October 24, 2024

Cybersecurity Developments in Health Care

Daniel Guggenheim
Quarles

Heidi Wachs
Stroz Friedberg, an Aon company

Rick Fitzgerald
Fireside Consulting

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Daniel Guggenheim
Partner
Quarles

Heidi Wachs
Managing Director
Stroz Friedberg, an Aon Company

Rick Fitzgerald
President
Fireside Consulting

Agenda

- Incidents and Enforcement Actions
- Evolving and Emerging Laws and Regulations
- Strategic Approaches and Tactics
- Tracking Technologies

Office for Civil Rights Enforcement Actions- Security Rule

- Providence Medical Institute Notice of Final Determination (announced October 3, 2024)
  - Ransomware enforcement action following 2018 breach report. Failure to have a BAA and failure to implement policies and procedures to allow only authorized persons or software access to ePHI.
- Cascade Eye and Skin Centers, P.C. Resolution Agreement and Corrective Action Plan (announced September 26, 2024)
  - Ransomware enforcement action following complaint. Failure to conduct compliant risk analysis and to have sufficient monitoring of its system activity to protect against cyber-attack.
- Heritage Valley Health System Resolution Agreement and Corrective Action Plan (announced July 1, 2024)
  - Ransomware compliance review following media reports. Failure to conduct accurate and thorough risk analysis, failure to establish and implement policies for responding to an occurrence that damages systems with ePHI and to restrict access.
- Green Ridge Behavioral Health, LLC Resolution Agreement and Corrective Action Plan (announced February 21, 2024)
  - Investigation following breach report revealed ransomware attack. Failure to conduct accurate and thorough risk analysis, failure to implement security measures to reduce risks and vulnerabilities to a reasonable level, to implement policies to regularly review records of system activity, and to disclose information only as permitted by Privacy Rule.
- Voluntary Resolution Agreement between HHS and Montefiore (announced February 6, 2024)
  - Investigation following breach notification for insider theft. Failure to conduct an accurate and thorough risk analysis, failure to implement procedures to regularly review records of system activity, and failure to implement technical and procedural mechanisms that record and examine system activity.
- Lafourche Medical Group LLC. Resolution Agreement and Corrective Action Plan (announced December 7, 2023)
  - Investigation following phishing attack. Failure to conduct risk analysis and no policies and procedures to monitor system activity.
- Doctors' Management Services, Inc. Resolution Agreement and Corrective Action Plan (announced October 31, 2023)
  - Investigation following breach notification after ransomware attack. Failure to conduct risk analysis, insufficient monitoring of system activity, and lack of Security Rule policies and procedures.

Enforcement Actions

- Resolution amounts from $40,000 - $4,750,000
- Corrective Action Plans include:
  - Conduct a Risk Analysis
  - Develop and implement a risk management plan
  - Implement process to regularly review records of system activity
  - Establish and implement a contingency plan
  - Implement process to assign unique user identification
  - Test and monitor the effectiveness of safeguards
  - Implement audit controls
  - Update Policies and Procedures, with HHS review
  - Conduct training
  - Identify, investigate and remediate non-compliance
  - Annual reports and attestations to OCR with monitoring

Incidents Reported

Health and Human Services, Office for Civil Rights, Annual Report to Congress on Breaches of Unsecured Protected Health Information, For CY 2022 (February 14, 2024)

- OCR received 626 notifications of breaches affecting 500 or more individuals
- Affected 42,000,000 individuals in aggregate
- Most commonly reported category of breach was Hacking/IT incident, which includes ransomware
- Largest Hacking/IT incident affected 3.4 million individuals

Incidents Reported . . .

DEPARTMENT OF HEALTH & HUMAN SERVICES — Office of the Secretary

Director
Office for Civil Rights
Washington, D.C. 20201

March 13, 2024

Re: Cyberattack on Change Healthcare

Dear Colleagues:

The Office for Civil Rights (OCR) is aware that Change Healthcare, a unit of UnitedHealth Group (UHG), was impacted by a cybersecurity incident in late February that is disrupting health care and billing information systems nationwide. The incident poses a direct threat to critically needed patient care and essential operations of the health care industry.

OCR administers and enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules, which establish the minimum privacy and security requirements for protected health information and breach notification requirements that covered entities (health care providers, health plans, and clearinghouses) and their business associates must follow. We are committed to ensuring access to care while enforcing laws that bolster patient privacy and security.

Given the unprecedented magnitude of this cyberattack, and in the best interest of patients and health care providers, OCR is initiating an investigation into this incident. OCR's investigation of Change Healthcare and UHG will focus on whether a breach of protected health information occurred and Change Healthcare's and UHG's compliance with the HIPAA Rules.

Laws and Regulations

Washington My Health My Data Act, Data Security Practices

RCW 19.373.050 Data security practices. (1) Except as provided in subsection (2) of this section, beginning March 31, 2024, a regulated entity and a small business shall:

(a) Restrict access to consumer health data by the employees, processors, and contractors of such regulated entity or small business to only those employees, processors, and contractors for which access is necessary to further the purposes for which the consumer provided consent or where necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business; and

(b) Establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's or the small business's industry to protect the confidentiality, integrity, and accessibility of consumer health data appropriate to the volume and nature of the consumer health data at issue.

(2) A small business must comply with this section beginning June 30, 2024. [2023 c 191 § 7.]

Quarles

Laws and Regulations

California Confidentiality of Medical Information Act

A business that electronically *stores* or maintains medical information on the provision of sensitive services, including, but not limited to, on an electronic health record system or electronic medical record system, on behalf of a provider of health care, health care service plan, pharmaceutical company, contractor, or employer, shall develop capabilities, policies, and procedures, on or before July 1, 2024, to enable all of the following:

(A) Limit user access privileges to information systems that contain medical information related to gender affirming care, abortion and abortion-related services, and contraception only to those persons who are authorized to access specified medical information.

(B) Prevent the disclosure, access, transfer, transmission, or processing of medical information related to gender affirming care, abortion and abortion-related services, and contraception to persons and entities outside of this state in accordance to this part.

(C) Segregate medical information related to gender affirming care, abortion and abortion-related services, and contraception from the rest of the patient's record.

(D) Provide the ability to automatically disable access to segregated medical information related to gender affirming care, abortion and abortion-related services, and contraception by individuals and entities in another state.

Laws and Regulations

Federal Trade Commission, Health Breach Notification Rule

- On April 26, 2024, the Federal Trade Commission finalized changes to the HBNR to strengthen protection for data collected by health apps and other technologies
- The HBNR requires vendors of PHRs and related entities that are not covered by HIPAA to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health information.
- The HBNR also requires third party service providers to vendors of PHRs and PHR related entities to notify such vendors and PHR related entities following the discovery of a breach
- Rule effective July 29, 2024

Laws and Regulations

New York Hospital Cybersecurity Requirements (October 2, 2024)

- Establish a comprehensive program
- Create defined cybersecurity policies
- Designate a CISO and sets personnel requirements
- Vulnerability testing
- Audit trails and records retention
- Risk assessments
- Policies for third-party cybersecurity vendors
- Identity and access management
- Training and Monitoring
- Incident Response Plan
- Report incidents affecting operations (72 hours)

One year to comply, except Incident Reporting immediately effective

NYS Register/October 2, 2024 Rule Making Activities

Possible rural concerns are not distinct from the concerns of other stakeholders, and stakeholders who participated in the discussions represent stakeholders in rural areas as well as other demographic and geographic areas of the State. NEDPA, the New York Farm Bureau, the Long Island Farm Bureau, local Soil and Water Conservation Districts, various county health departments, Environmental Justice communities and the general public were notified in advance of an informational webinar on the proposed revisions that was held on October 27, 2022. The Notice of Proposed Rule Making will be published in the State Register and in the Environmental Notice Bulletin, and at least one virtual public hearing will be held.

