The 405(d) Program

Aligning Health Care Industry Security Approaches

Legal Implications of a Cyber Attack

September 21, 2022

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) Task Group member; each iteration does not reflect the views of HHS as a whole. These presentations/engagements are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations. All Task Group Members have been invited to contribute to this webinar series.

* This Webinar is being recorded and will be available for future viewing. A note for any media representatives: While this event is open to the public, we would like to direct any media representatives to contact the public affairs office of whichever representative you have questions for to receive an official statement on behalf of the organization and refrain from quoting panelist during this event directly.

405(d) Events and Announcements

- **October**
  - Cybersecurity Awareness Month
    - 405(d) Toolkit
  - 405(d) Spotlight Webinar!
    - Date and Topic TBD

- **November**
  - National Critical Infrastructure and Resilience Month
  - 405(d) Post Release!

Agenda

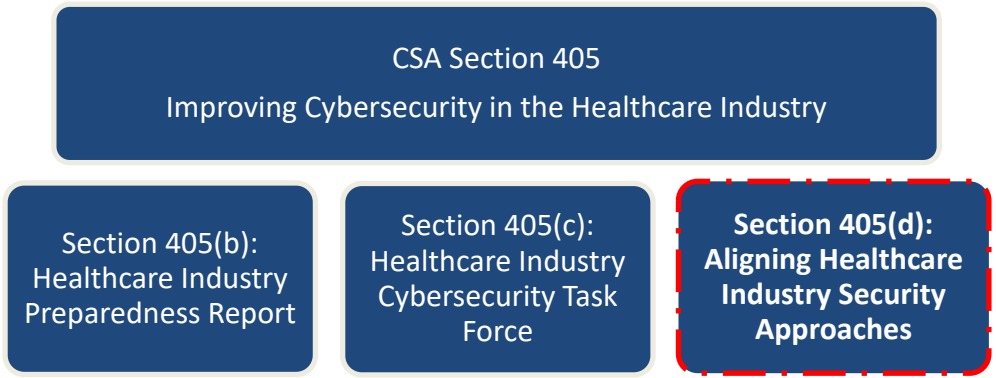
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Nick Rodriguez, HHS
40 Minutes	Legal Implications of a Cyber attack	Cindi Bassford, Dan Ongaro, Paul Otto
10 Minutes	Q&A and Closing	405(d) Team

Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of "Aligning Health Industry Security Approaches" by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



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.

Introductions to Our 405(d) Task Group Members/ Presenters

Cindi Bassford PMP, CISA, CISSP, CDPSE, LSSYB, is a partner at Guidehouse working in the areas of cybersecurity, health policy and system integration. She works across the U.S. Department of Health and Human Services, the U.S. Department of Education and on select publicly traded and privately held companies.

Dan Ongaro counsels clients on cybersecurity, data privacy, and data protection matters including corporate transactions, incident response, and investigations. Dan has been part of incidents involving ransomware, crypto-jacking, third party vendors, etc. and has helped clients respond to regulators, including the FTC, US state attorneys general, and international data protection authorities.

Lead of the Cybersecurity component of Hogan Lovells' practice, **Paul Otto** understands the regulatory environment surrounding cybersecurity risk management and incident response, with experience leading hundreds of cyber incident and assessment engagements.

Agenda


Introductions
Overview
Legal Landscape
Obligations and Costs
Litigation and Enforcement Highlights
Compliance Priorities

Overview

Legal Aspects of a Major Cybersecurity Incident

Immediate Response Actions /Crisis Management	Internal Incident Response & Investigation	Vulnerability Disclosures	Forensics and Technical Investigation	Post-Mortem Analysis and Enhancements
Insurance Coverage Review	Notifications to Individuals and Regulators	Customer/Partner Inquiries and Relations	Public Relations and Internal Communications	Coordination with Law Enforcement /Info Sharing
SEC Query or Investigation	Consumer Protection/Data Protection Authorities Inquiries and Investigations	Other Regulatory Inquiries and Investigations	Legislative Investigation and Inquires	Litigation (e.g., Consumer, Shareholder, B2B)

Do you Know What Data you Have?

