HIPAA Security Rule and Cybersecurity

Kim C. Stanger

(4/25)

Holland & Hart

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

Overview

- HIPAA Security Rule
  - Enforcement
  - Requirements
  - Resources
- Proposed Security Rule Changes
- Other Laws
- Cybersecurity Resources

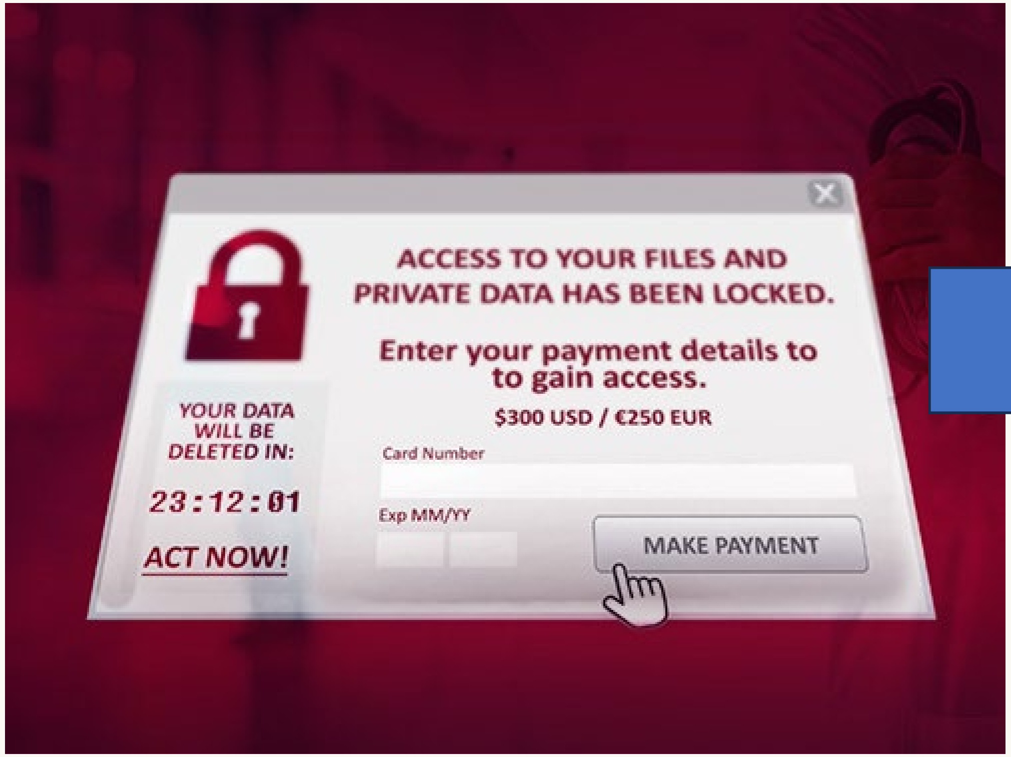
Health Insurance Portability and Accountability Act ("HIPAA")

- Security Rule, 45 CFR 164.301 et seq.
- Breach Notification Rule, 45 CFR 164.401 et seq.
  - Notice to individuals
  - Notice to HHS
  - Notice to local media
- Privacy Rule, 45 CFR 164.501 et seq.
  - Use and disclosure rules
  - Patient rights
  - Administrative requirements

Applies to:

- Covered entities
  - Health care providers who engage in certain electronic standard transactions.
  - Health insurers, including health plans with 50+ participants or that are administered by a third party.
- Business associates

Why you should care



ACCESS TO YOUR FILES AND PRIVATE DATA HAS BEEN LOCKED.

Enter your payment details to to gain access.

$300 USD / €250 EUR

Card Number

Exp MM/YY

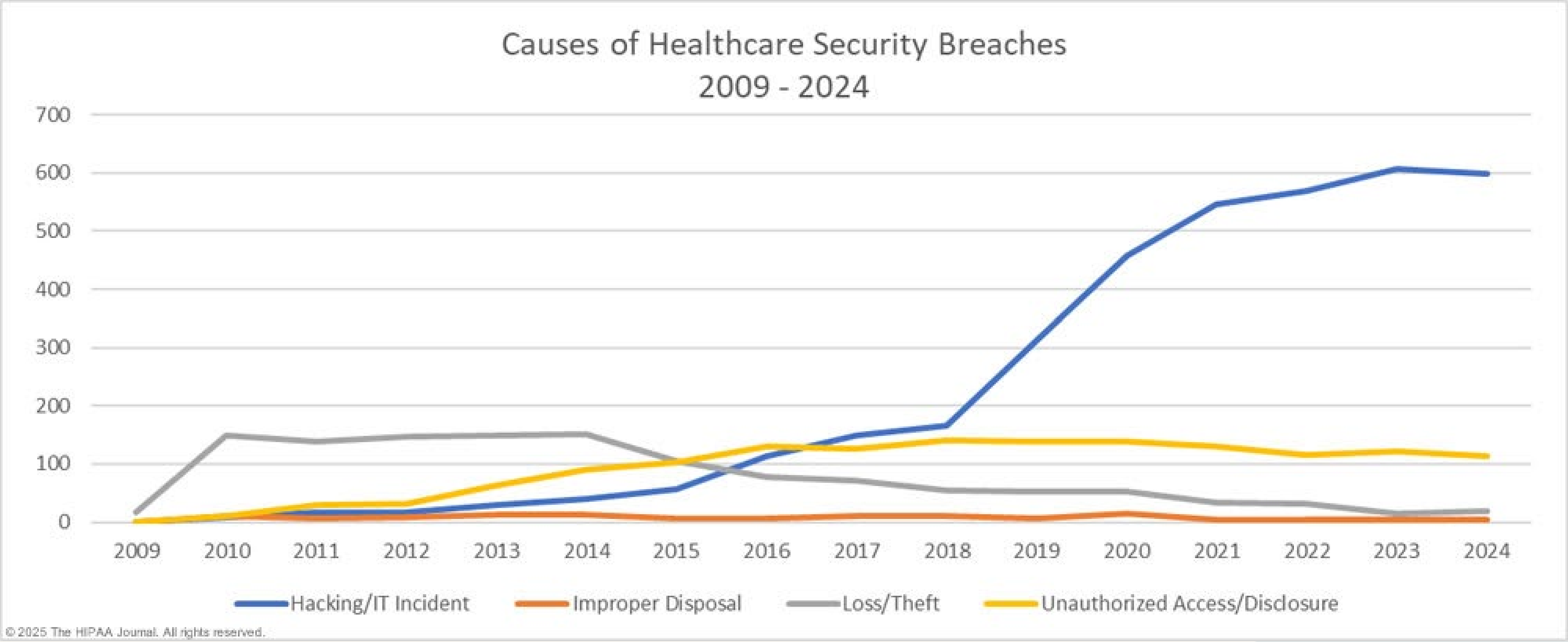
How would this affect--

- Patient care
  - No data on patients
  - Corrupt data on patients
- Bill for or receive payment for services
- Function without data, e.g., payroll, accounting, vendors, etc.
- Damage to IT infrastructure.
- Costs of responding and repairing.
- Potential exposure to regulatory fines and/or lawsuits
- Bad press

Cybersecurity Threats

According to HHS:

- 2018-22: 93% increase in large breaches
- 2018-22: 278% increase in large breaches from ransomware.
- 2023: 77% of large breaches resulted from hacking.
- 2023: Persons affected by large breaches increased 60% to 80,000,000.

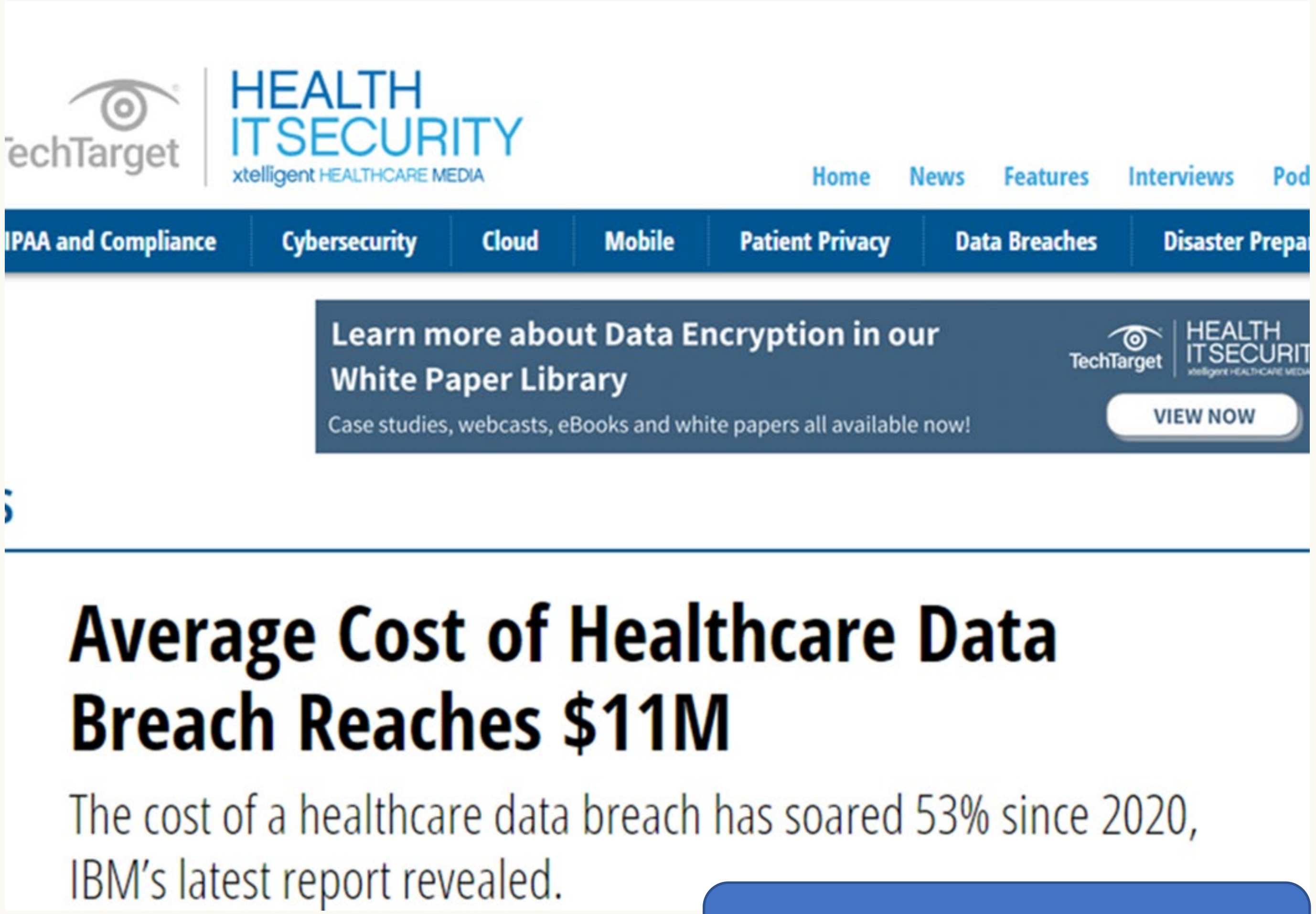


© 2025 The HIPAA Journal. All rights reserved.

Source: The HIPAA Journal
https://www.hipaajournal.com/healthcare-data-breach-statistics/

Holland & Hart

Costs of Data Breach



Learn more about Data Encryption in our White Paper Library

Case studies, webcasts, eBooks and white papers all available now!

Average Cost of Healthcare Data Breach Reaches $11M

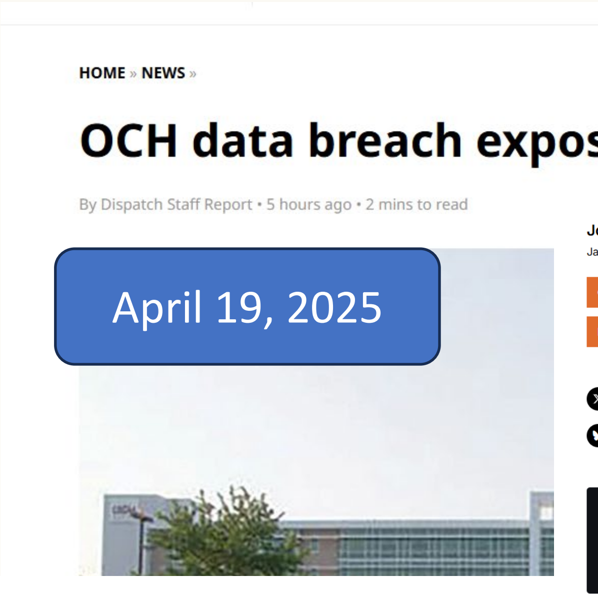
The cost of a healthcare data breach has soared 53% since 2020, IBM's latest report revealed.

Ponemon Institute (2024)

- Costs from:
  - Detection
  - Notification
  - Post-breach response
  - Lost business costs
- Highest cost across all industries.
- Ransomware cost average of $5,130,000.
- Average of 277 days from detection to containment.

Holland & Hart

Ransomware and other cyberthreats are pervasive

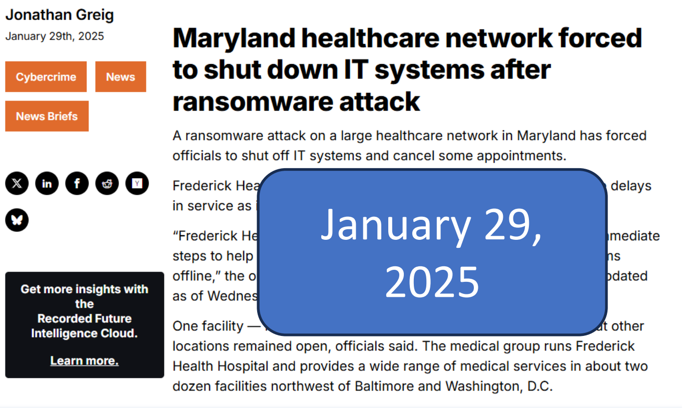


HOME » NEWS »

OCH data breach exposed 67K patient files

By Dispatch Staff Report • 5 hours ago • 2 mins to read

April 19, 2025



Jonathan Greig
January 29th, 2025

Maryland healthcare network forced to shut down IT systems after ransomware attack

A ransomware attack on a large healthcare network in Maryland has forced officials to shut off IT systems and cancel some appointments.

