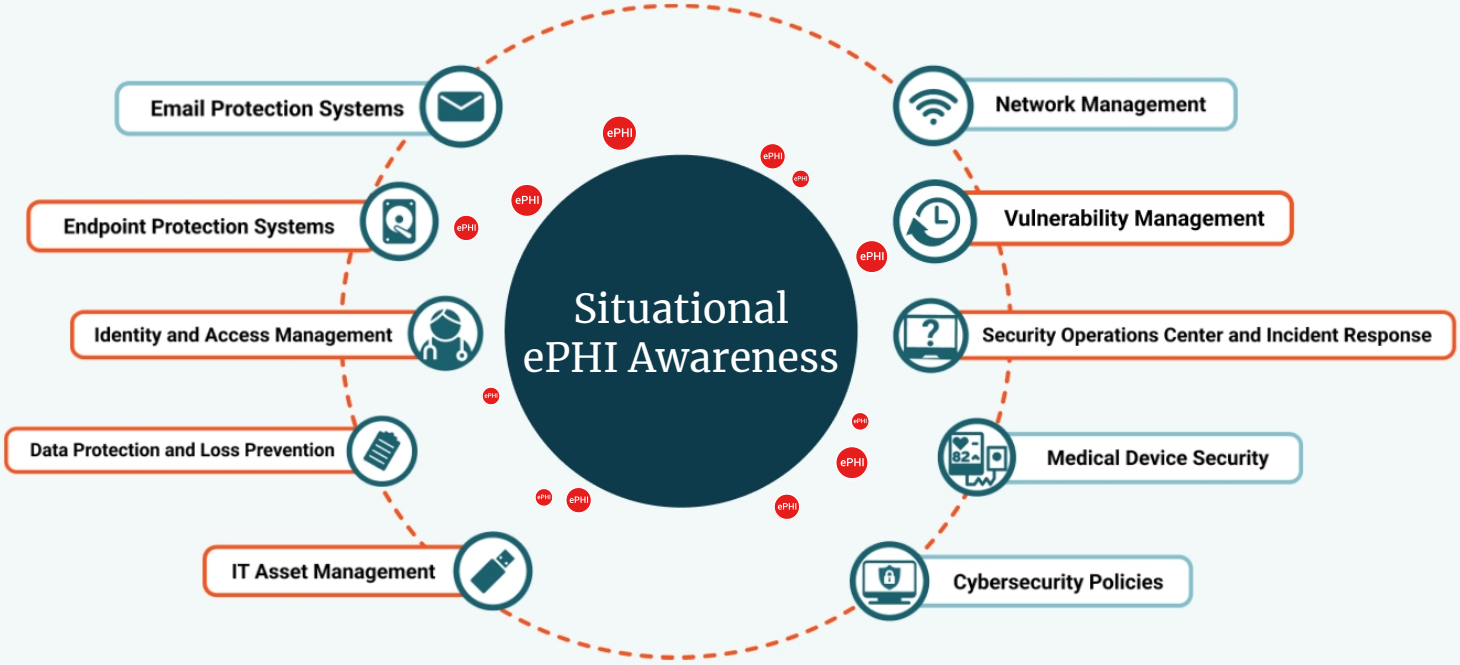
Large-scale information sharing is being accelerated by government policies and the rapid shift towards distributed care. Delivering on the promise of the 2009 HITECH (Health Information Technology for Economic and Clinical Health) Act, key provisions of the 21st Century Cures Act require providers, patients, payers, public health practitioners, technology developers, researchers, and other stakeholders to share ePHI.

- April 2021: Deadline for sharing of Consultation Note, Discharge Summary Note, History and Physical, Imaging Narrative, Laboratory Report Narrative, Pathology Report Narrative, Procedure Note, Progress Note
- October 2022: Deadline for expanding definition of EHI beyond USCDI
- December 2022: Deadline for use of standardized FHIR APIs for interoperability

Providers and patients need the freedom to share electronic health information (ePHI) in a compliant manner, inside or outside of the organization. As we realize the benefits that large-scale exchange of information have on improving patient outcomes and increasing efficiency of care, we also know that sharing ePHI between providers, patients, third parties and applications introduces greater and unfamiliar security risks.

Traditional cybersecurity was not designed to secure ePHI and clinical workflows at the edge of today's decentralized, virtual healthcare ecosystem. To help reduce risk, the U.S. Department of Health and Human Services (HHS) established the 405(d) Health Industry Cybersecurity Practices (HICP) Guide, which aligns with the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) and identifies ten fundamental cyber hygiene practices that are tailored to small, medium, and large organizations.