Personal Information

Personally Identifiable Information (PII)

- Such as name, address, contact info, date of birth

Sensitive Personal Information (SPI)

- Such as PHI, payment card info, financial accounts, SSN, government-issued IDs)

Sensitive and Proprietary Information

Intellectual Property (IP)

- Such as patented technology, trade secrets

Competitive/Confidential Information

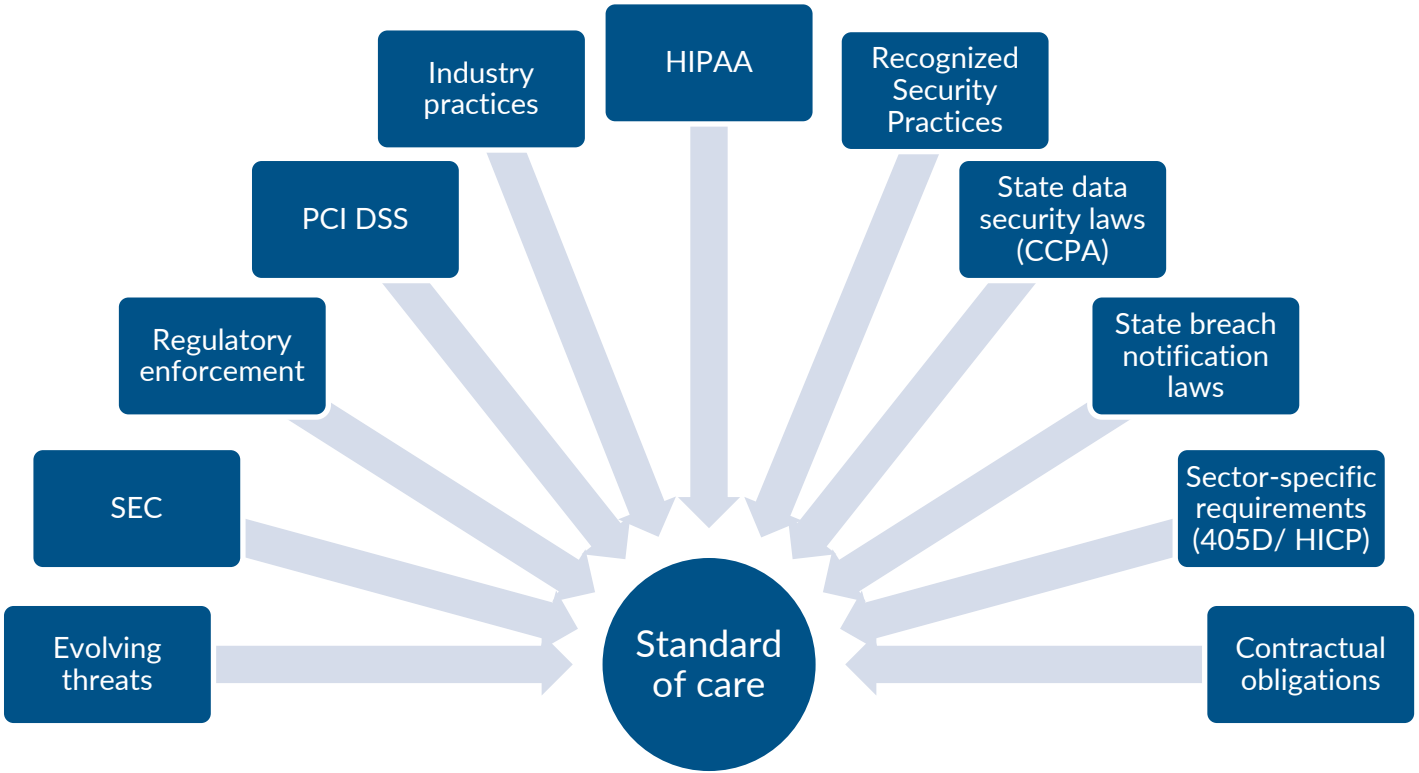
- Such as market analyses, financial reports, marketing strategies, new product development, customer lists

Collectively referred to as "sensitive information"