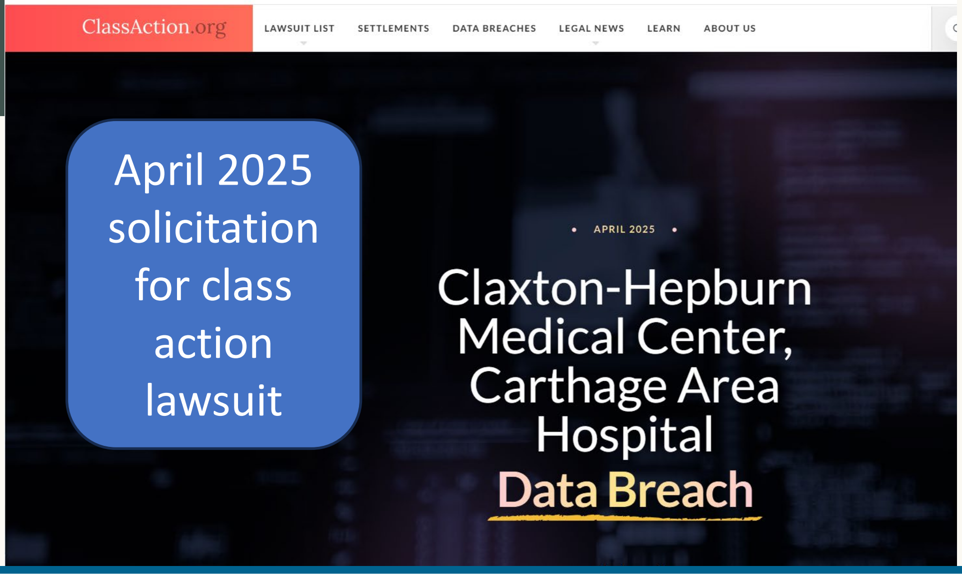
Frederick Hea … delays in service as …

"Frederick He … mediate steps to help … ns offline," the o … pdated as of Wednes…

One facility — … t other locations remained open, officials said. The medical group runs Frederick Health Hospital and provides a wide range of medical services in about two dozen facilities northwest of Baltimore and Washington, D.C.

Get more insights with the Recorded Future Intelligence Cloud.
Learn more.

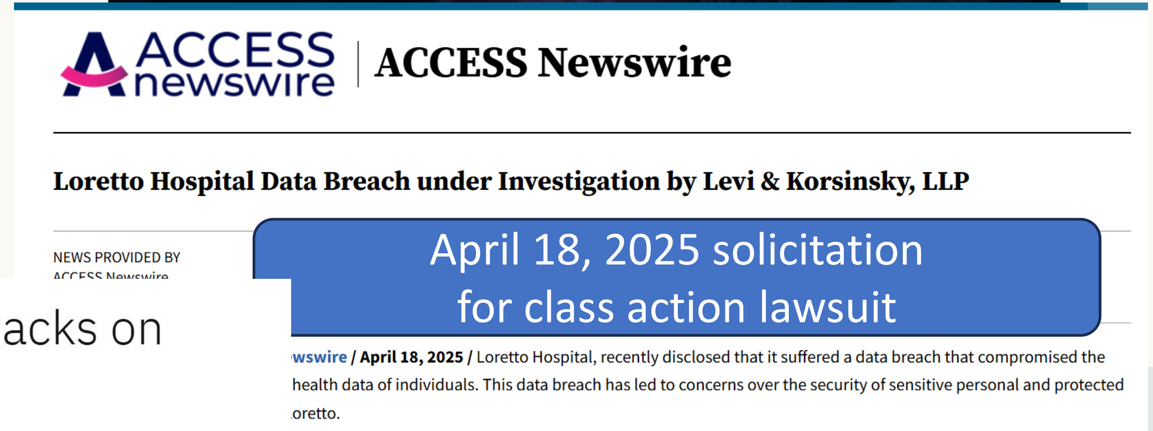
January 29, 2025



APRIL 2025

Claxton-Hepburn Medical Center, Carthage Area Hospital Data Breach

April 2025 solicitation for class action lawsuit



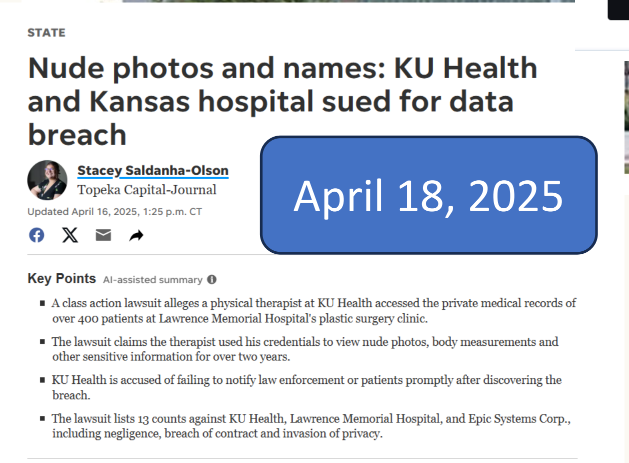
ACCESS newswire | ACCESS Newswire

Loretto Hospital Data Breach under Investigation by Levi & Korsinsky, LLP

NEWS PROVIDED BY
ACCESS Newswire

…wswire / April 18, 2025 / Loretto Hospital, recently disclosed that it suffered a data breach that compromised the health data of individuals. This data breach has led to concerns over the security of sensitive personal and protected … oretto.

April 18, 2025 solicitation for class action lawsuit



STATE

Nude photos and names: KU Health and Kansas hospital sued for data breach

Stacey Saldanha-Olson
Topeka Capital-Journal

Updated April 16, 2025, 1:25 p.m. CT

Key Points AI-assisted summary

- A class action lawsuit alleges a physical therapist at KU Health accessed the private medical records of over 400 patients at Lawrence Memorial Hospital's plastic surgery clinic.
- The lawsuit claims the therapist used his credentials to view nude photos, body measurements and other sensitive information for over two years.
- KU Health is accused of failing to notify law enforcement or patients promptly after discovering the breach.
- The lawsuit lists 13 counts against KU Health, Lawrence Memorial Hospital, and Epic Systems Corp., including negligence, breach of contract and invasion of privacy.

April 18, 2025

When ransomware kills: Attacks on healthcare facilities

Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	• $141* to $71,162* per violation • Up to $2,067,813* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Violation due to reasonable cause	• $1,379* to $71,162* per violation • Up to $2,067,813* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	• $14,232* to $71,162* per violation • Up to $2,067,813* per type per year • Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	• $71,162 to $2,134,831* per violation • Up to $2,134,831* per type per year • Penalty is mandatory

(45 CFR 102.3, 160.404; 85 FR 2879)

Recent HIPAA Resolutions

https://www.hhs.gov/hipaa/newsroom/index.html

Security Rule breaches make up majority of HIPAA settlements and have highest dollar values

Date	Conduct	Resolution
4/17/25	Hospital hit with ransomware attack + improper access.	$25,000
4/4/25	Radiology group data subject to unauthorized access.	$350,000
3/21/25	Business associate's PHI exposed to webcrawlers on internet.	$227,816
2/20/25	Eyeglasses company hacked.	$1,500,000
1/15/25	Neurosurgery group hit with ransomware attack.	$10,000
1/14/25	Medical supply company data breached following phishing scheme.	$3,000,000
1/8/25	Business associate's PHI deleted by unauthorized third party.	$337,750
1/7/25	Business associate hit with ransomware attack.	$80,000
12/10/24	Health care clearinghouse data available through Google search.	$250,000
10/31/24	Ambulance services hit with ransomware attack.	$90,000
10/31/24	Plastic surgeons hit with ransomware attack.	$500,000
10/17/24	Dentist office failed to provide timely access to records.	$70,000
10/3/24	Hospital hit with ransomware attack.	$240,000
9/26/24	Eye and Skin Center hit with ransomware attack	$250,000
8/1/24	EMS provider failed to provide timely access to records.	$115,200

HIPAA Enforcement

- Must self-report breaches of unsecured protected health info
  - To affected individuals.
  - To HHS.
  - To media if breach involves > 500 persons.
- In future, individuals may recover portion of penalties or settlement.
  - On 4/6/22, HHS issued notice soliciting input. (87 FR 19833)
- Must sanction employees who violate HIPAA.
- Possible lawsuits by affected individuals or others.
- State attorney general can bring lawsuit.
  - $25,000 fine per violation + fees and costs

HIPAA Security Rule

Holland & Hart

Privacy v. Security Rule

HIPAA PRIVACY RULE

- Applies directly to covered entities.
- Protects privacy of PHI.
- Patient rights.
- Administrative requirements.
- Breach in violation of privacy rule requires notice.

HIPAA SECURITY RULE

- Applies directly to
  - Covered entities, and
  - Business associates.
- Protects electronic PHI ("ePHI"):
  - Confidentiality
  - Integrity
  - Availability

Security Rule

- Conduct risk analysis
- Implement safeguards
  - Administrative
  - Technical
  - Physical
- Execute business associate agreements ("BAAs")
- Implement and maintain policies, procedures and documentation.
- Ensure workforce complies.

(45 CFR 164.301 et seq.)

Intended to protect ePHI:

- Confidentiality
  - It remains confidential.
- Integrity
  - It is accurate and reliable; has not been corrupted.
- Availability
  - Can access and use it if needed.

Risk Analysis

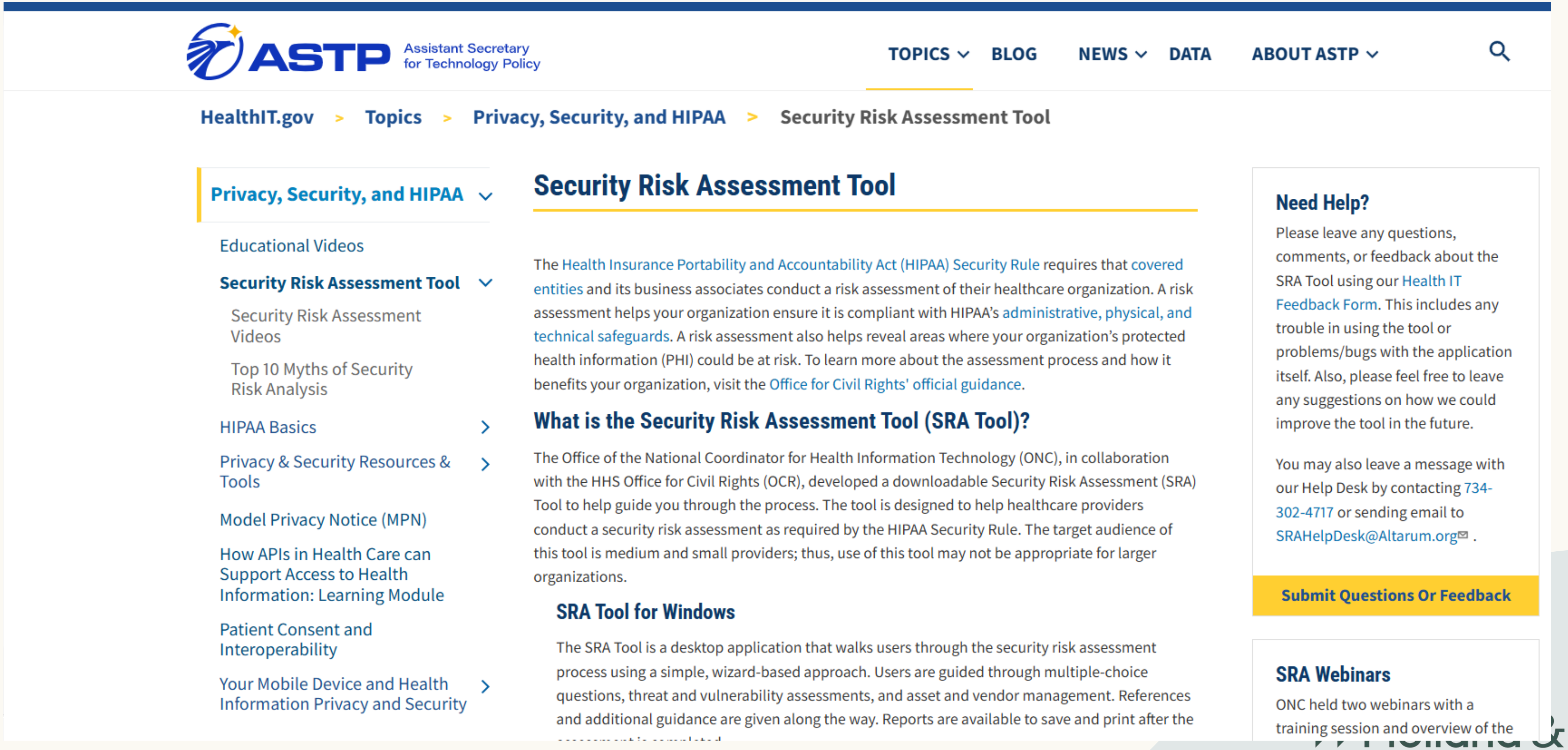
- Must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of [ePHI]..."
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
- Periodically reevaluate analysis.
  - No specific timeline.
  - Consider new systems or equipment and mobile devices.

(45 CFR 164.308(a))

Failure to conduct or follow through with risk analysis is frequently cited by OCR to support penalties for security rule violations.

HHS Risk Assessment Tool

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool


ASTP Assistant Secretary for Technology Policy
TOPICS
BLOG
NEWS
DATA
ABOUT ASTP
HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool
Privacy, Security, and HIPAA
Educational Videos
Security Risk Assessment Tool
Security Risk Assessment Videos
Top 10 Myths of Security Risk Analysis
HIPAA Basics
Privacy & Security Resources & Tools
Model Privacy Notice (MPN)
How APIs in Health Care can Support Access to Health Information: Learning Module
Patient Consent and Interoperability
Your Mobile Device and Health Information Privacy and Security

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the Office for Civil Rights' official guidance.

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

Need Help?

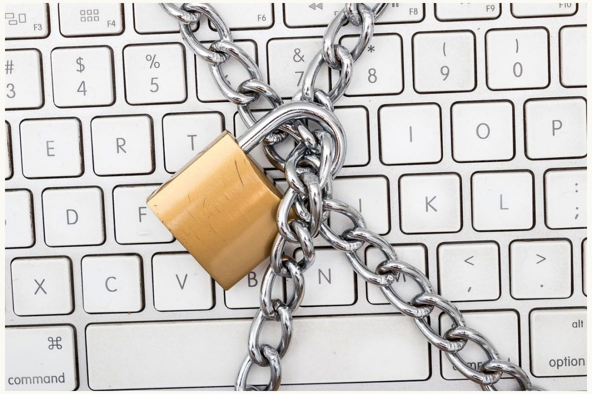
Please leave any questions, comments, or feedback about the SRA Tool using our Health IT Feedback Form. This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.

You may also leave a message with our Help Desk by contacting 734-302-4717 or sending email to SRAHelpDesk@Altarum.org .