Job Impact Statement

It is apparent from the nature and purpose of the proposed rules, as set forth in the Summary of Express Terms, that they will not have a substantial adverse impact on jobs and employment opportunities. The proposed rules will have no positive or negative impact on jobs and employment opportunities at all, except that the proposed rules are expected to result in a slight decrease in the need for consulting services that is not substantial for facilities that obtain pumping test waivers or that qualify for a permit exemption based upon the rule making revisions. The Department made this determination based on an analysis of the consulting services that would be needed after the rule making compared to those services currently needed.

Department of Health

NOTICE OF ADOPTION

Hospital Cybersecurity Requirements

I.D. No. HLT-49-23-00001-A
Filing No. 771
Filing Date: 2024-09-13
Effective Date: 2024-10-02

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Addition of section 405.46 to Title 10 NYCRR.

Statutory authority: Public Health Law, section 2803

Subject: Hospital Cybersecurity Requirements.

Purpose: To create cybersecurity program requirements at all article 28 regulated facilities.

Substance of final rule: The proposed regulation would create a new section 405.46 of Title 10 (Health) of the Official Compilation of Codes, Rules and Regulations of the State of New York, to create cybersecurity requirements for all hospital facilities.

Section 405.46(a) identifies all general hospitals in New York State as subject to the regulations.

Section 405.46(b) defines certain terms and language for purposes of the section.

Section 405.46(c) establishes the requirements for hospitals to have a cybersecurity program and defines protocols, procedures, and core functions of such program.

Section 405.46(d) defines the cybersecurity policies that general hospitals will need to create and the topics that should be considered after a risk assessment has been performed.

Section 405.46(e) requires general hospitals to designate a Chief Information Security Officer.

Section 405.46(f) sets forth the requirements for testing and vulnerability of a general hospital's cybersecurity program.

Section 405.46(g) outlines the audit trails and records maintenance and retention requirements of a general hospital's cybersecurity program.

Section 405.46(h) sets forth the requirements for cybersecurity risk assessments and the considerations for policies and procedures relative to those risk assessments.

Section 405.46(i) sets forth the requirements for cybersecurity personnel general hospitals must utilize.

Section 405.46(j) sets forth the policies for third-party service providers of cybersecurity programs.

Section 405.46(k) sets forth the requirements for identity and access management.

Section 405.46(l) sets forth the requirements for training and monitoring of the cybersecurity program.

Section 405.46(m) defines the requirements for an incident response plan in the event of a cybersecurity incident.

Section 405.46(n) defines the reporting requirements for a general hospital during a cybersecurity incident.

Section 405.46(o) refers to confidentiality and the applicability of State and federal statutes.

Section 405.46(p) provides general hospitals one (1) year from the date of adoption to comply with the new regulatory requirements, except that general hospitals must immediately begin reporting to the Department as required by subdivision (n) of this section.

Section 405.46(q) states that if any provisions of the section are found to be invalid, it shall not affect or impair the validity of other provisions of the section.

Final rule as compared with last published rule: Nonsubstantial changes were made in section 405.46(b)(7), (8), (e)(3)(v), (g)(2), (h)(1), (n)(1) and (p)(1).

Revised rule making(s) were previously published in the State Register on May 15, 2024.

Text of rule and any required statements and analyses may be obtained from: Katherine Ceroalo, DOH, Bureau of Program Counsel, Reg. Affairs Unit, Room 2438, ESP Tower Building, Albany, NY 12237, (518) 473-7488, email: regsqna@health.ny.gov

Revised Regulatory Impact Statement

Statutory Authority:

Public Health Law (PHL) § 2803(2)(a) authorizes the Public Health and Health Planning Council (PHHPC) to adopt and amend rules and regulations, subject to the approval of the Commissioner of Health (Commissioner), to implement PHL Article 28 and establish minimum standards for health care facilities, including general hospitals.

Legislative Objectives:

The legislative objectives of PHL Article 28 include the protection of the health of the residents of the State by promoting the efficient provision and proper utilization of high-quality health services at a reasonable cost.

These regulations fulfill this legislative objective by ensuring that general hospitals within New York State implement minimum cybersecurity controls to safeguard protected health information (PHI) and personally identifying information (PII) from being publicly disclosed or used for identity theft.

Needs and Benefits:

The healthcare industry is one of the most targeted communities for cybersecurity scams and breaches due to the significant amount of sensitive and financially lucrative information healthcare facilities collect. Currently in New York State there are no cybersecurity requirements for the safeguarding and security of patients' protected health information (PHI) and personally identifying information (PII). As a result, New Yorkers seeking medical care have no guaranteed minimum levels of protection of their information. As a result of this, there have been several high-profile cybersecurity breaches at facilities across the state which have resulted in not only a loss of patient financial and health data, but in some cases has also delayed care.

Additionally, cybersecurity events at hospitals can have significant, far-reaching, and long-term impacts to the provision of patient care and operation of the facility. Governor Hochul has been focusing on cybersecurity and ensuring that New Yorkers data stays safe no matter where they go. The promulgation and implementation of cybersecurity focused regulations supports this initiative. These regulations will ensure all hospitals develop, implement, and maintain minimum cybersecurity standards, including cybersecurity staffing, network monitoring and testing, policy and program development, employee training and remediation, incident response, appropriate reporting protocols and records retention.

There will be multiple benefits to the adoption of these regulations. Given the significant differences in preparedness statewide against cybersecurity attacks, these regulations will ensure hospitals are required to maintain a minimum level of readiness to prepare for, respond to, and quickly recover from cybersecurity incidents.

Costs:

Costs to Regulated Parties:

The costs associated with the implementation by regulated facilities will vary significantly due to the varying levels of cybersecurity programs and policies hospitals currently have in place. Some facilities may have mature monitoring, training and response programs, whereas others may not. Therefore, the costs could vary from tens of thousands to tens of millions. Hospitals will be allowed to sub-contract for cybersecurity services and this may reduce the overall cost of program implementation. It is estimated that effective cybersecurity programs can cost between $250,000 and $10 Million to develop and implement initially and anywhere from $50,000 - $2 Million or more to maintain on a yearly basis depending on the facility size. For small hospitals (of which there are 15 and are defined as less than 10 acute care or ICU beds), ongoing annual

Quarles

Laws and Regulations

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Notice of Proposed Rulemaking, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) (April 4, 2024)

Covered entities to report to CISA:

- covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred
- ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made.

To enhance CISA's ability to identify trends and track cyber threat activity across the cyber threat.

Comment period was extended to July 3, 2024.

Laws and Regulations

Healthcare Cybersecurity Act of 2024 (July)

118TH CONGRESS
2D SESSION

S. 4697

To enhance the cybersecurity of the Healthcare and Public Health Sector.

IN THE SENATE OF THE UNITED STATES

JULY 11 (legislative day, JULY 10), 2024

Ms. ROSEN (for herself, Mr. YOUNG, and Mr. KING) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To enhance the cybersecurity of the Healthcare and Public Health Sector.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Healthcare Cybersecurity Act of 2024".

SEC. 2. DEFINITIONS.

In this Act—

(1) the term "Agency" means the Cybersecurity and Infrastructure Security Agency;

118TH CONGRESS
2D SESSION

H. R. 9412

To enhance the cybersecurity of the Healthcare and Public Health Sector.

IN THE HOUSE OF REPRESENTATIVES

AUGUST 27, 2024

Mr. CROW (for himself, Mr. FITZPATRICK, Mr. KIM of New Jersey, and Ms. SALAZAR) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To enhance the cybersecurity of the Healthcare and Public Health Sector.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Healthcare Cybersecurity Act of 2024".

SEC. 2. DEFINITIONS.