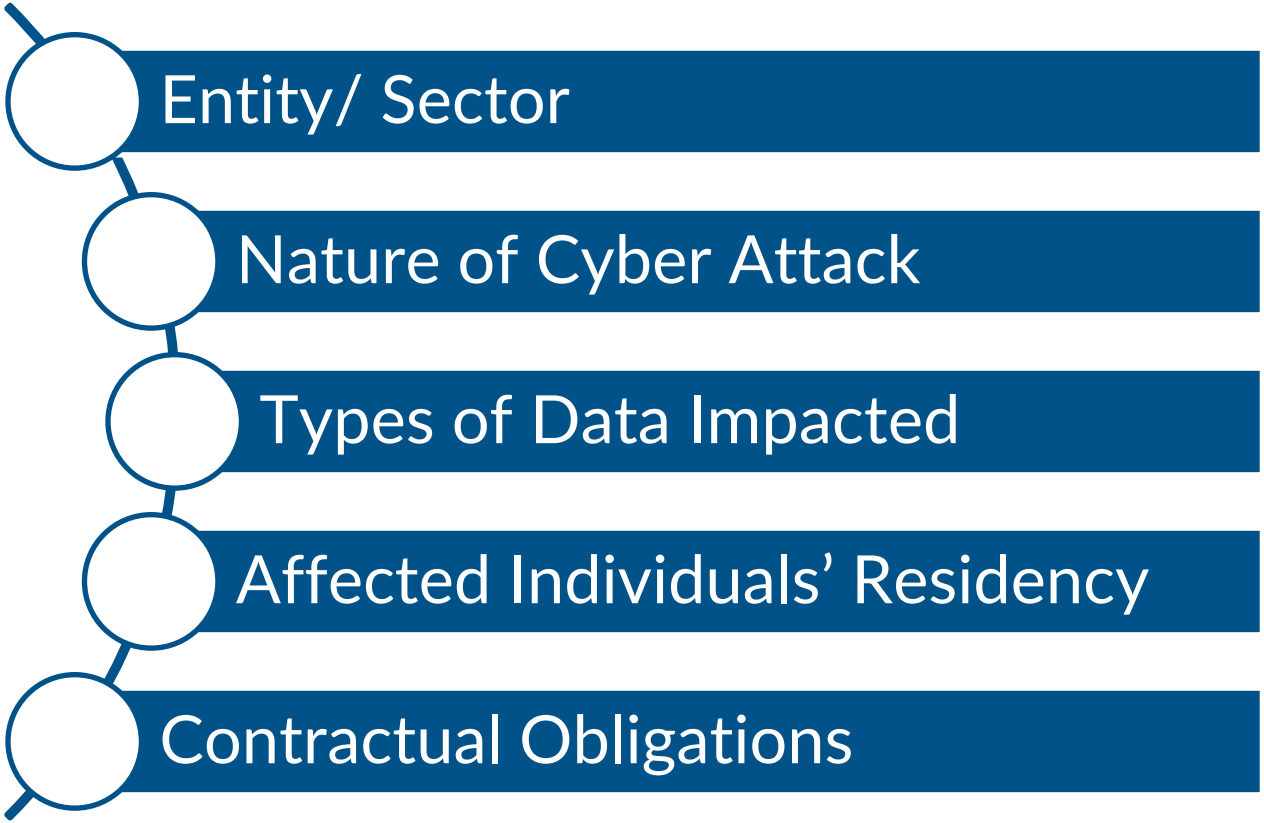
Legal Landscape

What are Organizations Expected to be doing?

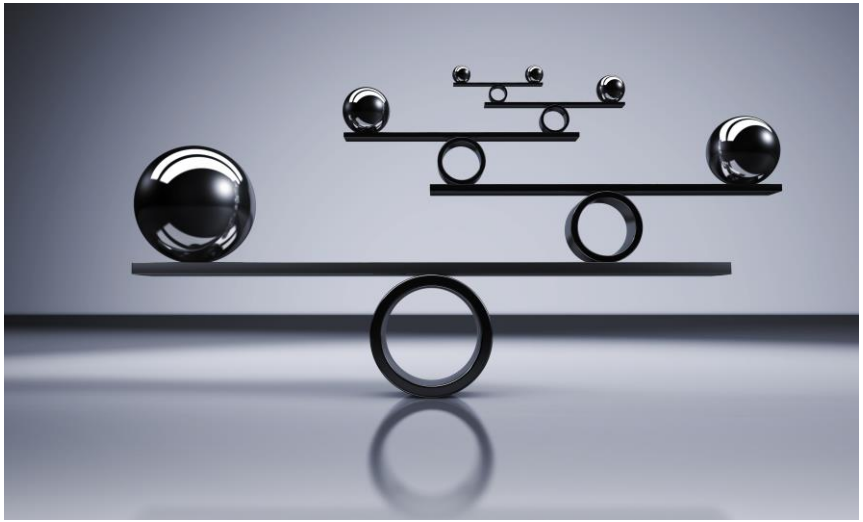
The legal standard of care an organization is expected to meet is shaped by numerous inputs



When do these Laws Apply in an Incident?