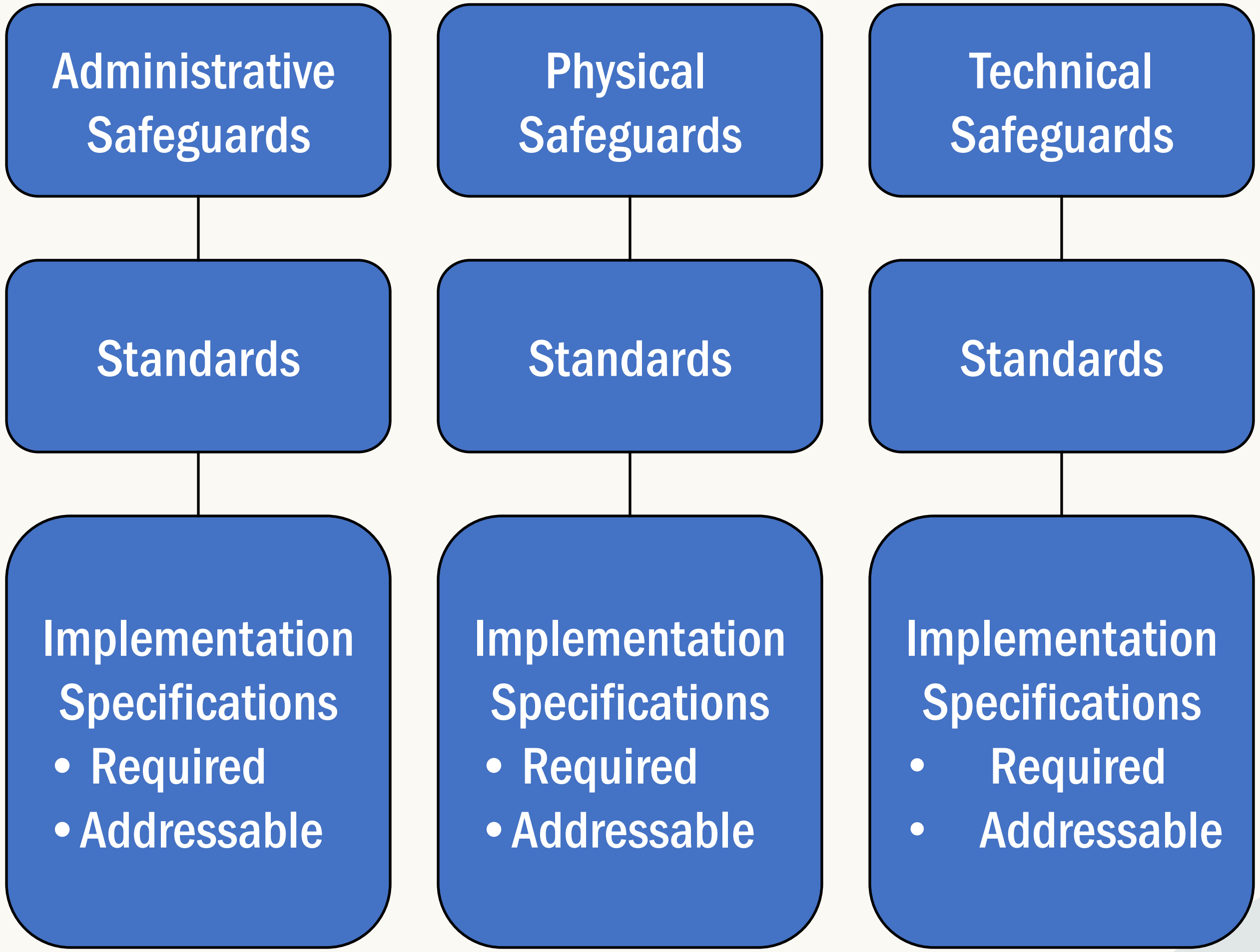
SRA Webinars

ONC held two webinars with a training session and overview of the

Safeguards



- Not technologically specific.
- Depends on--
  - Size, complexity and capabilities of entity.
  - Costs.
  - Probability and criticality of risks to ePHI.



Administrative Safeguards
Physical Safeguards
Technical Safeguards
Standards
Standards
Standards
Implementation Specifications • Required • Addressable
Implementation Specifications • Required • Addressable
Implementation Specifications • Required • Addressable

Implementation Specifications

- "Required": implement the specification.
- "Addressable":
  - Assess reasonableness of specification.
  - If spec is reasonable, implement it.
  - If spec is not reasonable,
    - Document why it is not reasonable (e.g., size, cost, risk factors, etc.), and
    - Implement alternative if reasonable.
- Must review and modify as needed.

Administrative Safeguards

- Security management process.
  - Risk analysis (R)
  - Sanction workforce members for violations (R)
  - Regularly review system activity, e.g., audit logs, access reports, security incident tracking reports (R)
- Assigned security responsibilities to appropriate person.
- Workforce security.
  - Authorize and supervise workforce members who work with ePHI (A)
  - Process to determine if workforce access is appropriate (A)
  - Process to terminate access when it is no longer required (A)

(45 CFR 164.308(a)(1)-(3))

Administrative Safeguards

- Access management.
  - Process to grant access to ePHI through, e.g., workstation, transaction, program, etc. (A)
  - Establish, document, review and modify access as appropriate (A)
- Security awareness and training.
  - Periodic security reminders and updates (A)
  - Guard against, detecting and reporting malicious software (A)
  - Monitor log-in attempts and reporting discrepancies (A)
  - Create, change and safeguard passwords (A)
- Security incident procedures.
  - Identify, respond to, and mitigate suspected or known security incidents and document appropriate response (R)

(45 CFR 164.308(a)(4)-(7))

Administrative Safeguards

- Contingency plan (e.g., for fire, vandalism, system failure, natural disaster, etc.)
  - Data backup plan (R)
  - Disaster recovery plan (R)
  - Emergency mode operation plan (R)
  - Testing and revision of contingency plan (A)
  - Applications and data criticality analysis (A)
- Periodic evaluation of security rule compliance.

(45 CFR 164.308(a)(4)-(7))

Physical Safeguards

- Facility access controls
  - Contingency operations that allow access to ePHI under disaster recovery and emergency mode operations (A)
  - Safeguard against unauthorized access, tampering or theft (A)
  - Control and validate person’s access based on role or function, including visitors (A)
  - Document repairs and modifications to physical structures (e.g., hardware, walls, doors, locks, etc.)
- Workstation security, including safeguard access and restrict to authorized users.

(45 CFR 164.310(a)-(c))

Physical Safeguards

- Device and media controls, including processes re receipt, removal, and movement of hardware and electronic media.
  - Process for final disposition of ePHI or hardware on which it is stored (R)
  - Process for removing ePHI from media prior to re-use (R)
  - Document movement of hardware and electronic medial and persons responsible for same (A)
  - Create retrievable, exact copy of ePHI before movement of equipment.

(45 CFR 164.310(a)-(c))

Technical Safeguards

- Access controls.
  - Assign unique name or number for identifying and tracking users (R)
  - Emergency access procedures (R)
  - Automatic logoff after predetermined time of inactivity (A)
  - Encrypt and decrypt e-PHI (A)
- Audit controls that record and examine activity in info systems.
- Data integrity processes to protect against improper alteration or destruction of ePHI.
  - Electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in unauthorized manner (A)
- User authentication to verify that person seeking access to ePHI is the one authorized.

(45 CFR 164.312(a)-(d))

Technical Safeguards

- Transmission security to guard against unauthorized access to ePHI that is transmitted over electronic communications network.
  - Integrity controls to ensure transmitted ePHI is not pimproperly modified without detection (A)
  - Encrypt ePHI whenever deemed appropriate (A)

(45 CFR 164.312(a)-(d))

Encryption

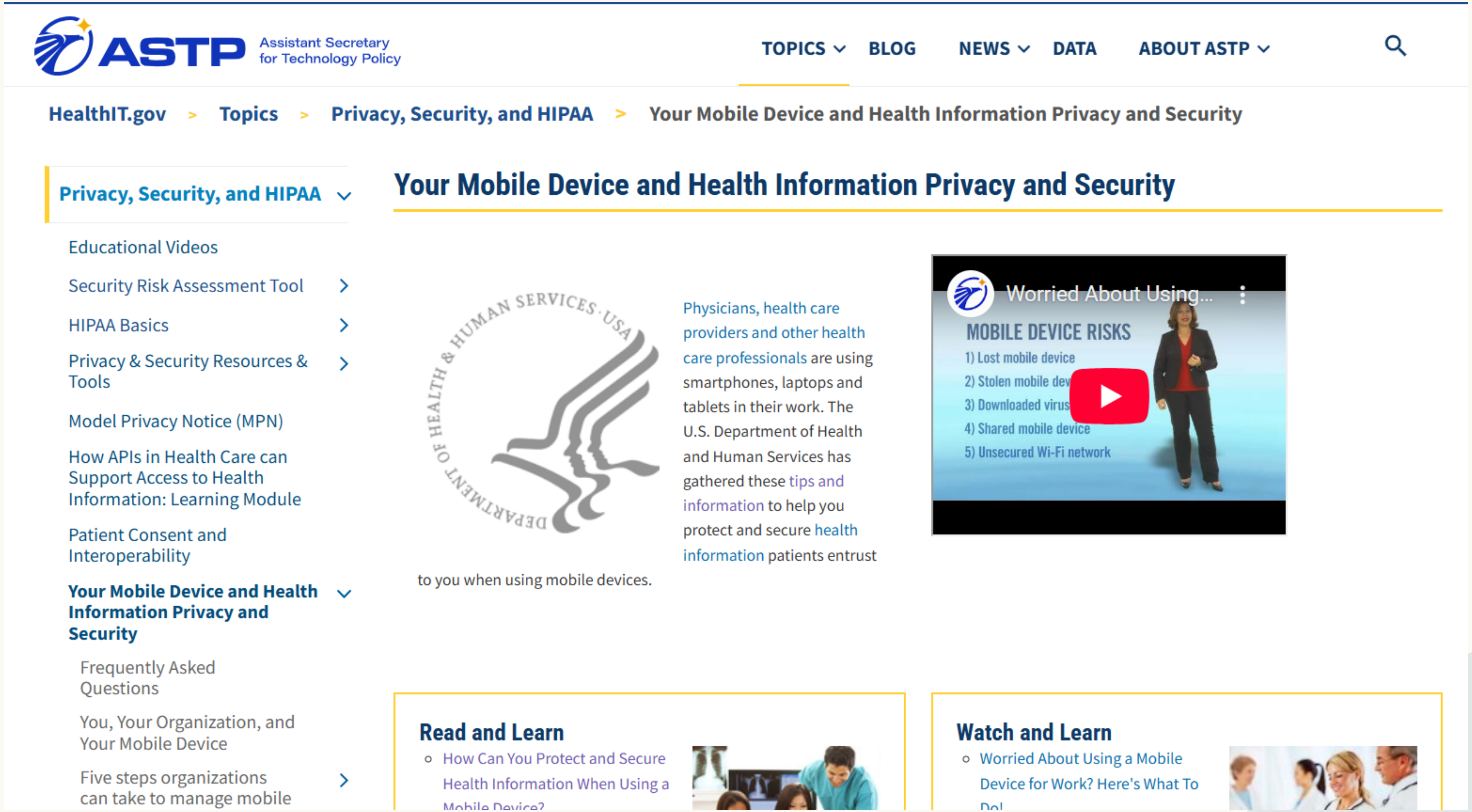
- Encryption is an addressable standard per 45 CFR 164.312:

> (e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.
> (2)(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

- *ePHI that is properly encrypted is "secured".*
  - *Not subject to breach reporting.*
- *OCR presumes that loss of unencrypted laptop, USB, mobile device is breach.*

Beware Mobile Devices

https://www.healthit.gov/topic/privacy-security-and-hipaa/your-mobile-device-and-health-information-privacy-and-security



HealthIT.gov > Topics > Privacy, Security, and HIPAA > Your Mobile Device and Health Information Privacy and Security

Privacy, Security, and HIPAA

- Educational Videos
- Security Risk Assessment Tool
- HIPAA Basics
- Privacy & Security Resources & Tools
- Model Privacy Notice (MPN)
- How APIs in Health Care can Support Access to Health Information: Learning Module
- Patient Consent and Interoperability
- **Your Mobile Device and Health Information Privacy and Security**
  - Frequently Asked Questions
  - You, Your Organization, and Your Mobile Device
  - Five steps organizations can take to manage mobile

Your Mobile Device and Health Information Privacy and Security

Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when using mobile devices.

Worried About Using...

MOBILE DEVICE RISKS

1) Lost mobile device
2) Stolen mobile dev
3) Downloaded virus
4) Shared mobile device
5) Unsecured Wi-Fi network

Read and Learn

- How Can You Protect and Secure Health Information When Using a Mobile Device?

Watch and Learn

- Worried About Using a Mobile Device for Work? Here's What To Do!

Communicating by E-mail or Text

- HIPAA Privacy Rule allows patient to request communications by alternative means or at alternative locations.
  - Including unencrypted e-mail.

(45 CFR 164.522(b))

- Omnibus Rule commentary states that covered entity or business associate may communicate with patient via unsecured e-mail so long as they warn patient of risks and patient elects to communicate via unsecured e-mail to text.

(78 FR 5634)

- Does not apply to disclosures between your employees or providers.

Business Associates

- May disclose PHI to business associates if have valid business associate agreement ("BAA").
  - Covered entity → business associate
  - Business associate → subcontractor business associate

(45 CFR 164.502)

- Failure to execute BAA = HIPAA violation
  - May subject you to HIPAA fines.
    - OCR settlement: gave records to storage company without BAA: $31,000 penalty.
  - Based on OCR settlements, may expose you to liability for business associate's misconduct.
    - Turned over x-rays to vendor; no BAA: $750,000.
    - Theft of business associate's laptop; no BAA: $1,550,000.

Business Associates

BUSINESS ASSOCIATES

- Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity (i.e., you want them to do something with your PHI) :
  - E.g., IT vendor, billing company, consultant, accountant, attorney, data storage vendor, etc.
- Covered entities acting as business associates.
  - E.g., medical directors, consultants, peer reviewers, etc.
- Subcontractors of business associates.