In this Act—

(1) the term "Agency" means the Cybersecurity and Infrastructure Security Agency;

Health Infrastructure Security and Accountability Act of 2024 (September)

118TH CONGRESS
2D SESSION

S. 5218

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 25, 2024

Mr. WYDEN (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Finance

A BILL

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Health Infrastructure Security and Accountability Act of 2024".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Quarles

Laws and Regulations

Florida Cybersecurity Incident Liability (Vetoed, June 2024)

HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/CS/HB 473 Cybersecurity Incident Liability
SPONSOR(S): Judiciary Committee and Commerce Committee, Giallombardo and others
TIED BILLS: **IDEN./SIM. BILLS:** CS/SB 658

FINAL HOUSE FLOOR ACTION: 81 **Y's** 28 **N's** **GOVERNOR'S ACTION:** Vetoed

SUMMARY ANALYSIS

CS/CS/HB 473 passed the House on March 1, 2024, and subsequently passed the Senate on March 5, 2024.

Current law requires counties and municipalities (referred to as local governments in this section) to implement, adopt, and comply with cybersecurity training, standards, and incident notification protocols. Local governments are required to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute for Standards and Technology (NIST) Cybersecurity Framework.

NIST is a non-regulatory federal agency housed within the United States Department of Commerce, whose role is to facilitate and support the development of cybersecurity risk frameworks. NIST is charged with providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks. While the NIST Cybersecurity Framework was developed with critical infrastructure in mind, it can also be used by organizations in any sector of the economy or society.

Additionally, current law requires covered entities, governmental entities, and third-party agents to comply with specified notification protocols in the event of a breach of security affecting personal information.

The bill provides that a county or municipality that substantially complies with the cybersecurity training, standards, and notification protocols under current law or any other political subdivision of the state that complies with these standards and protocols on a voluntary basis, is not liable in connection with a cybersecurity incident.

The bill also provides that a covered entity or third-party agent, that acquires, maintains, stores, processes, or uses personal information is not liable in connection with a cybersecurity incident if the covered entity or third-party agent substantially complies with notice protocols as provided in current law as applicable, and has also adopted a cybersecurity program that substantially aligns with the current version of any standards, guidelines, or regulations that implement any of the standards specified in the bill or with applicable state and federal laws and regulations. The bill provides certain requirements for a covered entity or third-party agent to retain its liability protection.

The bill does not establish a private cause of action. The bill further provides that its provisions apply to any suit filed on or after the effective date of the bill and to any putative class action not certified on or before the effective date of the bill.

The bill does not affect state or local government revenues or expenditures.

The effective date of the bill was upon becoming a law; however, this bill was vetoed by the Governor on June 26, 2024.

RON DESANTIS
GOVERNOR

FILED
2024 JUN 26 PM 5:03
DEPARTMENT OF STATE
TALLAHASSEE, FL

June 26, 2024

Secretary Cord Byrd
Secretary of State
R.A. Gray Building
500 South Bronough Street
Tallahassee, Florida 32399

Dear Secretary Byrd:

By the authority vested in me as Governor of the State of Florida, under the provisions of Article III, Section 8 of the Constitution of Florida, I do hereby veto and transmit my objection to Committee Substitute for Committee Substitute for House Bill 473 (CS/CS/HB 473), enacted during the 126th Session of the Legislature of Florida during the Regular Session 2024 and entitled:

An act relating to Cybersecurity Incident Liability

CS/CS/HB 473 provides broad liability protections for state and local governments and private companies that only substantially comply with minimum cybersecurity standards in the event of a data breach or other cybersecurity event.

As passed, the bill could result in Floridians' data being less secure as the bill provides across-the-board protections for only substantially complying with standards. This incentivizes doing the minimum when protecting consumer data. While my Administration has prioritized policies to reduce frivolous litigation, the bill before me today may result in a consumer having inadequate recourse if a breach occurs.

I encourage interested parties to coordinate with the Florida Cybersecurity Advisory Council to review potential alternatives to the bill that provide a level of liability protection while also ensuring critical data and operations against cyberattacks are protected as much as possible—and the disruption that comes with the release of potentially sensitive information.

For these reasons, I withhold my approval of CS/CS/HB 473 and do hereby veto the same.

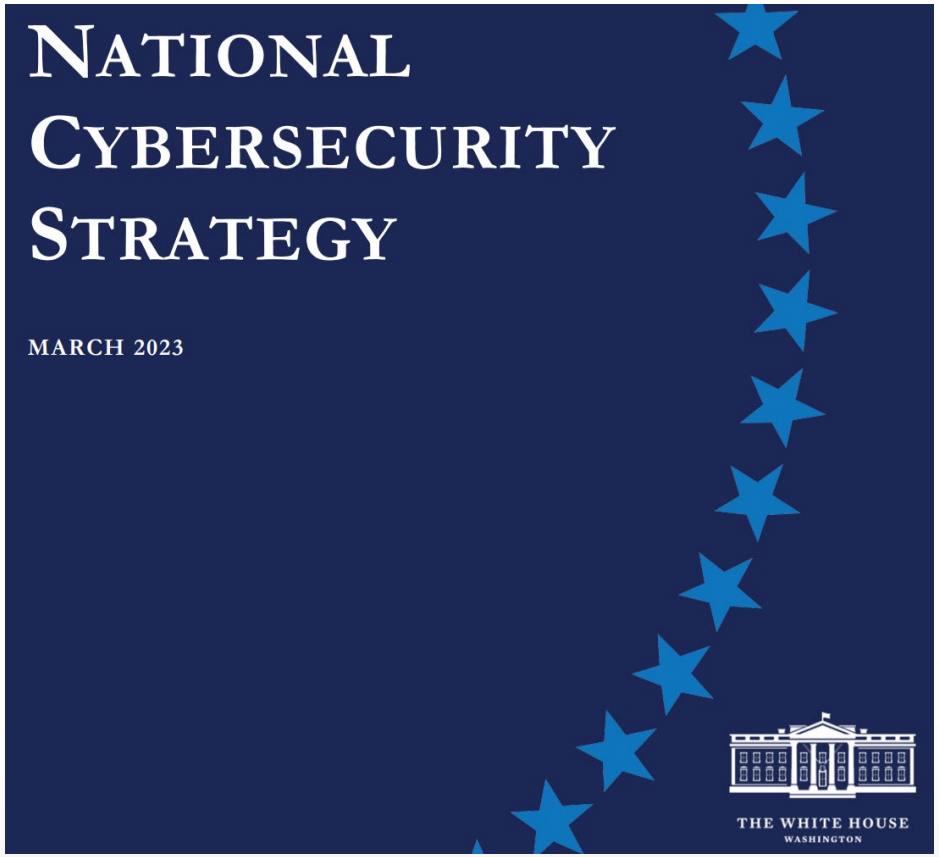
Sincerely,

Ron DeSantis
Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399 • (850) 717-9249