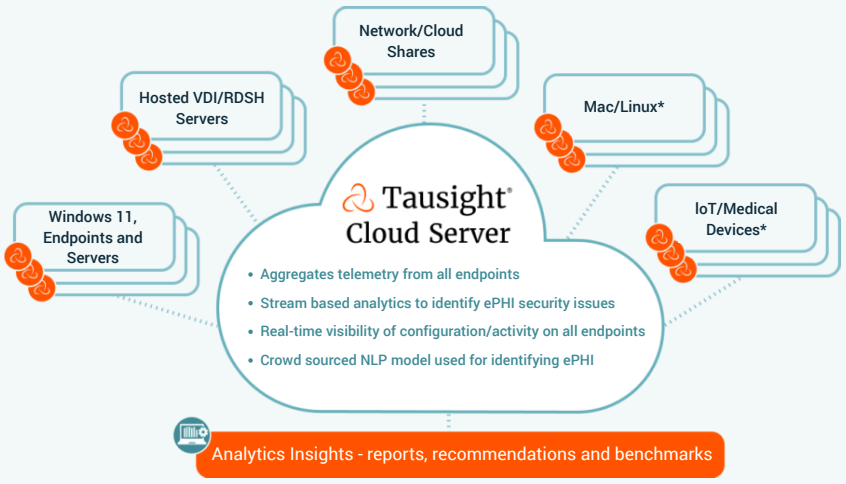
405(d) Healthcare Industry Cybersecurity Practices (HICP)



With the passing of Public Law 116-321 (HR 7898), also known as the Safe Harbor Act, in early 2021, Congress underscored the importance and value of 405d HICP by requiring the Secretary of Health and Human Services to consider it among the recognized security practices of covered entities and business associates when determining fines and penalties related to a breach of protected health information. Evidence that recognized security practices have been in place may be requested in regulatory inquiries and investigations. Additionally, alignment with 405(d) HICP can result in lower cyber insurance premiums, compliance with incident reporting regulations, simplified internal/external audits, and expedited cyber incident mitigation.

© Tausight™ 2022. Confidential. All rights reserved.

Validating cyber preparedness requires Situational ePHI Awareness



- SaaS service, self-updating sensor for Windows & VDI endpoints either inside/outside the firewall
- Real-time, full-stack ground truth telemetry for system, user, application, device, network, hardware, activity
- Content inspection detects ePHI at rest (files), in use (apps) and in transit (network, cloud)
- Natural language processing identifies ePHI in structured and unstructured data without pattern matching complexity
- Forensic audit trail for all activity events back to user accounts

Tausight Patented Sensors

* Future Offerings

Today's distributed healthcare delivery model relies on ePHI outside of the electronic medical record (EMR). To provide the level of security required to support the information-sharing demands of patients, providers and government regulations, one consolidated, real-time view into structured and unstructured data that is being created, received, maintained and transmitted between providers, patients, third parties and applications is required. The old model of layering multiple solutions designed to lock data down is cost-prohibitive, onerous, and ineffective. It's time to replace outdated, cross-industry technologies with a modern solution developed using leading-edge IoT and Natural Language Processing (NLP)/ Machine Learning (ML) to detect, classify and protect ePHI wherever it exists in today's information-sharing age. It's time for Situational ePHI Awareness.

Designed and built by healthcare experts, specifically for the modern healthcare ecosystem, Tausight provides real-time situational awareness across all endpoints, inside and outside of the organization to detect ePHI and determine whether they are being secured and defended as per the 405(d) HICP. Our ML-native, SaaS system provides 24x7 telemetry on the creation, access, storage, movement and replication of all ePHI, and produces actionable reports on security posture in alignment with HICP. Tausight's patented sensor monitor:

- Endpoint Protection
- Data Protection and Loss Prevention
- Identity and Access Management
- IT Asset Management
- Security Operations Center and Incident Response
- Vulnerability Management

Tausight data reports help IT, Security, Privacy and Compliance teams to measure and validate their cyber hygiene and security posture in real-time. They also provide an immutable, off-site audit trail with forensic-level details across all endpoints; before, during and after a cyber incident, including the information needed to quickly reconstitute the system and reconstruct any incident. This replaces the labor-intensive burden of manually constructing and reporting on limited sets of data activity with a self-service dashboard for comprehensive visibility into vulnerabilities and risk of ePHI at the edge.

© Tausight™ 2022. Confidential. All rights reserved.

405d HICP Snapshot Example Reports – Burlington General Hospital

The following example reports are based on the cyber preparedness of fictitious Burlington General Hospital and are designed to offer a view of the type of data that Tausight's patented sensor collects and the format in which that information is presented. The following is not a comprehensive set of the 405d HICP that Tausight supports, and it is just a sampling of the many reports that our Situational ePHI Awareness Platform generates.