(45 CFR 160.103)

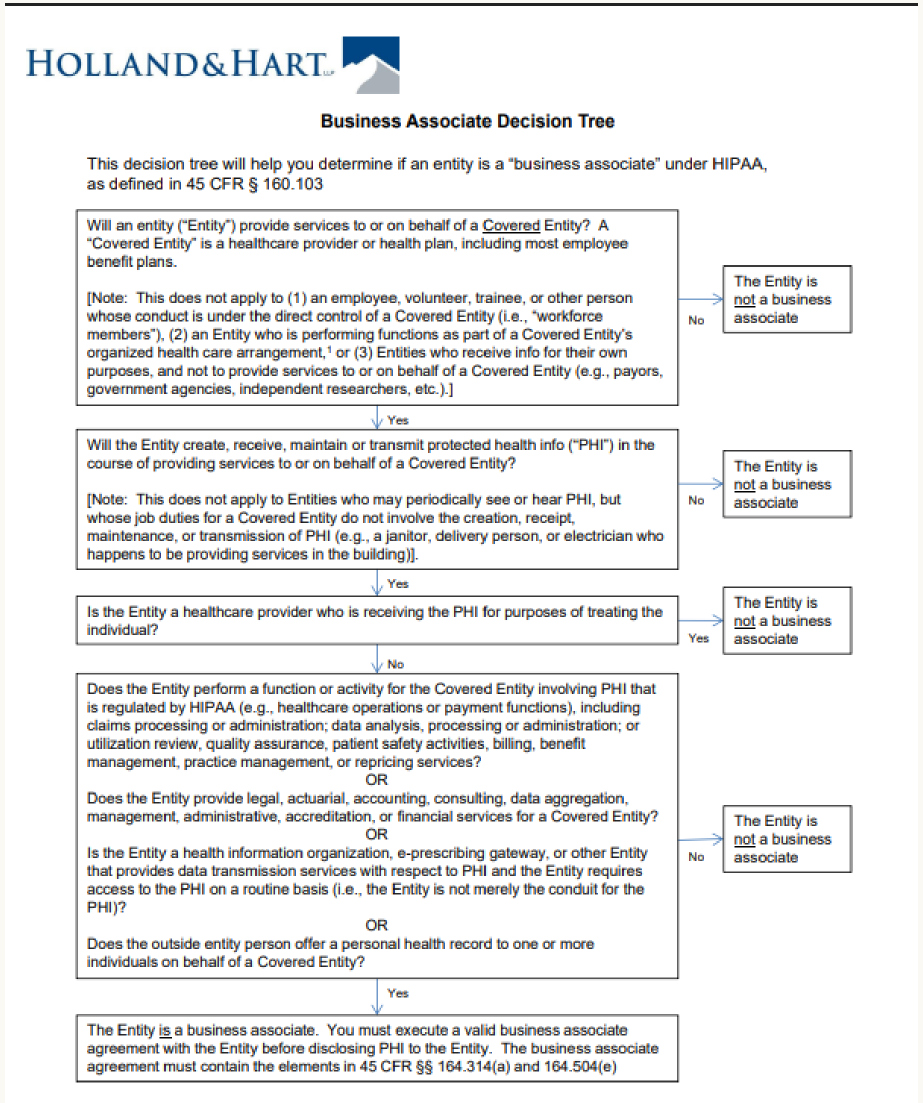
NOT BUSINESS ASSOCIATES

- Members of covered entity's workforce.
- Entities who do not handle PHI as part of their job duties.
  - E.g., janitor, mailman, some vendors, etc.
- Entities that receive PHI to perform functions on their own behalf.
  - E.g., banks, third-party payors, etc.
- Other healthcare providers while providing treatment.
- Data transmission companies that do not routinely access PHI.
  - E.g., entity is mere "conduit" of PHI.
- Members of an organized healthcare arrangement.
- Group of entities that provide coordinated care.

(See https://www.hollandhart.com/avoiding-business-associate-agreements)

Business Associate Decision Tree

https://www.hollandhart.com/pdf/Business_Associate_Decision_Tree.pdf



HOLLAND&HART LLP

Business Associate Decision Tree

This decision tree will help you determine if an entity is a "business associate" under HIPAA, as defined in 45 CFR § 160.103

Will an entity ("Entity") provide services to or on behalf of a Covered Entity? A "Covered Entity" is a healthcare provider or health plan, including most employee benefit plans.

[Note: This does not apply to (1) an employee, volunteer, trainee, or other person whose conduct is under the direct control of a Covered Entity (i.e., "workforce members"), (2) an Entity who is performing functions as part of a Covered Entity's organized health care arrangement,[1] or (3) Entities who receive info for their own purposes, and not to provide services to or on behalf of a Covered Entity (e.g., payors, government agencies, independent researchers, etc.).]

No → The Entity is not a business associate

Yes ↓

Will the Entity create, receive, maintain or transmit protected health info ("PHI") in the course of providing services to or on behalf of a Covered Entity?

[Note: This does not apply to Entities who may periodically see or hear PHI, but whose job duties for a Covered Entity do not involve the creation, receipt, maintenance, or transmission of PHI (e.g., a janitor, delivery person, or electrician who happens to be providing services in the building)].

No → The Entity is not a business associate

Yes ↓

Is the Entity a healthcare provider who is receiving the PHI for purposes of treating the individual?

Yes → The Entity is not a business associate

No ↓

Does the Entity perform a function or activity for the Covered Entity involving PHI that is regulated by HIPAA (e.g., healthcare operations or payment functions), including claims processing or administration; data analysis, processing or administration; or utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing services?

OR

Does the Entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a Covered Entity?

OR

Is the Entity a health information organization, e-prescribing gateway, or other Entity that provides data transmission services with respect to PHI and the Entity requires access to the PHI on a routine basis (i.e., the Entity is not merely the conduit for the PHI)?

OR

Does the outside entity person offer a personal health record to one or more individuals on behalf of a Covered Entity?

No → The Entity is not a business associate

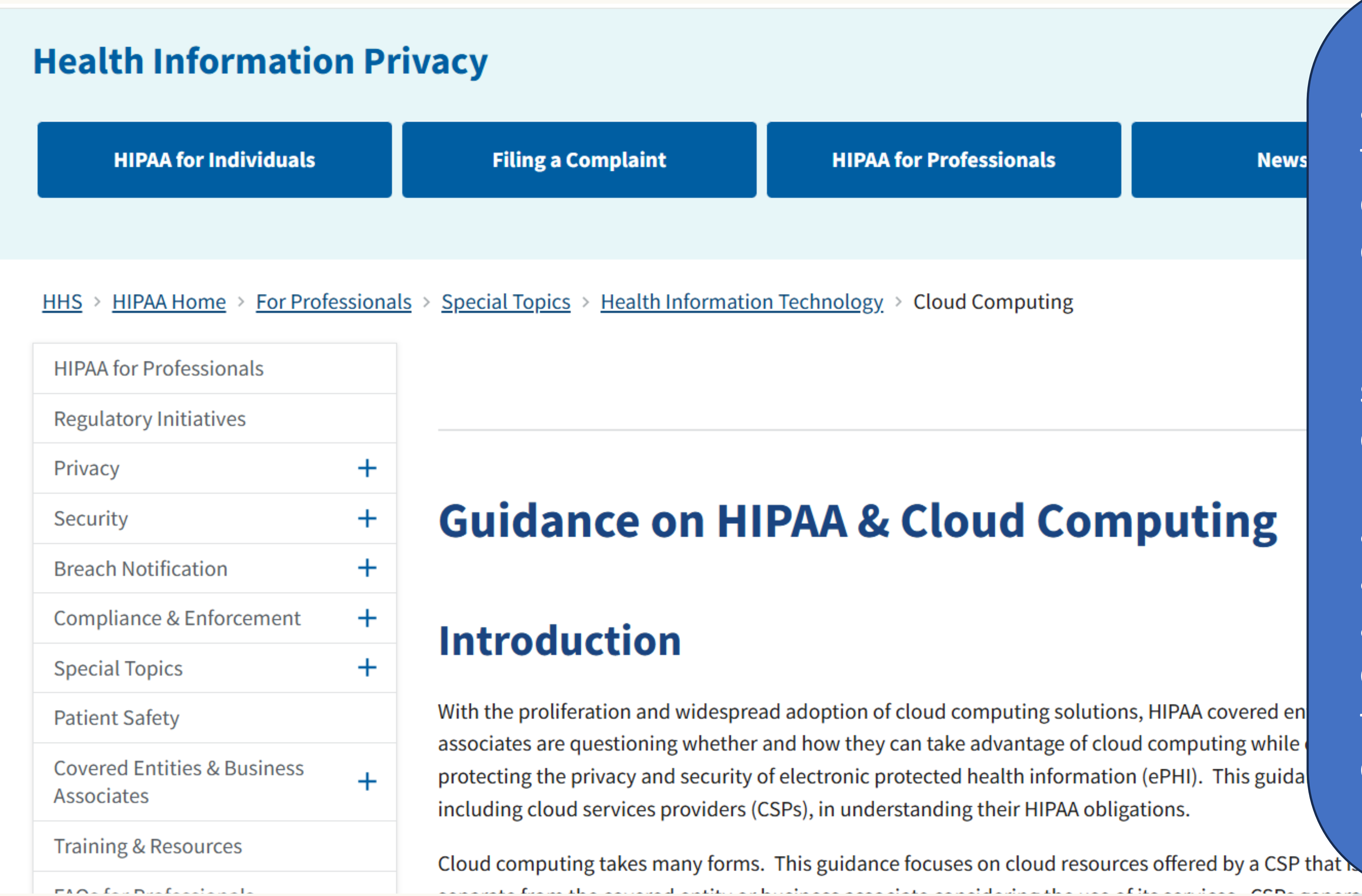
Yes ↓

The Entity is a business associate. You must execute a valid business associate agreement with the Entity before disclosing PHI to the Entity. The business associate agreement must contain the elements in 45 CFR §§ 164.314(a) and 164.504(e)

- See also https://www.hollandhart.com/avoiding-business-associate-agreements

HIPAA and Cloud Computing

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html



Health Information Privacy

HHS › HIPAA Home › For Professionals › Special Topics › Health Information Technology › Cloud Computing

Guidance on HIPAA & Cloud Computing

Introduction

With the proliferation and widespread adoption of cloud computing solutions, HIPAA covered en associates are questioning whether and how they can take advantage of cloud computing while protecting the privacy and security of electronic protected health information (ePHI). This guida including cloud services providers (CSPs), in understanding their HIPAA obligations.

Cloud computing takes many forms. This guidance focuses on cloud resources offered by a CSP that i

"When a covered entity [or business associate] engages the services of a CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate under HIPAA…. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data…. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules."

Business Associate Agreements

- BAAs must contain required terms.
  - Pass limits to business associate and subcontractors
  - Business associate is still subject to HIPAA even if there is no BAA.

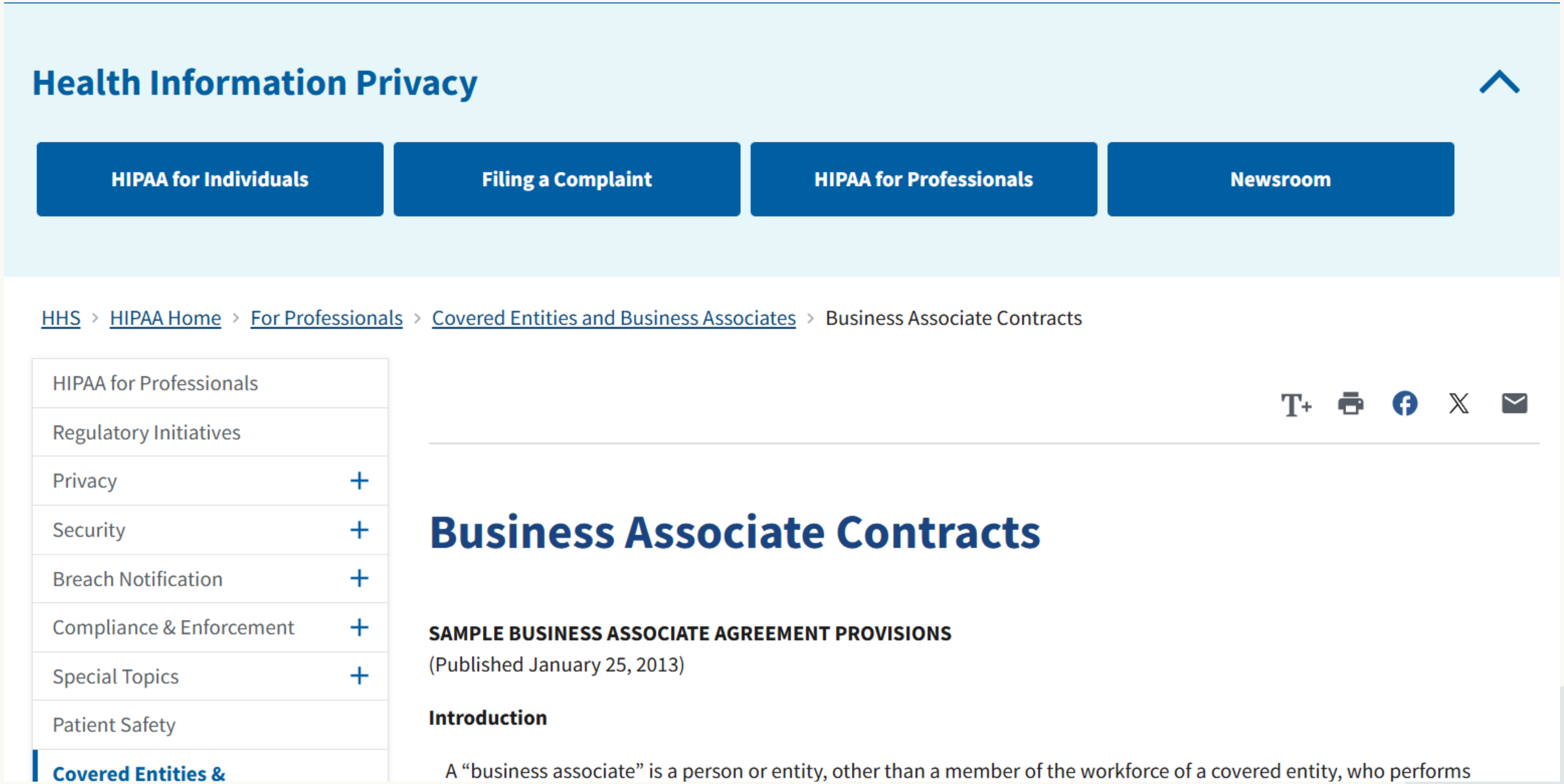
- *Beware business associate's use of PHI for its own purposes, e.g.*
  - *Product development*
  - *Data aggregation, mining, tracking, etc.*

- Establish permitted uses and disclosures.
- Require BA to—
  - Use appropriate safeguards.
  - Comply with security rule.
  - Report improper uses, disclosures or security incidents.
  - Execute subcontractor BAAs
  - Patient access, amendment and accounting of disclosures.
  - Provide access to HHS.
- Return PHI upon termination.