Quarles

Strategic Approaches



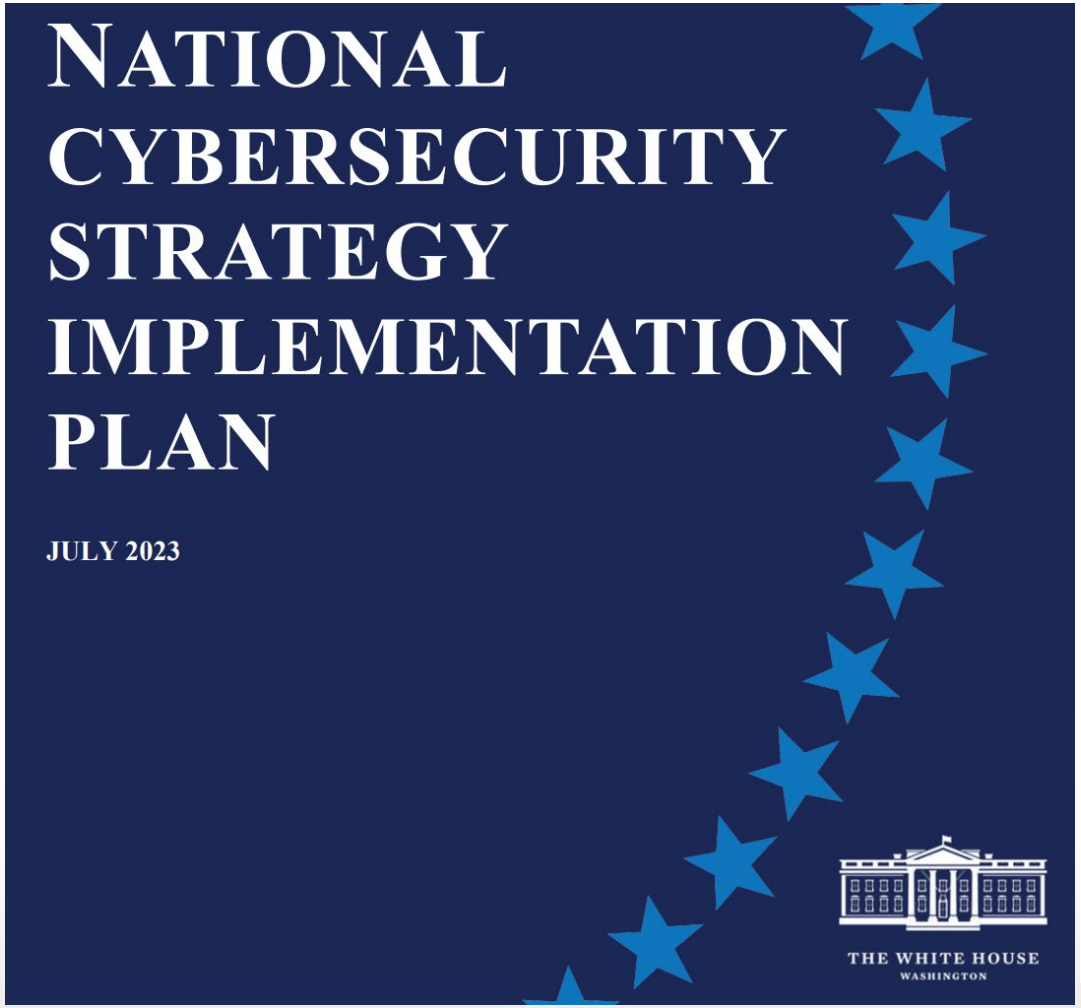
1) Defend Critical Infrastructure
2) Disrupt and Dismantle Threat Actors
3) Shape Market Forces to Drive Security and Resilience
4) Invest in a Resilient Future
5) Forge International Partnerships to Pursue Shared Goals

Strategic Approaches

Pillar Three

- Market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience
- Organizations that choose not to invest in cybersecurity negatively and unfairly impact those that do
- We must:
  - Hold the stewards of our data accountable for the protection of personal data
  - Drive the development of more secure connected devices
  - Reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies

Tactics



Strategic Objective 3.3: Shift Liability for Insecure Software Products and Services

Initiative Number: 3.3.1

Initiative Title: Explore approaches to develop a long-term, flexible, and enduring software liability framework

Initiative Description

The Office of the National Cyber Director, working with stakeholders in academia and civil society, will host a legal symposium to explore different approaches to a software liability framework that draw from different areas of regulatory law and reflect inputs from computer scientists as to the extent that software liability may or may not be like these other regimes.

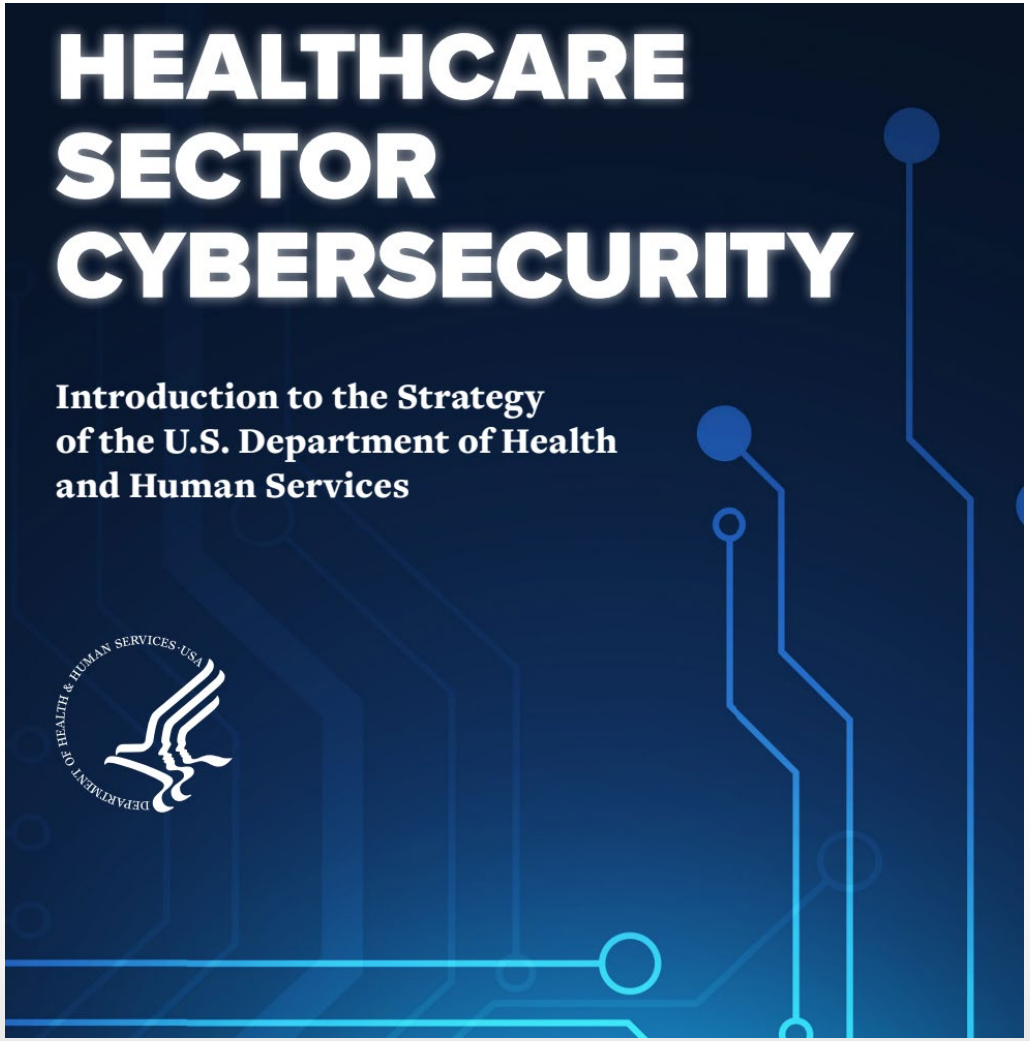
NCS Reference

To begin to shape standards of care for secure software development, the Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services... The Administration will work with Congress and the private sector to develop legislation establishing a liability regime for software products and services.

