HHS 405(d) PROGRAM

Protecting Patients and Organizations

Current State in the Healthcare and Public Health (HPH) Sector

In July 2021, there were **52** reported hacking/IT incidents in which the protected health information of **5,393,331** individuals was potentially compromised.

SOURCE: HIPAAJournal.com, *July 2021 Healthcare Data Breach Report*

52 INCIDENTS

5,393,331 INDIVIDUALS

$25 BILLION LOSS

The healthcare sector lost $25 billion alone in 2021.

SOURCE: Verizon, *2020 Data Breach Investigations Report—Executive Summary*

$65 BILLION

The healthcare industry is expected to spend around **$65 billion** on cybersecurity between 2017 and 2021.

SOURCE: Herjavec Group, *The 2020 Healthcare Cybersecurity Report*

In July 2021, there were **70** reported data breaches of **500** or more records.

SOURCE: HIPAAJournal.com, *July 2021 Healthcare Data Breach Report*

70 BREACHES **500+ RECORDS**

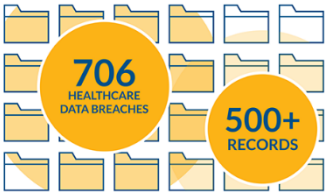
July 2021 was the **5th consecutive month** where data breaches in the healthcare sector have been reported at a rate of **2 or more per day.**

SOURCE: HIPAAJournal.com, *July 2021 Healthcare Data Breach Report*

From the start of August 2020 to the end of July 2021, the healthcare data of **44,369,781 individuals** has been exposed or compromised.

SOURCE: HIPAAJournal.com, *July 2021 Healthcare Data Breach Report*

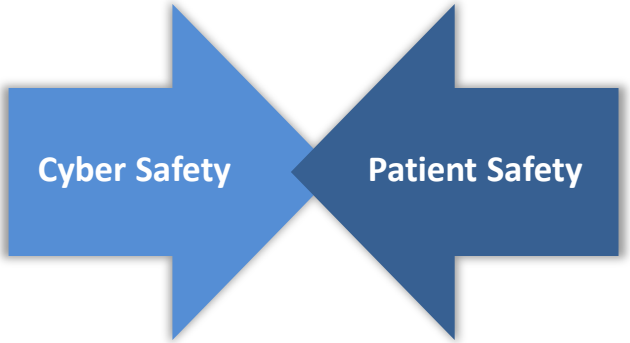
44,369,781 INDIVIDUALS' HEALTHCARE DATA BREACHED



From the start of August 2020 to the end of July 2021, there have been **706 reported healthcare data breaches** of **500 or more records.**

SOURCE: HIPAAJournal.com, *July 2021 Healthcare Data Breach Report*

Cyber Safety is Patient Safety

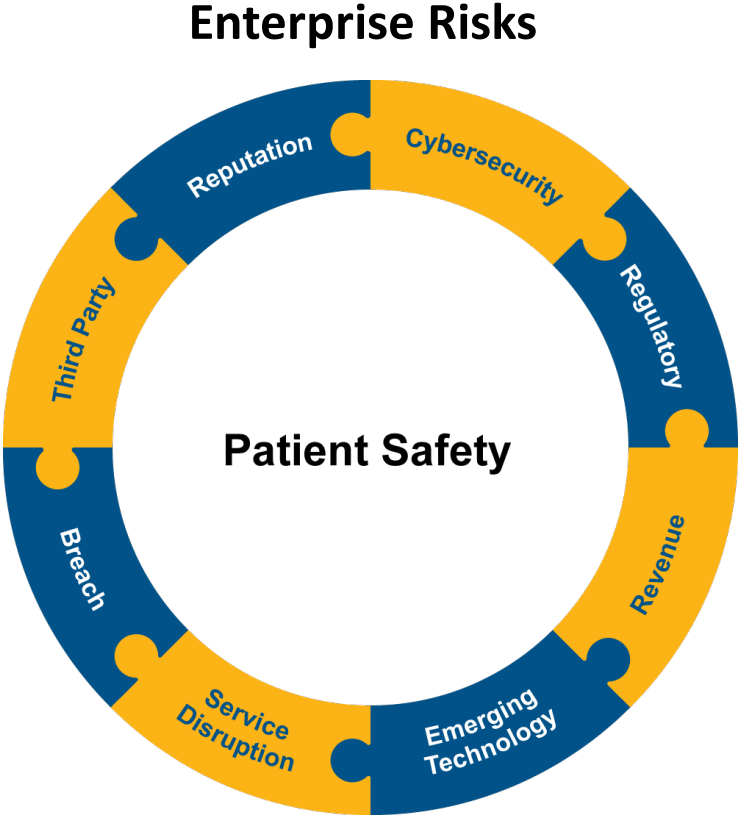


Cyber-attacks in healthcare affect every aspect of an organization, but most importantly they affect **patient safety.**

A single cyber-attack has the potential to shut down care facilities, erase important patient health history, and put your patients' health and identity at risk.