(45 CFR 164.314, -164.502(e) and 164.504(e))

OCR Sample BAA Language

https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html



Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS

(Published January 25, 2013)

Introduction

A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs

Liability for Acts of Business Associate or Subs

- May be liable for business associate's acts if:
  - Know of misconduct and fail to terminate BAA (45 CFR 164.504(e)(1)); or
  - Business associate acts as your agent under federal common law of agency, e.g.,
    - Contract terms and/or
    - Right to control conduct, give directions, control details;

(45 CFR 160.402(c), 164.504(e); 78 FR 5581-82)

To minimize liability:

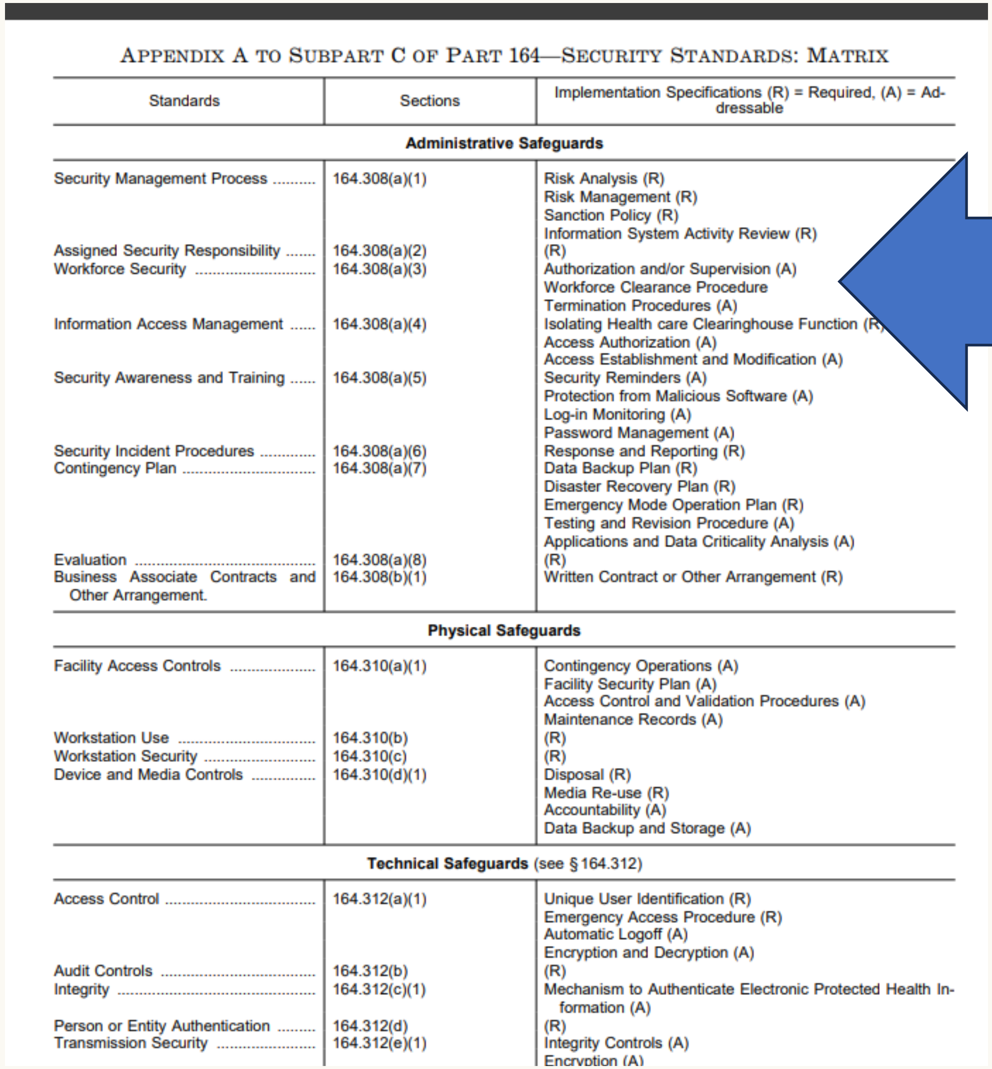
- Have BAA and include appropriate terms, e.g.,
  - Confirm independent contractor status.
  - Cooperate in responding to breach.
  - Pay for cost of mitigation, defense, indemnification, etc.
  - Cyberliability or breach insurance.
- Don't exercise too much control over business associate.
- Respond promptly if you learn of breach or misconduct, including terminating BAA.

Documentation

- Implement written policies and procedures to comply with standards and specs.
- Maintain documentation in written or electronic form.
- Required
  - Maintain documents required by security rule for 6 years from later of creation or last effective date (R)
  - Make documents available to persons responsible for implementing procedures (R)
  - Review and update documentation periodically in response to environmental or operation changes affecting security of ePHI (R)

(45 CFR 164.316)

Security Rule Checklist

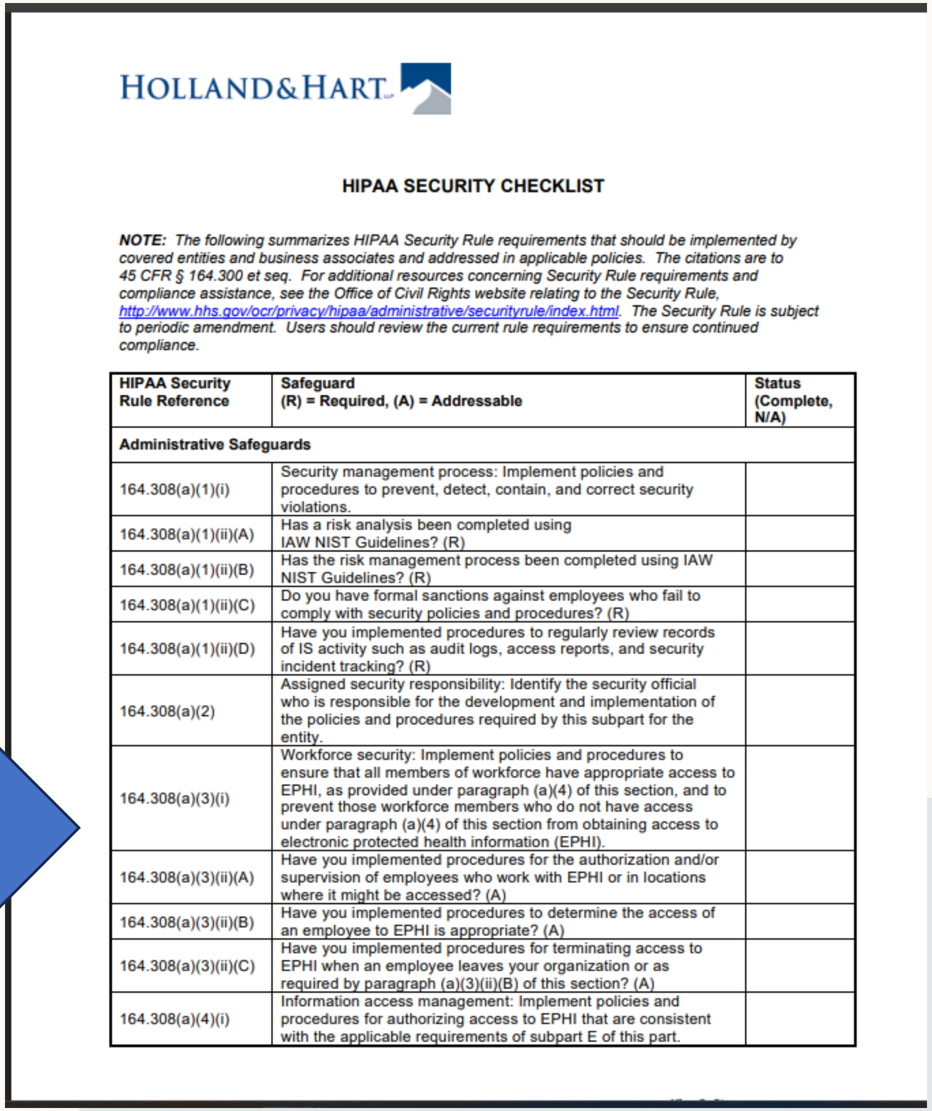


APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

https://www.govinfo.gov/content/pkg/CFR-2024-title45-vol2/pdf/CFR-2024-title45-vol2-part164.pdf

https://www.hollandhart.com/pdf/ HIPAA-Security-Checklist-HH.pdf



HOLLAND&HART.

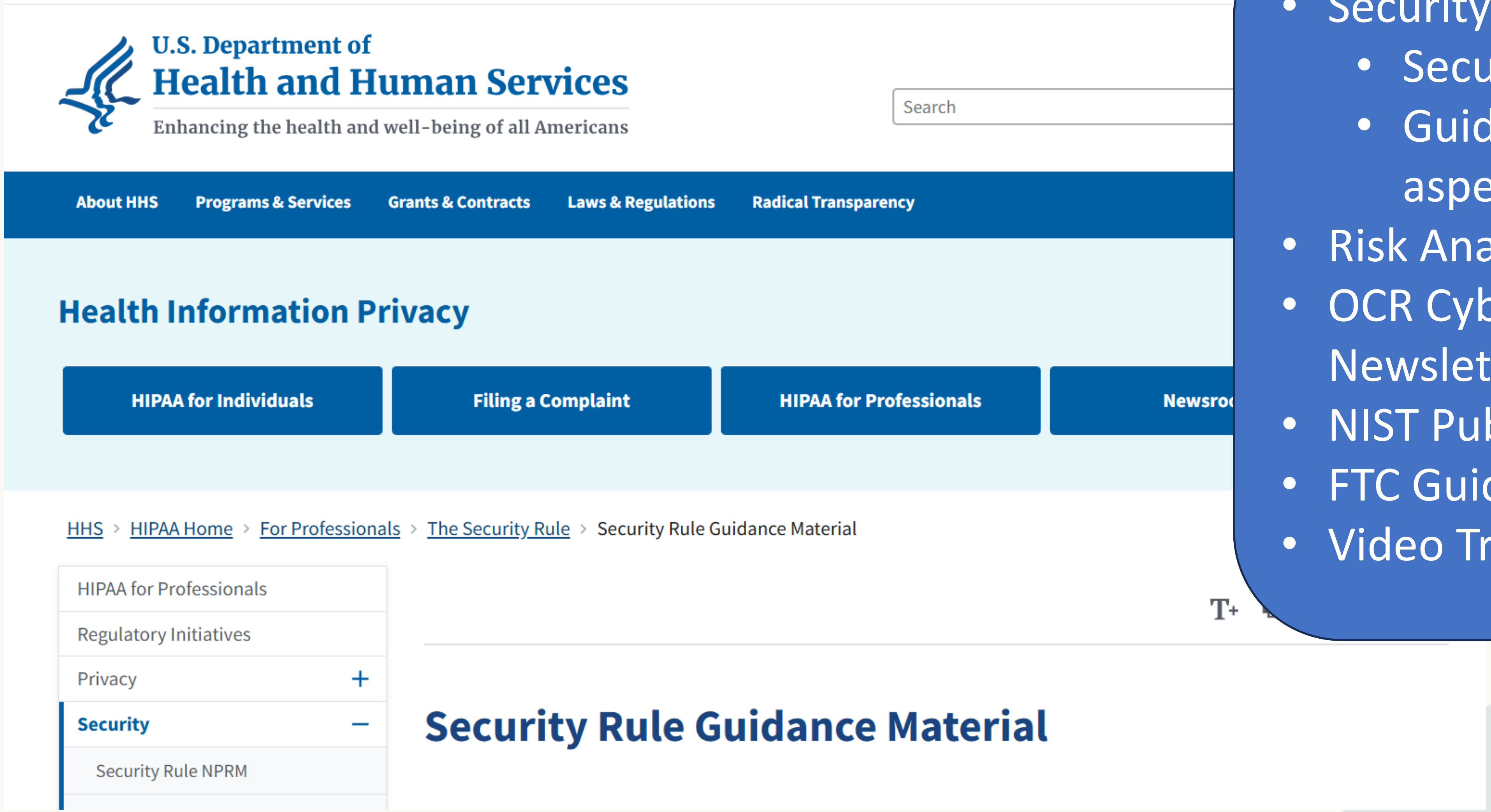
HIPAA SECURITY CHECKLIST

NOTE: *The following summarizes HIPAA Security Rule requirements that should be implemented by covered entities and business associates and addressed in applicable policies. The citations are to 45 CFR § 164.300 et seq. For additional resources concerning Security Rule requirements and compliance assistance, see the Office of Civil Rights website relating to the Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html. The Security Rule is subject to periodic amendment. Users should review the current rule requirements to ensure continued compliance.*

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
Administrative Safeguards		
164.308(a)(1)(i)	Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	
164.308(a)(1)(ii)(A)	Has a risk analysis been completed using IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the risk management process been completed using IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)	
164.308(a)(2)	Assigned security responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	
164.308(a)(3)(i)	Workforce security: Implement policies and procedures to ensure that all members of workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine the access of an employee to EPHI is appropriate? (A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves your organization or as required by paragraph (a)(3)(ii)(B) of this section? (A)	
164.308(a)(4)(i)	Information access management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	

OCR Security Rule Guidance

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html



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

Search

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

Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroo

HHS > HIPAA Home > For Professionals > The Security Rule > Security Rule Guidance Material

- HIPAA for Professionals
- Regulatory Initiatives
- Privacy +
- Security −
  - Security Rule NPRM

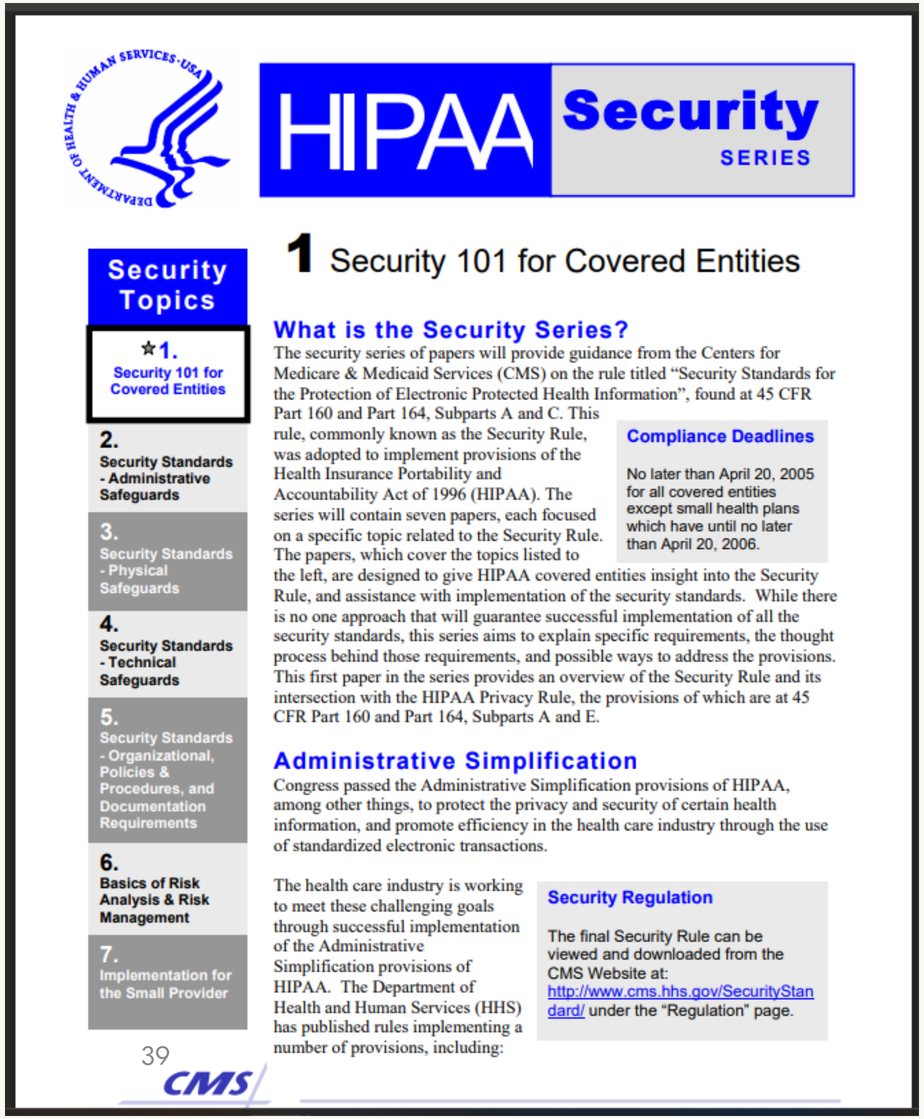
T+

Security Rule Guidance Material

- Security Rule Papers
  - Security 101 Series
  - Guidance on each aspect
- Risk Analysis Resources
- OCR Cyber Awareness Newsletters
- NIST Publications
- FTC Guidance
- Video Training

OCR Security Series

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html



HIPAA Security SERIES

Security Topics

☆1. Security 101 for Covered Entities

2. Security Standards - Administrative Safeguards

3. Security Standards - Physical Safeguards

4. Security Standards - Technical Safeguards

5. Security Standards - Organizational, Policies & Procedures, and Documentation Requirements

6. Basics of Risk Analysis & Risk Management

7. Implementation for the Small Provider

1 Security 101 for Covered Entities

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "Security Standards for the Protection of Electronic Protected Health Information", found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule, and assistance with implementation of the security standards. While there is no one approach that will guarantee successful implementation of all the security standards, this series aims to explain specific requirements, the thought process behind those requirements, and possible ways to address the provisions. This first paper in the series provides an overview of the Security Rule and its intersection with the HIPAA Privacy Rule, the provisions of which are at 45 CFR Part 160 and Part 164, Subparts A and E.