Responsible Agency: ONCD

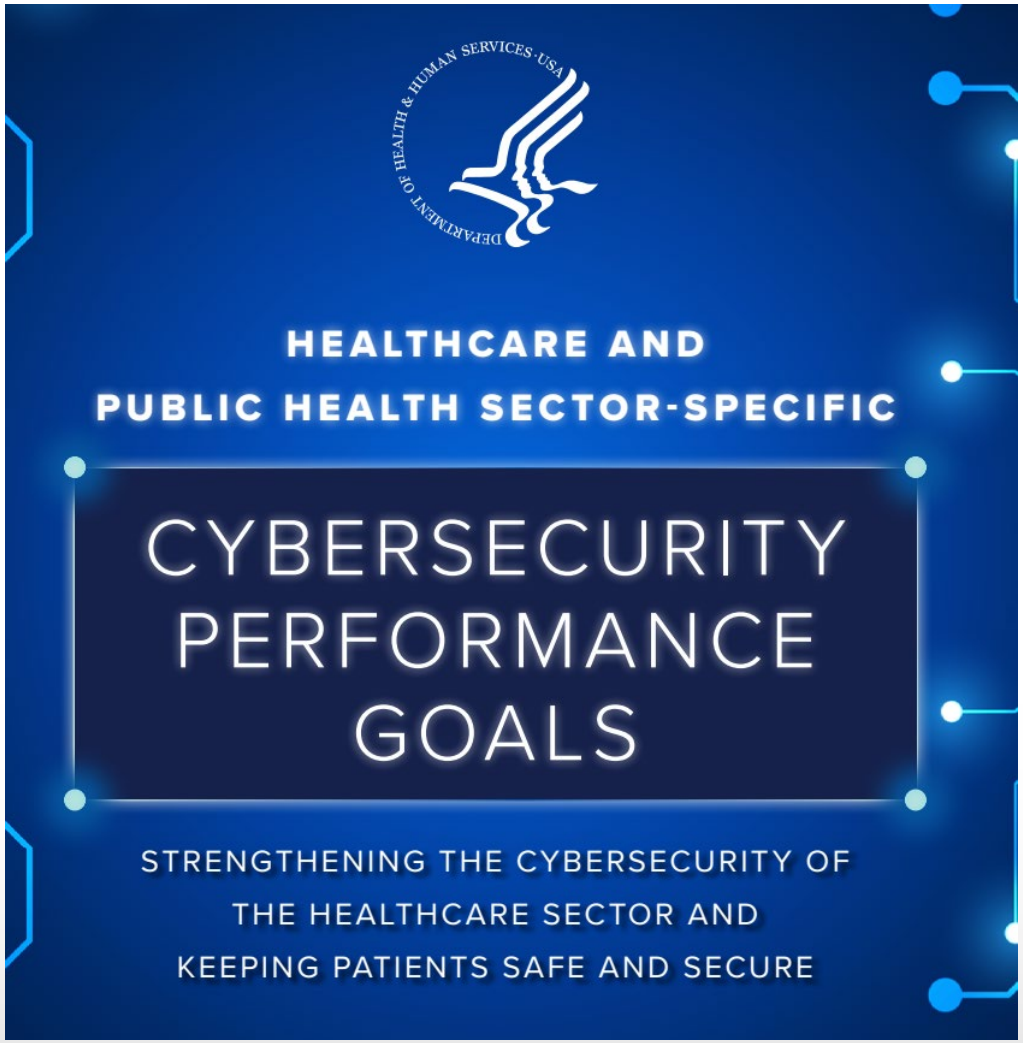
Completion Date: 2Q FY24

Strategic Approaches



- Establish voluntary cybersecurity performance goals for the healthcare sector
- Provide resources to incentivize and implement these cybersecurity practices
- Implement an HHS-wide strategy to support greater enforcement and accountability
- Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity

Tactics



ESSENTIAL GOALS
to help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.

Mapping HPH CPGs to Health Industry Cybersecurity Practices to Facilitate Implementation

- **Mitigate Known Vulnerabilities** 7.M.A, 7.M.B, 2.M.A
- **Email Security** 1.M.A, 1.M.B, 1.M.D
- **Multifactor Authentication** 3.M.A, 3.M.C, 3.M.D
- **Basic Cybersecurity Training** 1.M.D, 10.M.C
- **Strong Encryption** 1.M.C
- **Revoke Credentials** 3.M.B, 3.M.C
- **Basic Incident Planning and Preparedness** 10.M.A, 8.M.B, 4.M.D
- **Unique Credentials** 3.M.A, 3.M.B, 3.M.C, 3.M.D
- **Separating User and Privileged Accounts** 3.M.A, 3.M.B, 3.M.C, 3.M.D
- **Vendor/Supplier Cybersecurity Requirements** 10.M.B

ENHANCED GOALS
to help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

Mapping HPH CPGs to Health Industry Cybersecurity Practices to Facilitate Implementation

- **Asset Inventory** 5.M.A, 5.M.B, 5.M.C, 7.M.C
- **Third Party Vulnerability Disclosure** 10.M.B
- **Third Party Incident Reporting** 10.M.B, 7.M.D, 8.M.C
- **Cybersecurity Testing** 7.L.A, 7.L.C, 8.M.C
- **Cybersecurity Mitigation** 8.M.C, 7.M.D, 7.L.B
- **How to Respond to Relevant Threats** 2.L.C
- **Network Segmentation** 6.M.B
- **Centralized Log Collection** 8.M.A, 8.M.B
- **Centralized Incident Planning and Preparedness** 8.M.A, 8.M.B
- **Configuration Management** 7.M.D

Quarles

Strategy and Tactics

Principle 1: Take Ownership of Customer Security Outcomes

Principle 2: Embrace Radical Transparency and Accountability

Principle 3: Build Organizational Structure and Leadership to Achieve These Goals

Quarles

Tactics

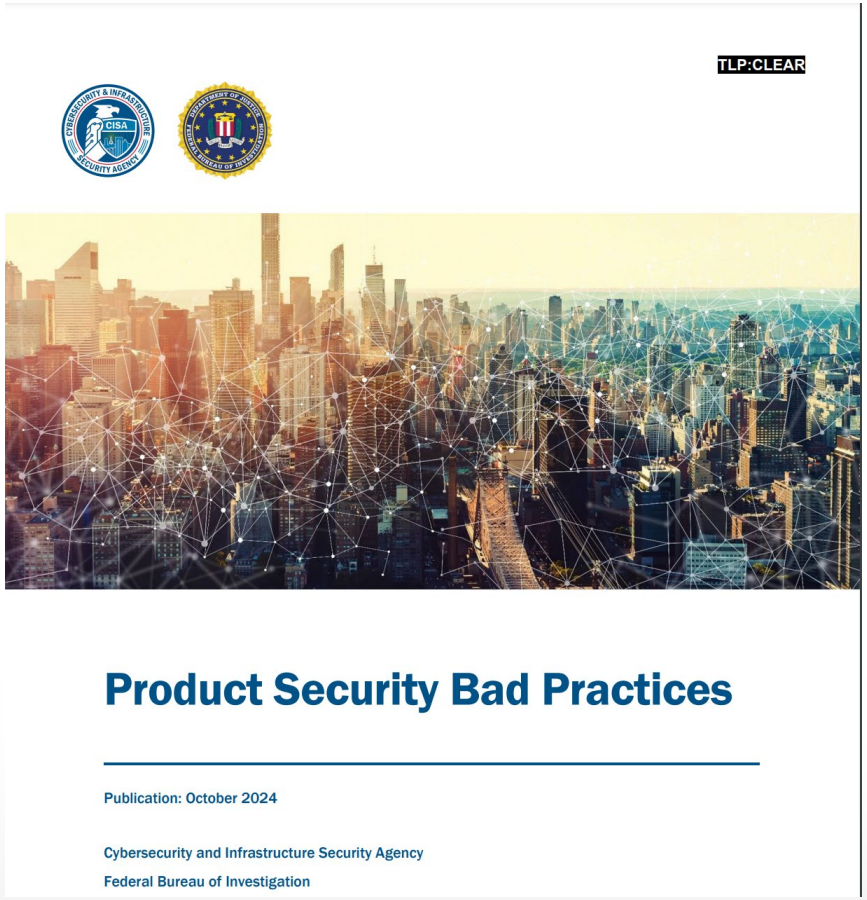


Table of Contents

Quarles

Tactics

ARPA-H announces program to automate cybersecurity for health care facilities

Published May 20, 2024
Proposals Due September 18, 2024

Advanced Research Projects Agency for Health

Investing $50 million to create tools for IT teams to overcome obstacles to current patches of connected devices in hospital environments

Solicitation forthcoming

Tactics

NIST Special Publication 800
NIST SP 800-66r2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2

Quarles

Strategy and Tactics

OFFICE OF SEN. MARK R. WARNER

Cybersecurity is Patient Safety

POLICY OPTIONS IN THE HEALTH CARE SECTOR

Mark R. Warner
US Senator from the Commonwealth of Virginia

NOVEMBER 2022

Policy under Consideration

One proposal under consideration is mandating a regular process to modernize HIPAA regulations to address a broader scope of cybersecurity threats instead of just focusing on covered entities' responsibility to protect a patient's personal health information. Congress could direct HHS to update HIPAA to expand what entities are covered and what actions are permitted.