Data Protection and Loss Prevention

Audit location of external movement

See files emailed externally, moved to removable media, and moved to cloud in real-time

Baseline comparison: <TBD>

Top Users Moving ePHI Files Outside of the Organization

Week Ending 10/31/21

45 Users
22.2% of total
– 4 from last week

User Moving the most ePHI Files	#of ePHI Files ↑	w/ High PII	Total Size of Files
nle	86	35	273 MB
hcong	79	20	155 MB
cokhwa	74	38	189 MB
syoomee	72	27	200 MB
sraikatuji	65	34	130 MB
citami	63	41	70 MB
stakizawa	60	4	102 MB
akanmani	59	25	67 MB
qcisse	43	22	62 MB
kconte	40	19	55 MB

10 of 45 Users

Data Protection and Loss Prevention

ePHI movement to removable media

See number of ePHI files moved to removable media for a given week as compared to the previous week

Considerations around movement of ePHI to USB:

- Are users authorized to move ePHI to USB according to organizational policies?
- Are users only using approved USB devices for the transfer of ePHI?
- Does the volume of activity stand out as very different from their peers?

Top Users Moving ePHI to Removable Media

Week Ending 10/31/21

31 Users
3.1% of total
– 2 from last week

User	Device	ePHI Files ↑	Total Size
jdunn	USB 3.0 (SanDisk)	60	50 MB
acurtis	USB 2.0 (SanDisk)	54	41 MB
bwood	USB 3.0 (PhotoStick)	50	25 MB
atamer	USB 3.1 (Apricorn)	10	5 MB
hsalam	USB 3.0 (SanDisk)	8	310 KB
mjohnson	USB 2.0 (SD Ultra)	8	290 KB
sberg	USB 3.1 (Apricorn)	2	281 KB
rkim	USB 2.0 (SanDisk)	2	199 KB
jmorris	USB 3.0 (SanDisk)	2	190 KB
pkozlov	USB 2.0 (Apricorn)	2	85 KB

10 of 31 Users Download CSV to view all

© Tausight™ 2022. Confidential. All rights reserved.

Endpoint Protection Systems

Audit endpoint encryption

See where ePHI lives on local drives and whether or not they are encrypted with BitLocker.

Recommendation:

For each device that handles ePHI, do one of the following, listed In order of preference:

01 Turn on full drive encryption (e.g., MS Windows bitlocker or Apple filevault)

02 Install a drive encryption solution

03 Secure the device, either by using cable locks or keeping the device in a locked room.

Goal is to have 99% of devices with encryption.

Baseline comparison: <TBD>

BURLINGTON HOSPITAL

Encryption Status

Month Ending 4/29/22

99%	91%	84%
Endpoints Encrypted	Volumes Encrypted	of All* ePHI Files Encrypted
+ 1% from last week	+ 3% from last week	- 6% from last week

All Unencrypted Endpoints

Endpoint with ePHI	↑ ePHI Files	w/ High PII	Total Size of ePHI
JillsLaptop	34	14	25 MB
Laptop_FDO943	28	6	12 KB
Laptop_FRR101	26	10	6 KB
Laptop_CLI864	20	5	15 MB
Desktop_FDO5438	18	6	35 MB
Desktop_CLI2007	14	11	3 MB
Laptop_FRR2129	14	3	2 MB
SanjaysLaptop	12	4	5 MB
Laptop_FRR8342	11	3	1 MB
Laptop_FDO1003	9	2	4 MB

10 of 23 Endpoints Download CSV to view all

Endpoint Protection Systems

Endpoint OS patch assessment

Understand which endpoints have gone unpatched for greater than 30 days on a monthly basis by comparing to common patches across your system

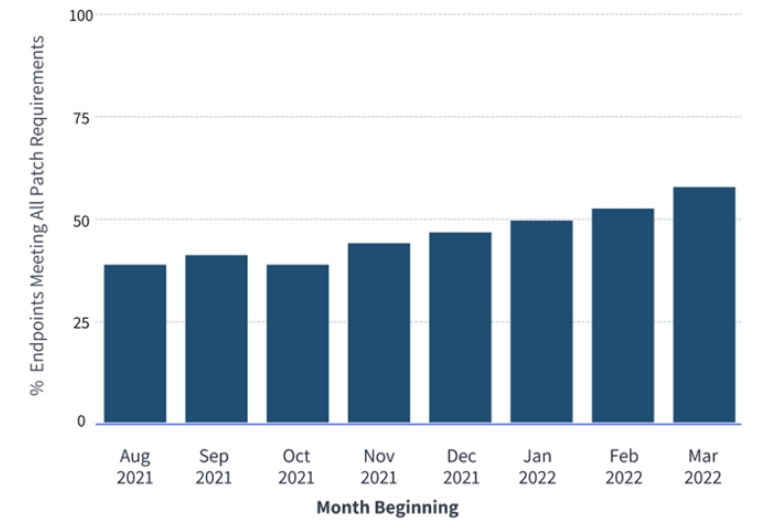
Recommendation:

- Identify the most vulnerable systems — those that have been unpatched the longest and contain the most ePHI — and apply updates ASAP.
- Identify systems that are not patched, perhaps because they were not rebooted, and work to ensure updates are applied regularly.
- Utilize these patching metrics to:
  - Monitor progress and identify risks
  - Provide real-time updates to the Board
  - Reduce cyber insurance rates
  - Validate "12 months of cybersecurity best practices" post breach, as noted in HR 7898 to qualify for reduced fines and shorter audits

Baseline comparison: <TBD>

BURLINGTON HOSPITAL

Endpoints Meeting All Patch Requirments Monthly



© Tausight™ 2022. Confidential. All rights reserved.

Endpoint Protection Systems

Low usage applications

Identify applications that are under-used and determine whether they need continued support or should be decommissioned

Recommendation:

Remove unused applications after confirming they are no longer needed. Such applications increase the "attack surface" and introduce risk.

Baseline comparison: <TBD>

BURLINGTON HOSPITAL

Applications Unused for Over 30 Days
(by endpoint instances)

As of Oct. 31, 2021

18 Apps
1.5% of total
– 0.6% from last month

Limiting the number of applications that have access to ePHI is important in reducing the ePHI attack surface of your system. Removing any unused applications...

Total Apps Unused for 60 days	18
Total Apps Unused for 90 days	7

Unused Applications that Access ePHI	Endpoint Instances ↑	Days Since Last Used
am_delta.exe v1.19.1	150	104
identity_helper.exe v20.1.76	144	65
hxtsr.exe v101.2865	120	87
steamengn.exe v19.12.37	120	156
anysearch.exe v4.11	111	68
bugsmash.exe v44.74.11	103	77
ufoclient.exe v9.1.39	99	102
maxcleanup.exe v16.90.112	84	93
cmdbash.exe v9009.2.38	83	61
specreducer.exe v7.0.12.8	60	70

10 of 18 apps Download CSV to view all

Status: Red - Machine Has Unencrypted ePHI

Lost / Stolen Laptop Report

WIN-DEV-108

unencrypted

371

ePHI Files on this Machine as of 2/22/22

BURLINGTON HOSPITAL

Last Seen: 2/22/22
Last Network Name (SSID): CUPOFJOE-WIFI

Users accessed this machine since 1/1/22: Jay Reams, Bob Finch
Last move of ePHI off Machine: 27 MB to removable media

ePHI Files on this Machine

Total Files: 371 (1.6 GB)

File Name	PII Density	File Size	File Path	Last User Accessed	Date Accessed
LabResult.doc	High	5 MB	c:\users\documents\labs	Jay Reams	2/22/22
NightShift.doc	High	1 MB	c:\desktop\...\shifts	Jay Reams	2/22/22
Rotation.txt	High	3 MB	c:\programdata\evernote	Jay Reams	2/10/22
RotationJan22.txt	High	111 KB	c:\jreams\...\myfiles	Jay Reams	2/10/22
Patient_Notes.txt	High	11 KB	c:\bfinch\...\myfiles	Bob Finch	2/1/22

View Full List of 330 Files

© Tausight™ 2022. Confidential. All rights reserved.

Incident Response

User Investigation

Supported Today: See all ePHI-related content and actions that an individual user is associated with

Baseline comparison: <TBD>

BURLINGTON HOSPITAL

Stan Smith

ssmith@hospital.com

Sep 1 - Dec 31, 2021

Total ePHI files moved	Files sent to unencrypted drive	Files sent to cloud	Files sent to external email
538 (489 MB)	**400** (183 MB)	**40** (101 MB)	**30** (186 MB)

Date	Suspicious Activity	Info
Dec 1, 2021	400 ePHI Files moved to unencrypted endpoint	network used: IP Address: Device Win-Dev-108
Sep 15, 2021	10 ePHI files sent to external email (recipient: rob258@gmail.com)	network used: IP Address: Device Win-Dev-108

The 405(d) HICP provide healthcare organizations of all sizes with a solid foundation for managing threats and protecting patients. Demonstrating alignment with these practices not only validates your organization's cyber preparedness, it can lower cyber insurance premiums, simplify compliance, streamline auditing and incident mitigation.

To Learn More Visit: www.tausight.com

© Tausight™ 2022. Confidential. All rights reserved.

Interested in validating your organization's cyber preparedness and alignment with 405(d) HICP?

Visit www.tausight.com/introducing_tausight/ for more information or a free trial and receive your 405(d) HICP alignment reports.

2022 Critical Insights Healthcare Data Breach Report on Cybersecurity report, which analyzes breach data reported to the U.S. Department of Health and Human Services (HHS) by healthcare organizations.

© Tausight™ 2022. Confidential. All rights reserved.