Consumer Litigation



- Standing
- State Consumer Protection Laws
- State Data Breach Notification Laws
- Negligence
- Breach of Contract / Implied Contract
- Unjust Enrichment

Obligations and Costs

Cyber Incident Response: Working with Legal

Contain and Control the Incident	• Provide legal guidance and support to incident response team • Help establish appropriate levels of privilege protection for response and investigation efforts • Establish a process to provide appropriate updates to senior leadership and the board
Work with Law Enforcement to Coordinate Activities	• Establish or supplement relationships with key law enforcement players • Assist in coordinating activities to avoid obstructing law enforcement operations • Obtain information from law enforcement to aid company response
Determine Scope and Nature of Incident	• Document how and when the incident occurred • Help assess risks and remediation options • Determine what information has been attacked
Guide Messaging and Assess Notification Obligations	• Identify relevant laws and contracts • Assess the scope, nature, and timing of any notification obligations (including law enforcement) • Review scope and nature of insurance coverage • Support and coordinate reports to senior management and board of directors
Assist with Notification Process If Necessary	• Review notice letters; internal messaging; customer notices; FAQs; letters to law enforcement, business partners, consumer reporting agencies, and other third parties; call center scripts; website notices; and media releases • Coordinate offering of remediation services (e.g., credit monitoring and identity theft insurance) • Coordinate with and support public relations and public affairs actions

Legal Aspects of a Major Cybersecurity Incident

Immediate Response Actions /Crisis Management	Internal Incident Response & Investigation	Vulnerability Disclosures	Forensics and Technical Investigation	Post-Mortem Analysis and Enhancements
Insurance Coverage Review	Notifications to Individuals and Regulators	Customer/Partner Inquiries and Relations	Public Relations and Internal Communications	Coordination with Law Enforcement /Info Sharing
SEC Query or Investigation	Consumer Protection/Data Protection Authorities Inquiries and Investigations	Other Regulatory Inquiries and Investigations	Legislative Investigation and Inquires	Litigation (e.g., Consumer, Shareholder, B2B)

Litigation and Enforcement Highlights

Increased State and Federal Regulatory Engagement

HHS OCR

- 122 cases with $133M+ in penalties
- **Anthem** (2018) $16M settlement for ~78.8M records in data breach (and $39.5M AG settlement in 2020)
- **Oklahoma State University – Center for Health Services** (2022) $875,000 settlement after post-incident investigation

FTC

- **Equifax** (2019) Unique $575M settlement with FTC, CFPB and nearly all U.S. states/territories (coordinated)
- Issued updated guidance in 2021 regarding health apps subject to specific breach notification requirements, signaling likely enforcement focus

State AGs

- **Uber** (2018) $148M settlement with 50 state AGs related to 2016 data incident
- **Premera Blue Cross** (2019) $10M settlement for ~10.4M records in 2015 data breach (along with $6.85M OCR settlement in 2020)
- **Medical Informatics Engineering** (2019) first multistate lawsuit involving a HIPAA-related data breach

SEC

- **Yahoo!** (2018) $35M settlement following alleged failures to disclose timely
- **First American**, **Pearson**, and others (2021)
- Issued proposed rules in March 2022 for updated cyber disclosure and reporting requirements

Plaintiff Trends

Smaller breaches (<10K victims) have seen an uptick in litigation, particularly with the right facts (e.g., sensitive data, California residents)

Plaintiffs continue to try to expand liability by:

- Including various causes of action (e.g., common law breach of confidence and intrusion upon seclusion)
- Testing novel theories of damages as a basis for larger awards (e.g., loss of privacy)

Forensic Investigator Incident Reports – *Capital One*

Nature & Timing

- Capital One had a preexisting contract with cyber consultant (Mandiant) for incident response services
- Later-in-time letter agreement between outside counsel and Mandiant did not alter the preexisting relationship or the core terms of that contract

Use of Report

- Cyber consultant's report was shared widely within Capital One and also with certain third parties, which underscored the "business needs" as opposed to a strong litigation purpose of the report
- Court noted these "disclosures are probative of the purposes for which the work produce was initially produced"