Policy under Consideration

Given the large number of actors and lack of clearly defined roles, particularly across operational divisions within the Department of Health and Human Services, there is a need for a senior leader at HHS who reports directly to the Secretary of Health and Human Services to lead the Department's work on and be accountable for cybersecurity. The person in this role should be empowered—both operationally and politically—to ensure HHS speaks with one voice regarding cybersecurity in health care, including expectations of external stakeholders and the government's role. This person should also work to effectively partner with other agencies to further these goals and advocate for HHS having the resources it needs to be successful.

MITRE Center for Data-Driven Policy

CYBERSECURITY AND PATIENT SAFETY IN THE HEALTHCARE SETTING

By Meredith Benedict, Penny Chase, and Margie Zuk

The healthcare sector faces a complex set of challenges in its information technology and operational environment, with threats that can impact patient care, business operations, medical devices, facilities, protected health information, and public confidence.[1] Healthcare delivery organizations (HDOs) remain a prime target for cyber attacks. Home and mobile health data collection and exchange increase attack surfaces; a number of steps need to be taken to enable these innovations to scale safely and engender user confidence.

Implementing cyber hygiene practices is a shared responsibility across the federal government and private sector. The technologies that are bringing new innovations to healthcare are rapidly evolving and attackers are becoming more sophisticated. The process for creating cyber hygiene practices needs to be streamlined and agile to adapt to different clinical environments and varying levels of expertise, resources, and computational capabilities. These practices must also be designed to not inadvertently interfere with patient safety.

As a nonprofit operator of federally funded research and development centers focused on both advancing cybersecurity innovation and modernizing healthcare, MITRE brings a unique perspective to this space. MITRE's interdisciplinary approach, informed by our work across federal agencies, helps healthcare stakeholders identify and capture best practices for incorporating cybersecurity into the healthcare setting, fortify their institutions against cyber attacks, and support the development of new cybersecurity policies to address emerging threats.

Initially derived in response to Senator Mark Warner's white paper *Cybersecurity is Patient Safety: Policy Options in the Health Care Sector*,

MAY 2023

MODERNIZING REGULATORY FRAMEWORKS, INCLUDING HIPAA SECURITY[3] AND PRIVACY[4] RULES, TO INCREASE CYBERSECURITY PROTECTIONS

The healthcare ecosystem now extends beyond healthcare providers and their business relationships. The federal government should increase assurance that patients have awareness and agency over data security, risk, and sharing, with the ability to seek redress for the unauthorized use of data.

4. Incorporate in each of the HIPAA Rules that non-covered entities cannot use the term "HIPAA compliant," and reference Federal Trade Commission (FTC) consumer protections against deceptive or misleading claims and marketing.
5. Capture additional data protection specifications for Health Information Technology in the HIPAA Security Rule from the Office of the National Coordinator (ONC) (e.g., data segmentation, data tagging) and require updates to the regulations as specifications change and are adopted.
6. Update HIPAA Rules to clarify that certain healthcare data collected by wearables, health Internet of Things (IoT) devices, and healthcare apps that may currently be deemed "health adjacent data" are protected health information and therefore subject to the HIPAA Rules.
7. Ensure a cohesive, integrated, and adaptable regulatory framework incorporating HIPAA, ONC regulations, FTC rules, and the rules and agreement on Human Subjects Research. This framework and these rules should be amended to:

Quarles

Tactics

OCR Update and 2024 Priorities

Melanie Fontes Rainer, Director
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

HIPAA Summit 41
February 27, 2024

2024 HIPAA Priorities

- Finalizing 2023 Notice of Proposed Rulemaking on the HIPAA Privacy Rule to Support Reproductive Health Care Privacy and Part 2 Rule
- Prioritizing investigations that follow HIPAA complaint and breach trends:
  - Hacking
  - Ransomware
  - *Right of Access Enforcement Initiative*
  - *Risk Analysis Enforcement Initiative*
- Engaging with Health Care Industry on Cybersecurity
  - Increased presence regionally across the country
  - Videos/Guidance/Newsletters
  - Webinars/Technical Assistance
- Review HIPAA Security Rule

Cybersecurity Performance Goals

- In 2023, HHS released voluntary health care specific Cybersecurity Performance Goals (CPGs) to help healthcare organizations implement high-impact cybersecurity practices
- Designed to better protect the healthcare sector from cyberattacks, improve response when events occur, and minimize residual risk.
- Works in tandem with HIPAA Security Rule
- Find the CPGs here: https://hphcyber.hhs.gov/performance-goals.html

Quarles

Tactics

Report on 2016-2017 HIPAA Audits

SUMMARY

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) requires HHS to periodically audit covered entities and business associates for their compliance with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)/HITECH Privacy, Security, and Breach Notification Rules (HIPAA Rules).[1] In 2016 and 2017, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) conducted audits of 166 covered entities and 41 business associates regarding compliance with selected provisions of the HIPAA Rules. Based on its findings, OCR concluded that most covered entities met the timeliness requirements for providing breach notification to individuals, and most covered entities (that maintained a website about their customer services or benefits) also satisfied the requirement to prominently post their Notice of Privacy Practices (NPP) on their website. However, OCR also found that most covered entities failed to meet the requirements for other selected provisions in the audit, such as adequately safeguarding protected health information (PHI), ensuring the individual right of access, and providing appropriate content in their NPP. OCR also found that most covered entities and business associates failed to implement the HIPAA Security Rule requirements for risk analysis and risk management.

HHS offers many tools to assist entities in complying with HIPAA. For example, entities can consult the recently updated HHS Security Risk Assessment Tool and OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule for help in evaluating whether they have a compliant risk analysis and risk management process. An entity can use one of OCR's model notices of privacy practices, as a template, to ensure it includes all of the HIPAA required statements in its NPP. Additionally, OCR's access guidance clarifies how covered entities can improve patients' access to their health information by implementing improved policies and procedures and digital technologies. This report includes links to HHS guidance and other resources offered to covered entities and business associates to improve their compliance with the HIPAA Rules.

HHS Civil Rights
@HHSOCR

OCR will be holding a webinar on The HIPAA Security Rule Risk Analysis Requirement. The webinar will be on October 31st at 3:00 pm EST. #CybersecurityAwarenessMonth

Please join us and register here: shorturl.at/iEJ38

7:09 AM · Oct 26, 2023 · **309** Views

OCR Update and 2024 Priorities

Melanie Fontes Rainer, Director
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

HIPAA Summit 41
February 27, 2024

OCR HIPAA Risk Analysis Webinar

- Video on the HIPAA Security Rule Risk Analysis requirement.
- Discusses what is required to conduct an accurate and thorough assessment of potential risks and vulnerabilities to ePHI and review common risk analysis deficiencies OCR has identified in investigations.
- Topics covered include:
  - How to prepare for a risk analysis
  - How should ePHI be assessed
  - What does it mean to be accurate and thorough
  - What purpose does a risk analysis serve once completed
  - Examples from OCR investigations
  - Resources

The video may be found on OCR's YouTube channel at:
https://www.youtube.com/watch?v=hxfxhokzKEU

Risk Analysis Initiative

- New Enforcement Initiative
- Focus on compliance with key HIPAA Security Rule requirement
- Most OCR large breach investigations reveal a lack of a compliant risk analysis
- Drive better practices to protect electronic protected health information (ePHI)
- Better overall security of data

Title of the Collection: HIPAA Audit Review Survey.

Type of Collection: Reinstatement, with Change, of a Previously Approved Collection OMB No. 0945-0005: Office for Civil Rights (OCR)—Health Information Privacy Division.

Abstract: This information collection consists of 39 online survey questions that will be sent to 207 covered entities and business associates that participated in the 2016-2017 OCR HIPAA Audits. The survey will gather information relating to the effect of the audits on the audited entities and the entities' opinions about the audit process.