Cyber Risks are Patient Risks

Cybersecurity risks are one of many enterprise risks. These risks can affect every aspect of your organization including care delivery. The most important risk is to **patient safety,** which is the corner stone of every health organization.



Why Enterprise Risk Management?

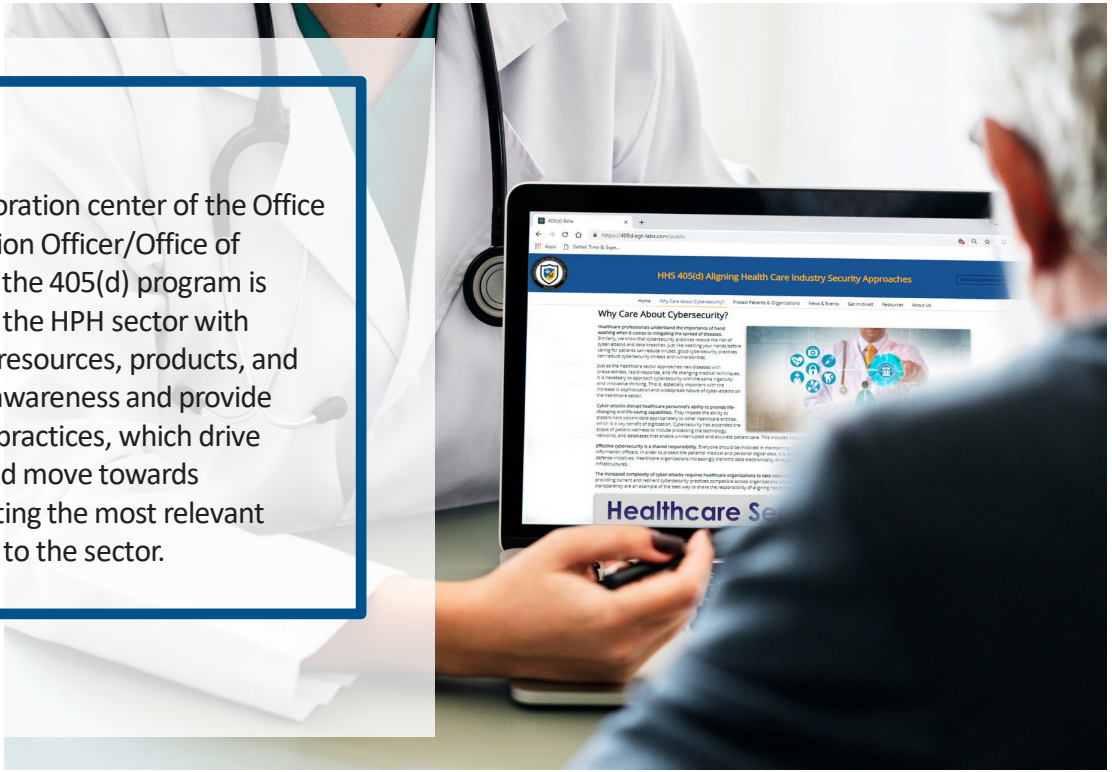
ERM-is an effective organization-wide approach to addressing the full spectrum of the organization's significant risks by **considering the combined array of risks as an interrelated portfolio**, rather than addressing risks only within siloes.

- Risks are **interrelated**
- ERM helps tie these **into mission impacts**
- ERM supports **credible decision-making** based on risk and opportunity information
- ERM **normalizes risks across many domains** to allow comparability

Aligning Healthcare Industry Security Approaches

Mission

As the leading collaboration center of the Office of the Chief Information Officer/Office of Information Security, the 405(d) program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector.



405(d) Task Group

The core of the 405(d) program is it's task group members. Convened by HHS in 2017, the 405(d) task group is comprised of over **230 +** information security officers, medical professionals, privacy experts, and industry leaders.

The task group members help drive all aspects of the 405(d) program, to include official program products, awareness campaigns, engagements, and outreach channels.

The task group is actively collaborating and working on a host of new resources for the sector including an update to the HICP publication and a new ERM Cybersecurity publication both of which are planned to be released in 2022/early 2023