Compliance Deadlines

No later than April 20, 2005 for all covered entities except small health plans which have until no later than April 20, 2006.

Administrative Simplification

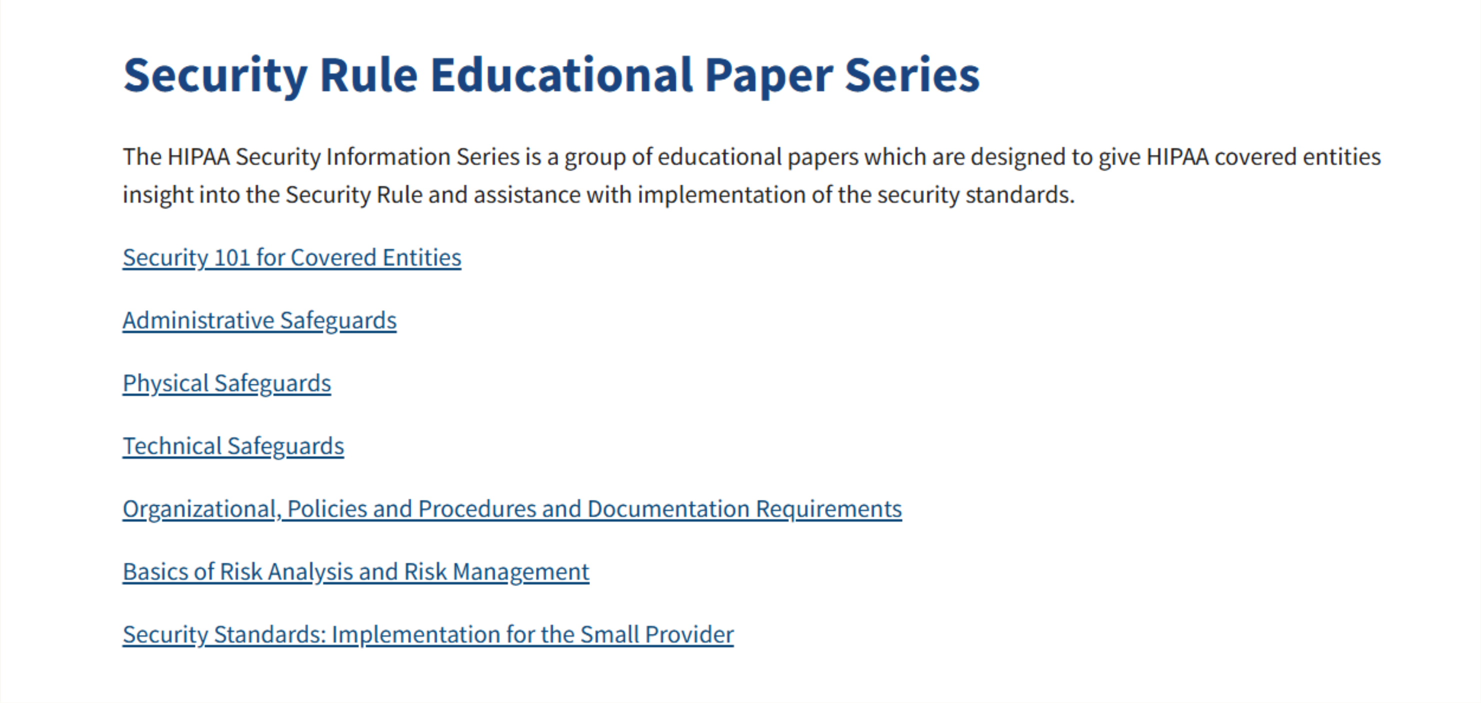
Congress passed the Administrative Simplification provisions of HIPAA, among other things, to protect the privacy and security of certain health information, and promote efficiency in the health care industry through the use of standardized electronic transactions.

The health care industry is working to meet these challenging goals through successful implementation of the Administrative Simplification provisions of HIPAA. The Department of Health and Human Services (HHS) has published rules implementing a number of provisions, including:

Security Regulation

The final Security Rule can be viewed and downloaded from the CMS Website at: http://www.cms.hhs.gov/SecurityStandard/ under the "Regulation" page.

CMS



Security Rule Educational Paper Series

The HIPAA Security Information Series is a group of educational papers which are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards.

Security 101 for Covered Entities

Administrative Safeguards

Physical Safeguards

Technical Safeguards

Organizational, Policies and Procedures and Documentation Requirements

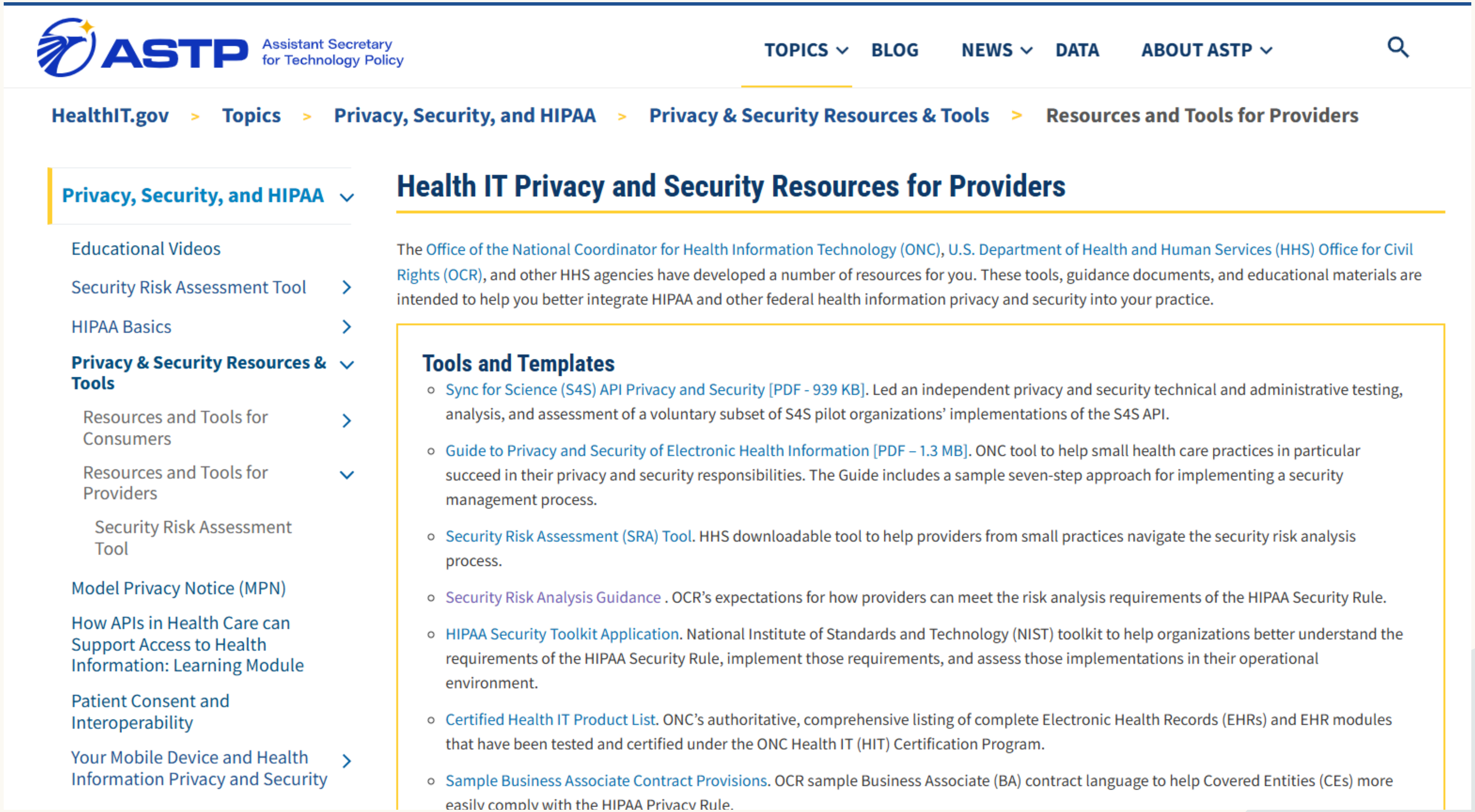
Basics of Risk Analysis and Risk Management

Security Standards: Implementation for the Small Provider

Holland & Hart

HealthIT.Gov

https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers



ASTP Assistant Secretary for Technology Policy
TOPICS
BLOG
NEWS
DATA
ABOUT ASTP

HealthIT.gov > Topics > Privacy, Security, and HIPAA > Privacy & Security Resources & Tools > Resources and Tools for Providers

Privacy, Security, and HIPAA
Educational Videos
Security Risk Assessment Tool
HIPAA Basics
Privacy & Security Resources & Tools
Resources and Tools for Consumers
Resources and Tools for Providers
Security Risk Assessment Tool
Model Privacy Notice (MPN)
How APIs in Health Care can Support Access to Health Information: Learning Module
Patient Consent and Interoperability
Your Mobile Device and Health Information Privacy and Security

Health IT Privacy and Security Resources for Providers

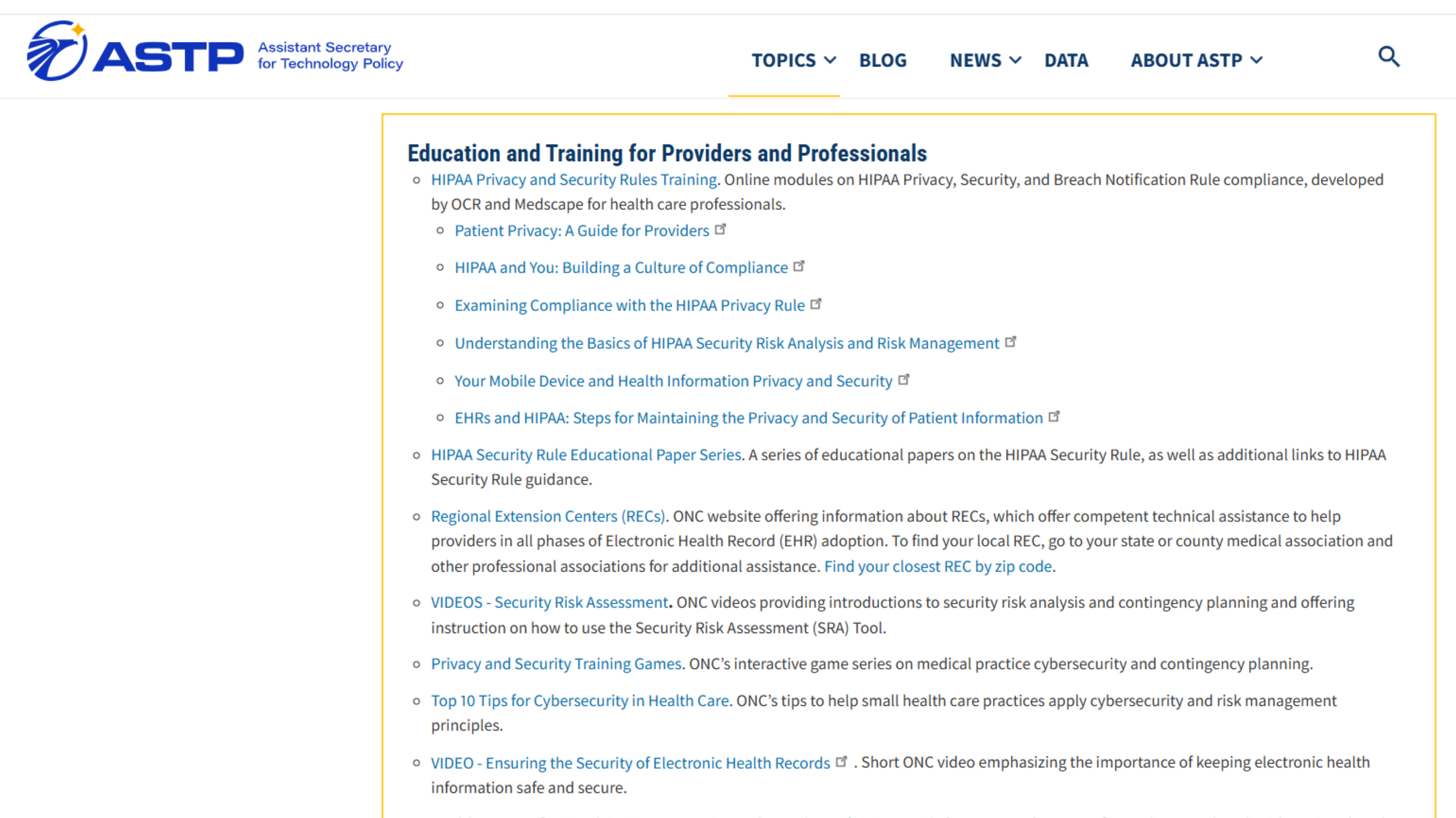
The Office of the National Coordinator for Health Information Technology (ONC), U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and other HHS agencies have developed a number of resources for you. These tools, guidance documents, and educational materials are intended to help you better integrate HIPAA and other federal health information privacy and security into your practice.

Tools and Templates

- Sync for Science (S4S) API Privacy and Security [PDF - 939 KB]. Led an independent privacy and security technical and administrative testing, analysis, and assessment of a voluntary subset of S4S pilot organizations' implementations of the S4S API.
- Guide to Privacy and Security of Electronic Health Information [PDF – 1.3 MB]. ONC tool to help small health care practices in particular succeed in their privacy and security responsibilities. The Guide includes a sample seven-step approach for implementing a security management process.
- Security Risk Assessment (SRA) Tool. HHS downloadable tool to help providers from small practices navigate the security risk analysis process.
- Security Risk Analysis Guidance . OCR's expectations for how providers can meet the risk analysis requirements of the HIPAA Security Rule.
- HIPAA Security Toolkit Application. National Institute of Standards and Technology (NIST) toolkit to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment.
- Certified Health IT Product List. ONC's authoritative, comprehensive listing of complete Electronic Health Records (EHRs) and EHR modules that have been tested and certified under the ONC Health IT (HIT) Certification Program.
- Sample Business Associate Contract Provisions. OCR sample Business Associate (BA) contract language to help Covered Entities (CEs) more easily comply with the HIPAA Privacy Rule.