OCR is conducting a review of the 2016-2017 HIPAA Audits to determine its efficacy in assessing the HIPAA compliance efforts of covered entities. (🗋 print page 9858) As part of that review, the online survey will be used to:

Measure the effect of the 2016-2017 HIPAA Audits on covered entities' and business associates' subsequent actions to comply with the HIPAA Rules.

Provide entities with an opportunity to give feedback on the Audit and its features, such as the helpfulness of HHS' guidance materials and communications, the utility of the online submission portal, whether the Audit helped improve entity compliance, and the entities' responses to the Audit-report findings and recommendations.

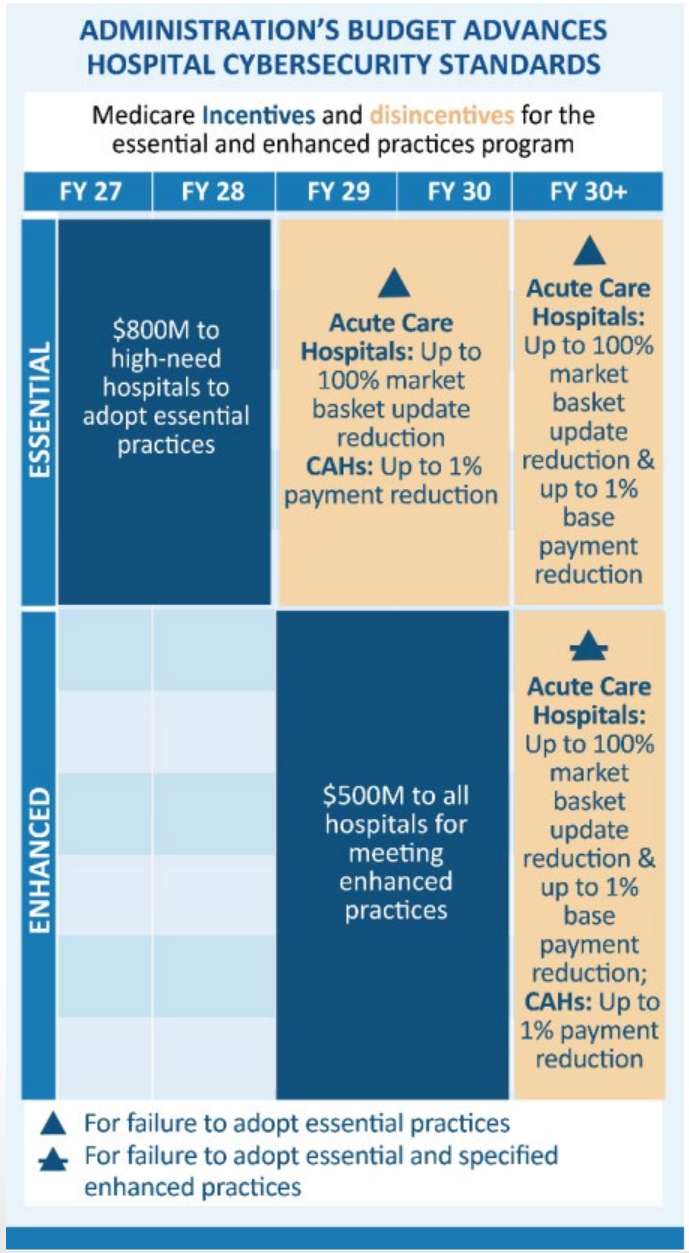
Provide OCR with information on the burden imposed on entities to collect audit-related documents and to respond to audit-related requests; and

Seek feedback on the effect of the HIPAA Audit program on the entities' day-to-day business operations.

The information, opinions, and comments collected using the online survey will be used to improve future OCR HIPAA Audits.

Quarles

Tactics



Quarles

Laws and Regulations

Healthcare Cybersecurity Act of 2024 (July)

118TH CONGRESS
2D SESSION

S. 4697

To enhance the cybersecurity of the Healthcare and Public Health Sector.

IN THE SENATE OF THE UNITED STATES

JULY 11 (legislative day, JULY 10), 2024

Ms. ROSEN (for herself, Mr. YOUNG, and Mr. KING) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To enhance the cybersecurity of the Healthcare and Public Health Sector.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Healthcare Cybersecurity Act of 2024".

SEC. 2. DEFINITIONS.

In this Act—

(1) the term "Agency" means the Cybersecurity and Infrastructure Security Agency;

118TH CONGRESS
2D SESSION

H. R. 9412

To enhance the cybersecurity of the Healthcare and Public Health Sector.

IN THE HOUSE OF REPRESENTATIVES

AUGUST 27, 2024

Mr. CROW (for himself, Mr. FITZPATRICK, Mr. KIM of New Jersey, and Ms. SALAZAR) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To enhance the cybersecurity of the Healthcare and Public Health Sector.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Healthcare Cybersecurity Act of 2024".

SEC. 2. DEFINITIONS.

In this Act—

(1) the term "Agency" means the Cybersecurity and Infrastructure Security Agency;

Health Infrastructure Security and Accountability Act of 2024 (September)

118TH CONGRESS
2D SESSION

S. 5218

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 25, 2024

Mr. WYDEN (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Finance

A BILL

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Health Infrastructure Security and Accountability Act of 2024".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Quarles

Pixels and other Tracking Technologies

Quarles

Common Tracking Technologies

Source: https://en.wikipedia.org/wiki/File:LinkedIn_2021.svg

Source: https://en.m.wikipedia.org/wiki/File:Meta_Platforms_Inc._logo.svg

Source: https://en.wikipedia.org/wiki/Matomo_(software)