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients

405(d)'s Cornerstone Publication

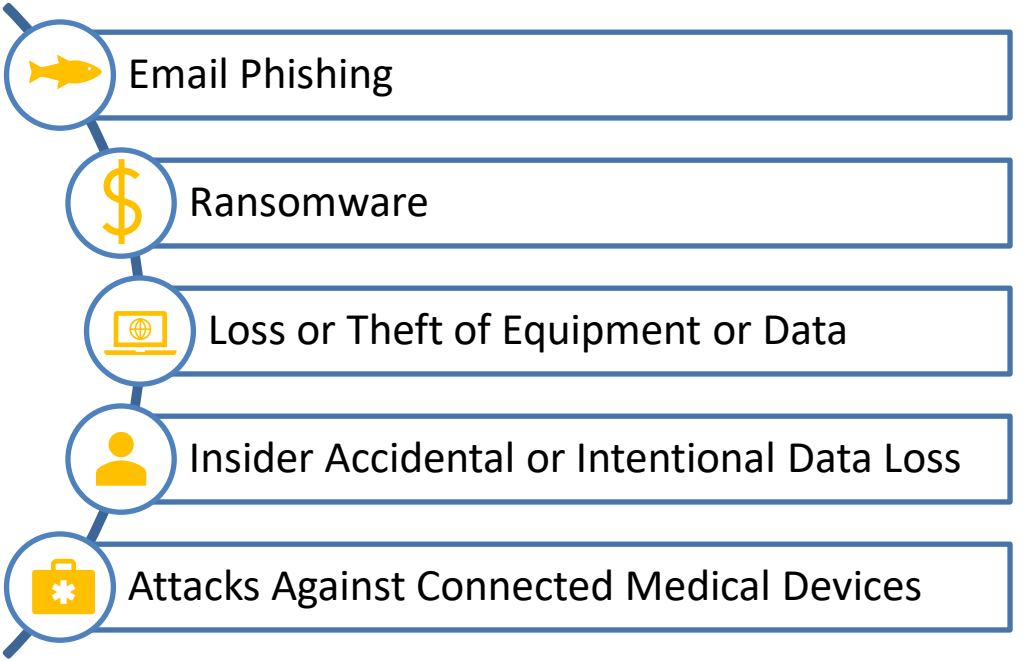
After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The **Main Document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.

Top 5 Threats



Top 10 Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

New 2021 HITECH Amendment

H.R.7898 — 116th Congress (2019-2020)

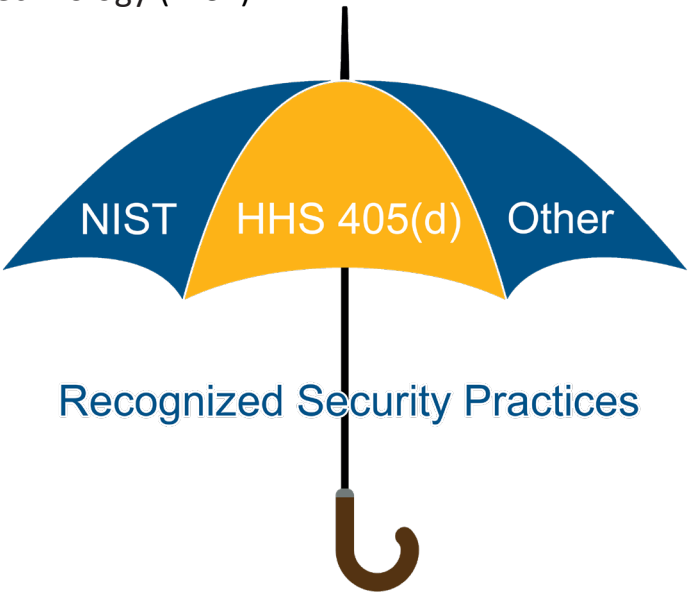
> To amend the Health Information Technology for Economic and Clinical Health Act (HITECH) to require the Secretary of Health and Human Services (HHS) to consider ***certain recognized security practices*** of covered entities and business associates when making certain determinations, and for other purposes.

Signed January 5, 2021 | Public Law No: 116-321

What are Recognized Security Practices?

The standards, guidelines, best practices, methodologies, procedures, and processes developed under the:

- National Institute of Standards and Technology (**NIST**) ***Cybersecurity Framework***
- ***HHS 405(d) Program*** approaches
- Other programs and processes that address cybersecurity and are developed, recognized, or promulgated through regulations under other statutory authorities



405(d) Outreach & Program Resources

Below you can find examples of communication products from 405(d) and the corresponding category the items fall under.

HHS/405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released more than 60 awareness products which organizations across the HPH sector can leverage.

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication!

405(d) SBAR

The 405(d) SBAR is a timely, event-oriented document to help healthcare organizations react and relate to current cyber events. Standing for Situation, Background, Analysis, and Recommendation, the 405(d) SBAR takes existing cyber alerts and tailors them to speak to the HPH sector.

Official Task Group Products

These resources are official products produced by the 405(d) Task Group. Examples include the HICP Publication, Quick Start Guides, New Cyber ERM Publication, and 5 threat flyers.

405d Website!

The new 405(d) Website is a one-stop shop for all the HPH sector's cybersecurity needs. On it you will find the HICP Publication, one-pagers, webinars, the Threat Mitigation Matrix, and more!

Tabs Include:

Why Care about Cybersecurity- Overview of the importance of cyber in the HPH sector

Protecting Patients and Organizations- HICP Publication, 5 threat and ten practices resources

News & Awareness Resources-405(d) post, Webinars, Cyber awareness resources

Get Involved-Sign up to be a part of the Task Group or get on our mailing list

Resources-Sign up to be a part of the Task Group or get on our mailing list

Questions?

Do you follow us on Social Media?
Check us out at **@ask405d**

Also, check out our new website!
405d.hhs.gov