HealthIT.Gov

https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers



Education and Training for Providers and Professionals

- HIPAA Privacy and Security Rules Training. Online modules on HIPAA Privacy, Security, and Breach Notification Rule compliance, developed by OCR and Medscape for health care professionals.
  - Patient Privacy: A Guide for Providers
  - HIPAA and You: Building a Culture of Compliance
  - Examining Compliance with the HIPAA Privacy Rule
  - Understanding the Basics of HIPAA Security Risk Analysis and Risk Management
  - Your Mobile Device and Health Information Privacy and Security
  - EHRs and HIPAA: Steps for Maintaining the Privacy and Security of Patient Information
- HIPAA Security Rule Educational Paper Series. A series of educational papers on the HIPAA Security Rule, as well as additional links to HIPAA Security Rule guidance.
- Regional Extension Centers (RECs). ONC website offering information about RECs, which offer competent technical assistance to help providers in all phases of Electronic Health Record (EHR) adoption. To find your local REC, go to your state or county medical association and other professional associations for additional assistance. Find your closest REC by zip code.
- VIDEOS - Security Risk Assessment**.** ONC videos providing introductions to security risk analysis and contingency planning and offering instruction on how to use the Security Risk Assessment (SRA) Tool.
- Privacy and Security Training Games. ONC's interactive game series on medical practice cybersecurity and contingency planning.
- Top 10 Tips for Cybersecurity in Health Care. ONC's tips to help small health care practices apply cybersecurity and risk management principles.
- VIDEO - Ensuring the Security of Electronic Health Records . Short ONC video emphasizing the importance of keeping electronic health information safe and secure.

HIPAA Security Rule: Proposed Changes

HIPAA Proposed Security Rule

- Proposed rule published 1/6/25 (90 FR 898)
  - "[I]n recent years, there has been an alarming growth in the number of breaches affecting 500 or more individuals reported to the Department, the overall number of individuals affected by such breaches, and the rampant escalation of cyberattacks using hacking and ransomware. The Department is concerned by the increasing numbers of breaches and other cybersecurity incidents experienced by regulated entities. We are also increasingly concerned by the upward trend in the numbers of individuals affected by such incidents and the magnitude of the potential harms from such incidents…." (90 FR 900)
- If adopted, changes would generally take effective 180 days after final rule is published. (90 FR 901)

HIPAA Proposed Security Rule

- Eliminates "addressable" standards; all standards are required.

Proposed Security Requirements: Annual Requirements

- At least once every 12 months, each covered entity or business associate must:
  - Review/update written inventory of devices containing ePHI and network map re flow of ePHI.
  - Review/update written risk analysis addressing elements specified in the rule.
  - Review/update written risk management plan.
  - Review and test policies and procedures re required standards.
  - Review/update workforce sanctions policies.
  - Review and test written policies re system activity reports.
  - Review/update workforce security policies.

Proposed Administrative Safeguards

1. Technology asset inventory and network mapping
2. Risk analysis
3. Evaluation of changes and affect on ePHI
4. Patch management
5. Risk management
6. Workforce sanctions
7. Information system activity review
8. Assigned security responsibility
9. Workforce security
10. Access management
11. Security awareness training
12. Security incident procedures
13. Contingency plan
14. Compliance audit, including verification that business associate has complied.

Generally, must implement then review, update and/or test the policies and procedures at least once every 12 months

Proposed Physical Safeguards

1. Facility access controls
    a. Contingency operations
    b. Facility security plan
    c. Access management and validation
    d. Physical maintenance records
    e. Maintenance
2. Workstation use
3. Workstation security
4. Technology asset controls, including disposal
    a. Disposal
    b. Media sanitization
    c. Maintenance

Generally, must implement then review, update and/or test the policies and procedures at least once every 12 months

Proposed Technical Safeguards

1. Access controls
    a. Unique identification
    b. Administrative and increased access privileges
    c. Emergency access procedure
    d. Automatic logoff
    e. Log-in attempts
    f. Network segmentation
    g. Data controls
2. Encryption and decryption,
3. Configuration management
    a. Anti-malware protection
    b. Software removal
    c. Configuration
    d. Network ports

Generally, must implement then review, update and/or test the policies and procedures at least once every 12 months

Proposed Technical Safeguards

4. Audit trail and system log controls
   a. Monitor and identify activity
   b. Record real time activity
   c. Retain records of activity
5. Integrity, i.e., protect from improper modification or destruction
6. Authentication
   a. Info access management policies
   b. Multi-factor authentication
7. Transmission security

Generally, must implement then review, update and/or test the policies and procedures at least once every 12 months

Proposed Technical Safeguards

8. Vulnerability management
    a. Vulnerability scanning
    b. Monitoring
    c. Penetration testing
    d. Patch and update installation
9. Data backup and recovery
    a. Data backup
    b. Monitor, identify and alert
    c. Record success, failure and errors of backups
10. Information systems backup and recovery

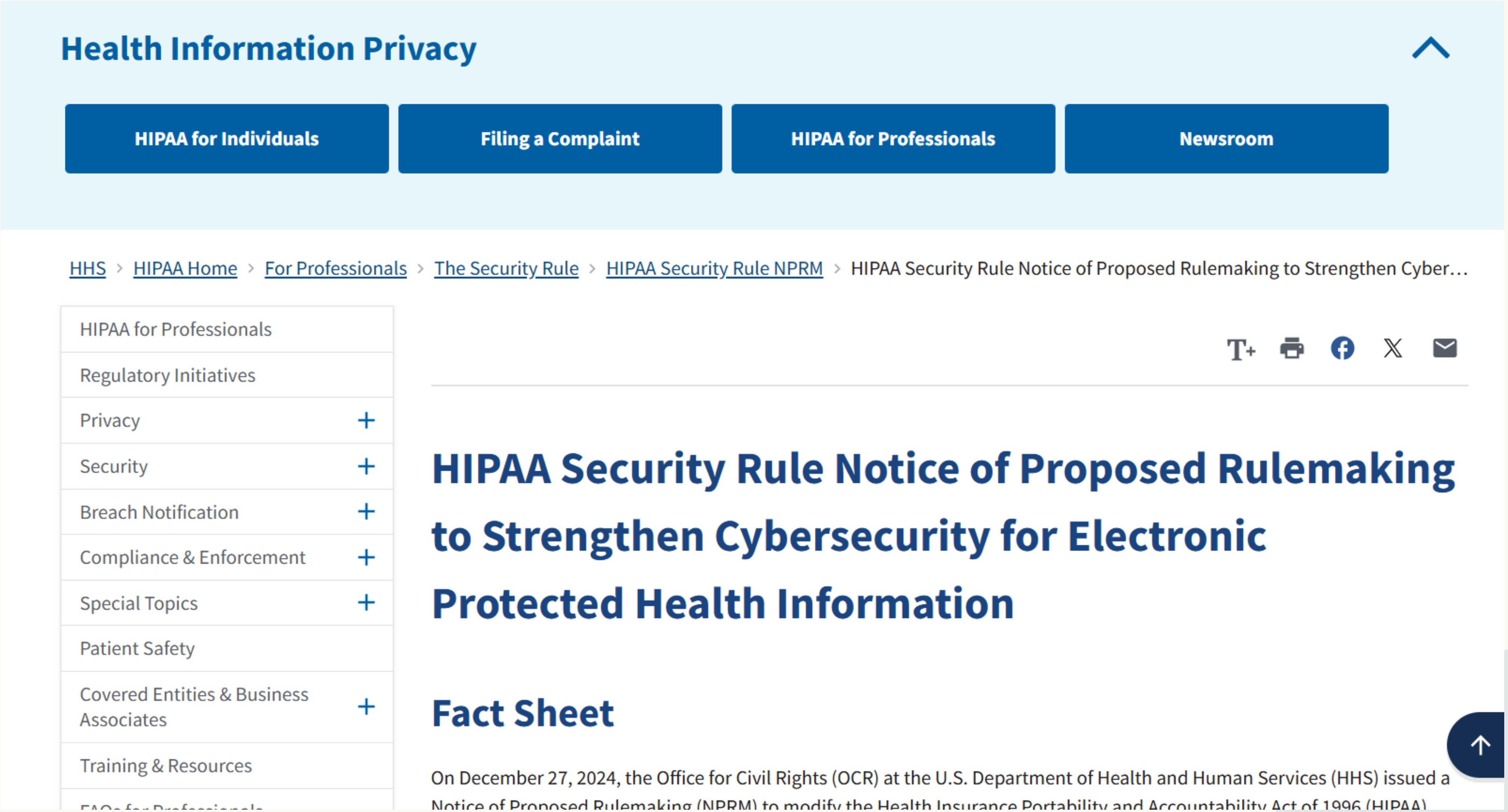
Generally, must implement then review, update and/or test the policies and procedures at least once every 12 months and, in some cases, sooner.

Proposed Business Associate Standards

- In addition to usual BAA requirements, business associate must:
  - Report activation of its contingency plan

HIPAA Proposed Security Rule Changes

https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

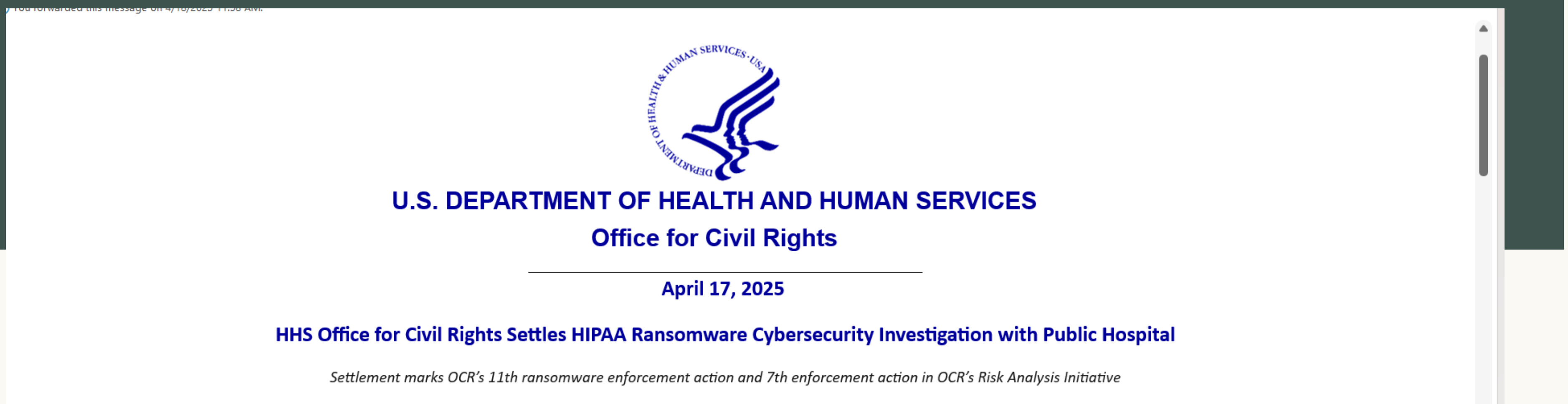


Health Information Privacy
HIPAA for Individuals
Filing a Complaint
HIPAA for Professionals
Newsroom
HHS › HIPAA Home › For Professionals › The Security Rule › HIPAA Security Rule NPRM › HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cyber…
HIPAA for Professionals
Regulatory Initiatives
Privacy +
Security +
Breach Notification +
Compliance & Enforcement +
Special Topics +
Patient Safety
Covered Entities & Business Associates +
Training & Resources
FAQs for Professionals
T+

HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information

Fact Sheet

On December 27, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA)



You forwarded this message on 4/18/2025 11:58 AM.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

April 17, 2025

HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation with Public Hospital

Settlement marks OCR's 11th ransomware enforcement action and 7th enforcement action in OCR's Risk Analysis Initiative

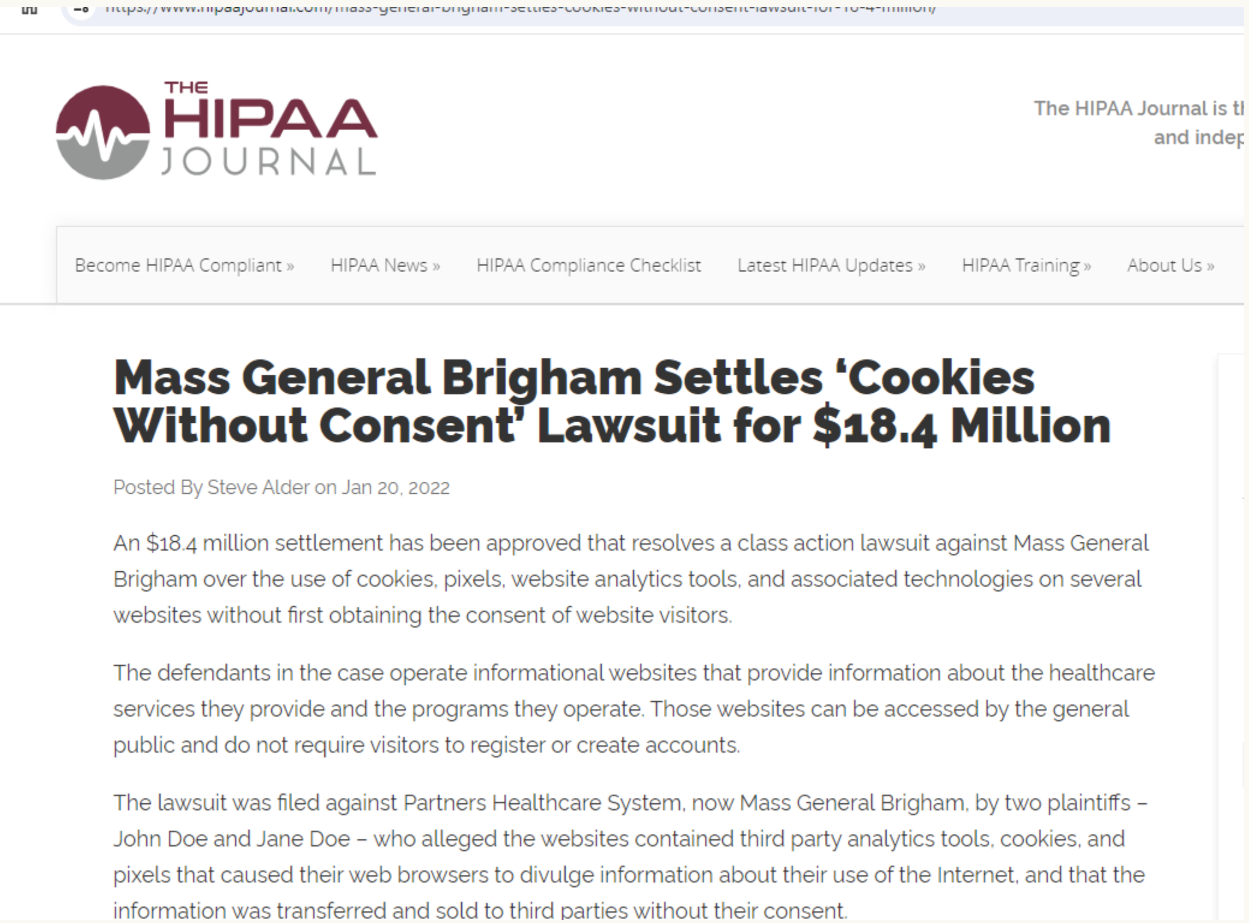
"OCR recommends that health care providers, health plans, … and business associates that are covered by HIPAA take the following steps to mitigate or prevent cyber-threats:

- Identify where ePHI is located in the organization, including how ePHI enters, flows through, and leaves the organization's information systems.
- Integrate risk analysis and risk management into the organization's business processes.
- Ensure that audit controls are in place to record and examine information system activity.
- Implement regular reviews of information system activity.
- Utilize mechanisms to authenticate information to ensure only authorized users are accessing ePHI.
- Encrypt ePHI in transit and at rest to guard against unauthorized access to ePHI when appropriate.
- Incorporate lessons learned from incidents into the organization's overall security management process.
- Provide workforce members with regular HIPAA training that is specific to the organization and to the workforce members' respective job duties."