Source: https://developers.google.com/analytics/terms/branding-policy

Source: https://newrelic.com/about/media-assets

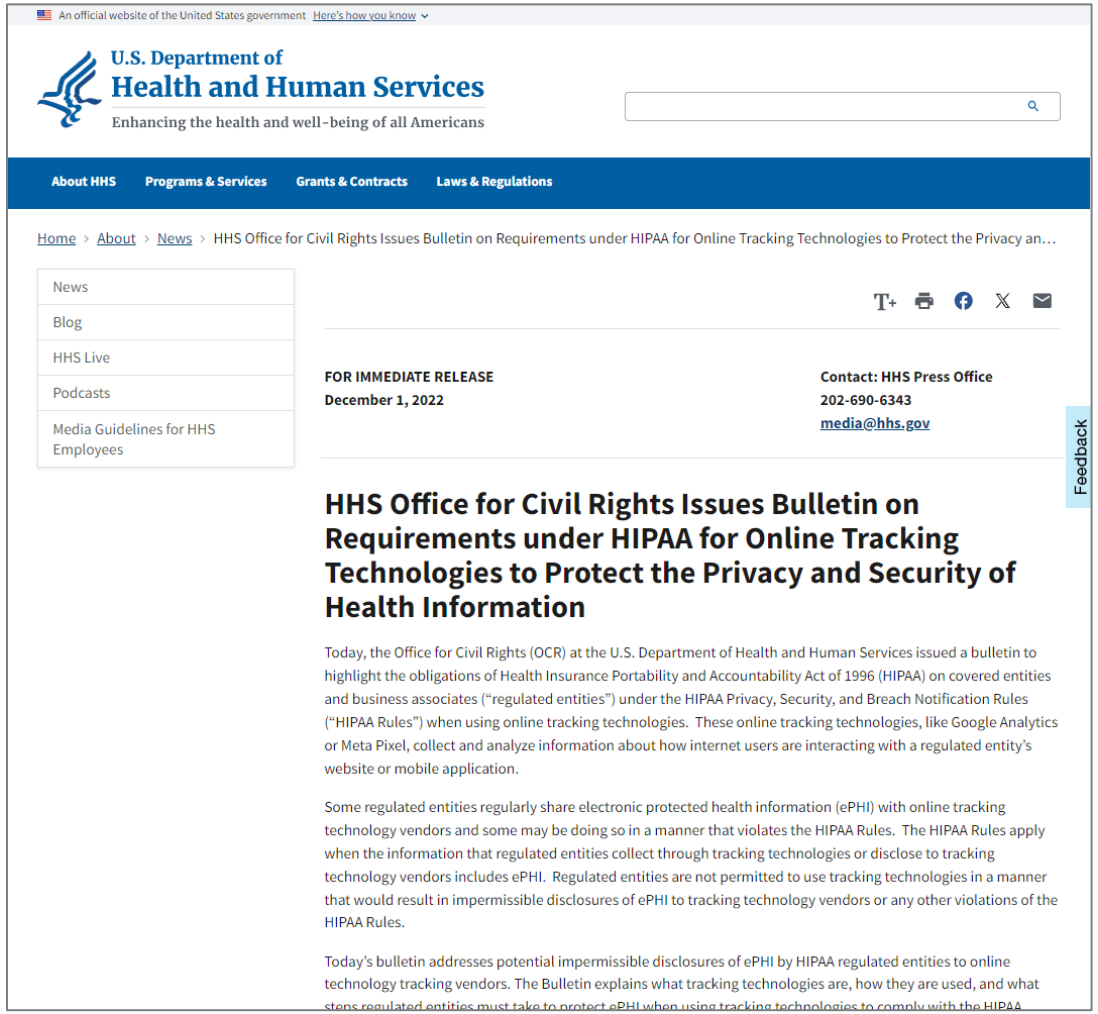
Source: https://www.heap.io/press

Source: https://en.wikipedia.org/wiki/File:Adobe_Corporate_logo.svg

Proliferation of Pixels & Related Technologies

- Lack of Data Portability
- Plug ‘n Play Model
- Free

Evolution of Interest in Pixels



An official website of the United States government Here's how you know

U.S. Department of Health and Human Services
Enhancing the health and well-being of all Americans

About HHS | Programs & Services | Grants & Contracts | Laws & Regulations

Home › About › News › HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy an…

News
Blog
HHS Live
Podcasts
Media Guidelines for HHS Employees

FOR IMMEDIATE RELEASE
December 1, 2022

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Feedback

HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information

Today, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services issued a bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) on covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies. These online tracking technologies, like Google Analytics or Meta Pixel, collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application.

Some regulated entities regularly share electronic protected health information (ePHI) with online tracking technology vendors and some may be doing so in a manner that violates the HIPAA Rules. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes ePHI. Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of ePHI to tracking technology vendors or any other violations of the HIPAA Rules.

Today's bulletin addresses potential impermissible disclosures of ePHI by HIPAA regulated entities to online technology tracking vendors. The Bulletin explains what tracking technologies are, how they are used, and what steps regulated entities must take to protect ePHI when using tracking technologies to comply with the HIPAA

- In 2022, OCR HHS released "The Bulletin" that set guidelines for "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates."
- The Bulletin spurred a series of class action lawsuits under a variety of state and federal laws and legal theories.

Legal & Regulatory Landscape

- State Privacy Laws
- Wiretapping Laws
- Video Privacy Protection Act (VPPA)
- HIPAA

OCR Bulletin and Litigation

FOR IMMEDIATE RELEASE
December 1, 2022

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information

Today, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services issued a bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) on covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies. These online tracking technologies, like Google Analytics or Meta Pixel, collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application.

Some regulated entities regularly sha
technology vendors and some may b
when the information that regulated
vendors includes ePHI. Regulated en
result in impermissible disclosures of

Today's bulletin addresses potential
technology tracking vendors. The Bu
steps regulated entities must take to
Specifically, the Bulletin provides ins

- Tracking on webpages
- Tracking within mobile apps
- HIPAA compliance obligations for

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

[1] *See, e.g.*, Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.
[2] *See, e.g.*, Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.
[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.
[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

INTRODUCTION AND SUMM

1. The American Hospital Association and th
(Associations), along with Texas Health Resources and Unite
(Hospitals), bring this action because the federal government
hospitals and health systems a new rule that is flawed as a matt
administrative process, and harmful as a matter of policy. Th
Department of Health and Human Services (HHS), prohibits th
make healthcare providers' public webpages more effective in s
community. Yet even as HHS is actively enforcing this new
country, the federal government's own healthcare providers c
prohibited technologies on their websites. A gross overreach by
without any input from the public or the healthcare providers m
exceeds the government's statutory and constitutional authority
for agency rulemaking, and harms the very people it purports to
rule's enforcement.

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

AMERICAN HOSPITAL ASSOCIATION, ET AL.,

Plaintiffs,

v. **No. 4:23-cv-01110-P**

XAVIER BECERRA, ET AL.,

Defendants.

OPINION & ORDER

Before the Court are cross-motions for summary judgment. ECF Nos. 24, 50. Having considered the motions, briefs, and applicable law, the Court **GRANTS in part** and **DENIES in part** Plaintiffs' motion (ECF No. 24) and **DENIES** Defendants' motion (ECF No. 50).

BACKGROUND

Congress passed the Health Insurance Port
Accountability Act ("HIPAA") in 1996 because health
needed more protections and the world needed more acron
seeks to "assure that individuals' health information
protected" while "allowing the flow of health informatic
provide and promote high quality healthcare." The De
Health and Human Services ("HHS") enforces this mandat
are reported to HHS's Office for Civil Rights ("OCR"), who
reports and recommends corrective action. This case invol
confidentiality protections (the "Privacy Rule") for "prot
information" ("PHI"). More specifically, the case concern
applicability to one subset of PHI: "individually identi
information" ("IIHI"). HIPAA defines IIHI as informat
"relates to" an individual's healthcare and (2) "identifies th
or provides "a reasonable basis to believe that the inform
used to identify the individual."

IN THE UNITED STATES COURT
FOR THE FIFTH CIRCU

AMERICAN HOSPITAL ASS'N, ET AL.,

Plaintiffs-Appellees,

v.

XAVIER BECERRA, SECRETARY, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, ET AL.,

Defendants-Appellants.

Nos. 24-10775

MOTION TO VOLUNTARILY DISMISS APPEAL UNDER FEDERAL RULE OF APPELLATE PROCEDURE 42(b)

Pursuant to Rule 42(b) of the Federal Rules of Appellate Procedure, the federal government hereby respectfully moves to voluntarily dismiss this appeal, with each side to bear their own costs. Counsel for plaintiffs have indicated they consent to this motion.

Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

*On June 20, 2024, the U.S. District Court for the Northern District of Texas issued an order declaring unlawful and vacating a portion of this guidance document. See Am. Hosp. Ass'n v. Becerra, — F. Supp. 3d ----, No. 4:23-cv-1110, 2024 WL 3075865 (N.D. Tex. June 20, 2024). Specifically, the Court vacated the guidance to the extent it provides that HIPAA obligations are triggered in "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a[n] [unauthenticated public webpage] addressing specific health conditions or healthcare providers." Id. at *2. HHS is evaluating its next steps in light of that order.*

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities[1] and business associates[2] ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[3] OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities' noncompliance with the HIPAA Rules. A regulated entity's failure to comply with the HIPAA Rules may result in a civil money penalty.[4]

Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations.[5] The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI).[6] Some regulated entities may share sensitive information with tracking technology vendors and such sharing may involve unauthorized disclosures of PHI with such vendors.[7] **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures[8] of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[9]

Quarles

Lessons Learned from Pixel Investigations

- Remnants or old tracking technologies that may no longer be in use
- Third-party components of your organizations digital footprint that may be leveraging unapproved or privacy risky tracking technologies
- Unmanaged tracking technologies – not managed by centralized tag manager
- Digital Footprint and Tracking Tech minimization
- Misconfigured Cookie and Tracker Consent Management Tools

THANK YOU!

Quarles

Questions & Contacts

Privacy+ Security Forum

Daniel Guggenheim
Partner
Quarles
dan.guggenheim@quarles.com

Heidi Wachs
Managing Director
Stroz Friedberg, an Aon Company
heidi.Wachs@strozfriedberg.com

Rick Fitzgerald
President
Fireside Consulting