Payment terms

- At the time, Capital One designated Mandiant's work as a "Business Critical" expense as opposed to a "legal" one
- Mandiant was paid out of the incident response retainer and cybersecurity budget before these costs were re-designated as legal expenses months later

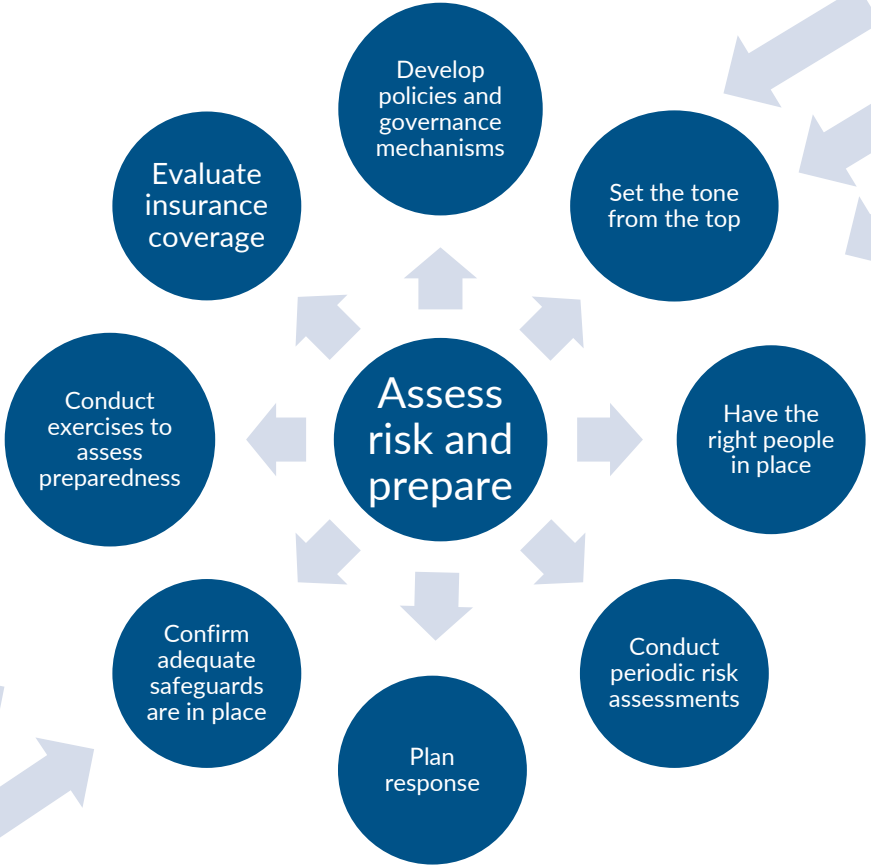
Key Takeaway: Use outside counsel and revisit retainer agreements

Compliance Priorities

Current and Emerging Cyber Issues

- Data breaches
- Ransomware and cyber extortion
- Law enforcement and information sharing
- Standard of care
- Vendor and supply chain risk
- GDPR & CCPA – "reasonable security"
- Cybersecurity maturity
- DDoS attacks/disruption
- IP theft and strategic attacks
- Litigation risk

What does Preparedness Mean for your Organization?



Technical activities

Technical activities

Cyber Legal Risk Management Opportunities

Incident response plan	Use of a cybersecurity framework	Encryption
• Can incorporate leading industry guidance, be tested regularly, and updated based on lessons learned	• Can align organization's cybersecurity to a framework • Can alter legal considerations. For example, some states have "safe harbor" laws for organizations who can show a cybersecurity framework	• Can cause an otherwise reportable data breach from a cyber-attack to fall outside the law's requirements and remedies • Encrypted backups can be the difference from a quick recovery and prolonged downtime

Cyber Legal Risk Management Opportunities

Contractual protections

- Limitation of liability
- Indemnification
- Audit Rights
- Representations for complying with cybersecurity and privacy requirements

Cyber insurance

- Opportunity to transfer some monetary risk from an attack

Law enforcement relationships and cooperation

- A proactive relationship with law enforcement allows for greater preparedness in the event of a cyber-attack
- Cooperation can also factor into legal considerations

Thank you!

Questions?

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

Linkedin.com/company/hhs-ask405d

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

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

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate. Read the entire publication on our website: [405d.hhs.gov](405d.hhs.gov)