HIPAA and Online Tracking Technologies

Holland & Hart

Online Tracking Concerns


https://www.hipaajournal.com/mass-general-brigham-settles-cookies-without-consent-lawsuit-for-18-4-million/
THE HIPAA JOURNAL
The HIPAA Journal is th
and indep
Become HIPAA Compliant »
HIPAA News »
HIPAA Compliance Checklist
Latest HIPAA Updates »
HIPAA Training »
About Us »

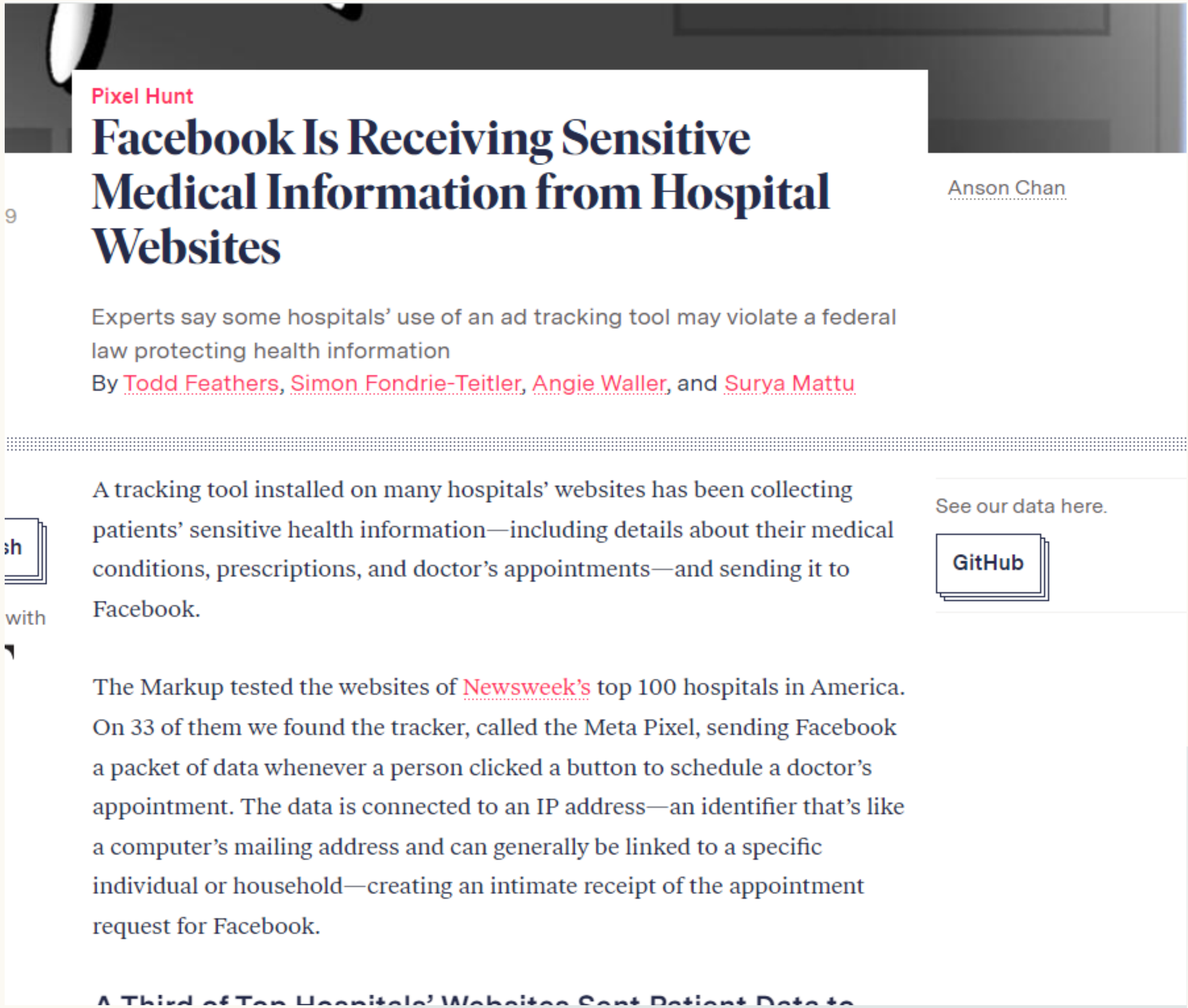
Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for $18.4 Million

Posted By Steve Alder on Jan 20, 2022

An $18.4 million settlement has been approved that resolves a class action lawsuit against Mass General Brigham over the use of cookies, pixels, website analytics tools, and associated technologies on several websites without first obtaining the consent of website visitors.

The defendants in the case operate informational websites that provide information about the healthcare services they provide and the programs they operate. Those websites can be accessed by the general public and do not require visitors to register or create accounts.

The lawsuit was filed against Partners Healthcare System, now Mass General Brigham, by two plaintiffs – John Doe and Jane Doe – who alleged the websites contained third party analytics tools, cookies, and pixels that caused their web browsers to divulge information about their use of the Internet, and that the information was transferred and sold to third parties without their consent.



Pixel Hunt

Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Experts say some hospitals' use of an ad tracking tool may violate a federal law protecting health information

By Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu

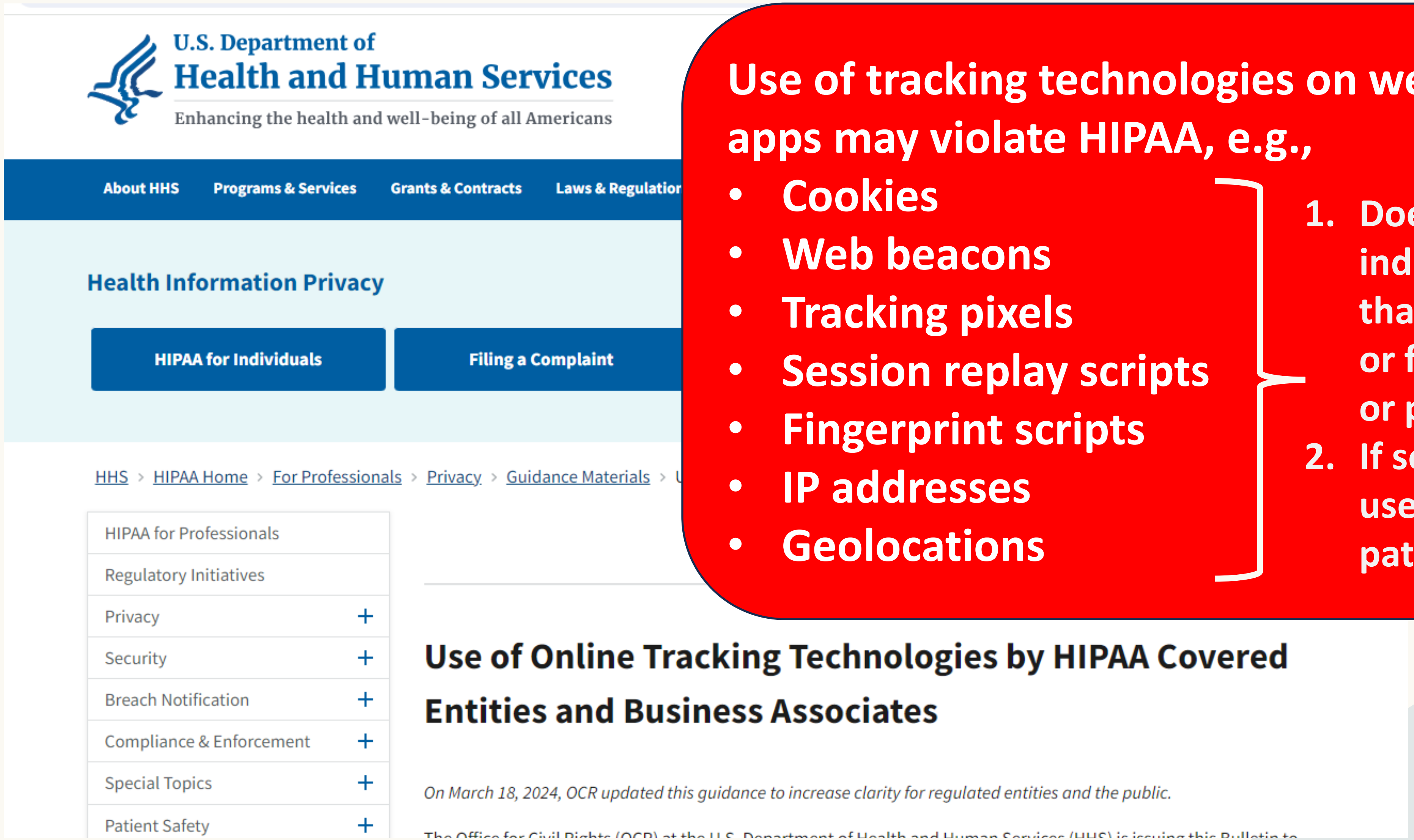
A tracking tool installed on many hospitals' websites has been collecting patients' sensitive health information—including details about their medical conditions, prescriptions, and doctor's appointments—and sending it to Facebook.

The Markup tested the websites of Newsweek's top 100 hospitals in America. On 33 of them we found the tracker, called the Meta Pixel, sending Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment. The data is connected to an IP address—an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook.

A Third of Top Hospitals' Websites Sent Patient Data to

HIPAA and Online Tracking

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html



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

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

Health Information Privacy

HIPAA for Individuals | Filing a Complaint

HHS > HIPAA Home > For Professionals > Privacy > Guidance Materials > U

- HIPAA for Professionals
- Regulatory Initiatives
- Privacy +
- Security +
- Breach Notification +
- Compliance & Enforcement +
- Special Topics +
- Patient Safety +

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

On March 18, 2024, OCR updated this guidance to increase clarity for regulated entities and the public.

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to

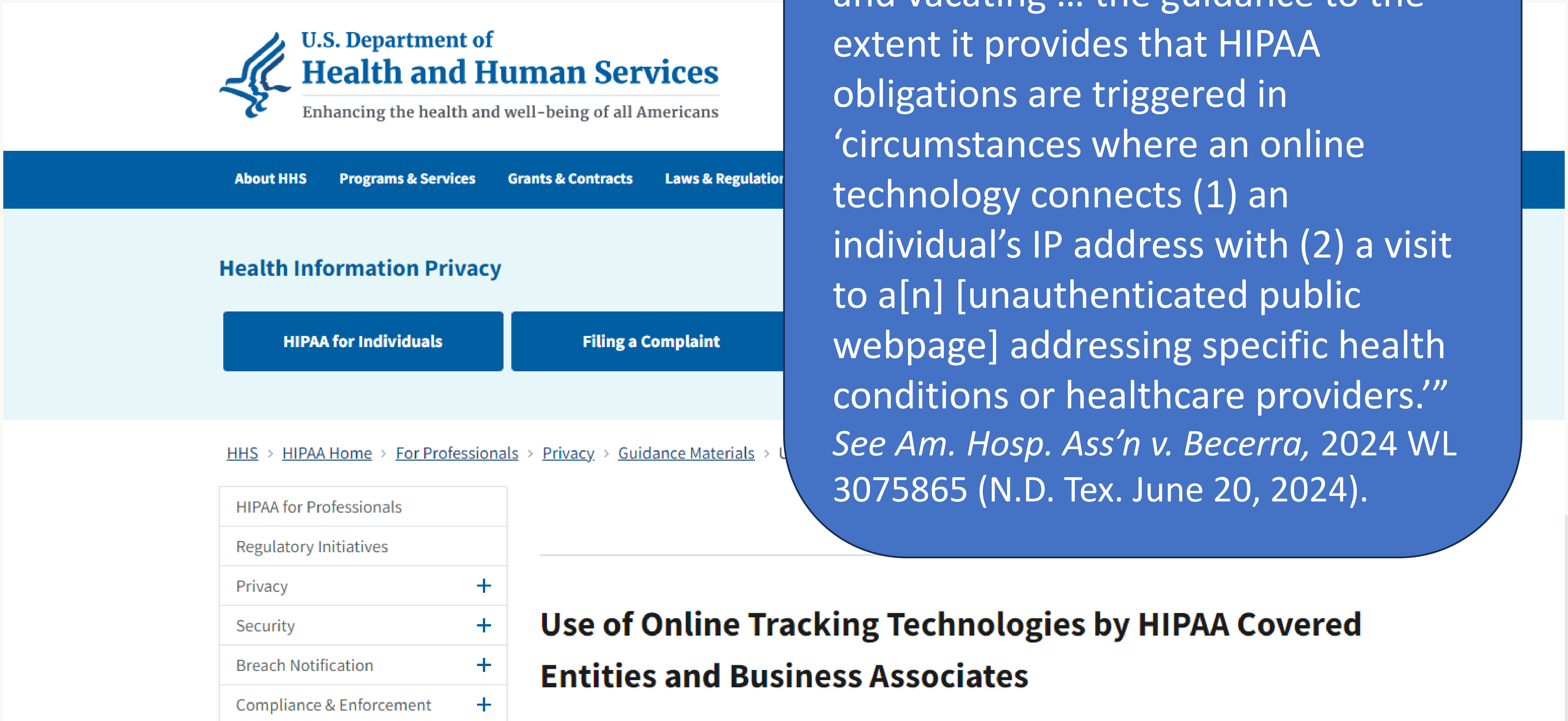
Use of tracking technologies on websites and mobile apps may violate HIPAA, e.g.,

- **Cookies**
- **Web beacons**
- **Tracking pixels**
- **Session replay scripts**
- **Fingerprint scripts**
- **IP addresses**
- **Geolocations**

1. **Does the data contain individually identifiable info that relates to past, present, or future health, healthcare or payment?**
2. **If so, does HIPAA permit the use or disclosure without patient authorization?**

Holland & Hart

HIPAA and Online Tracking



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

Health Information Privacy

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

"On June 20, 2024, [a district court] issued an order declaring unlawful and vacating … 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.'" *See Am. Hosp. Ass'n v. Becerra*, 2024 WL 3075865 (N.D. Tex. June 20, 2024).

HIPAA and Online Tracking

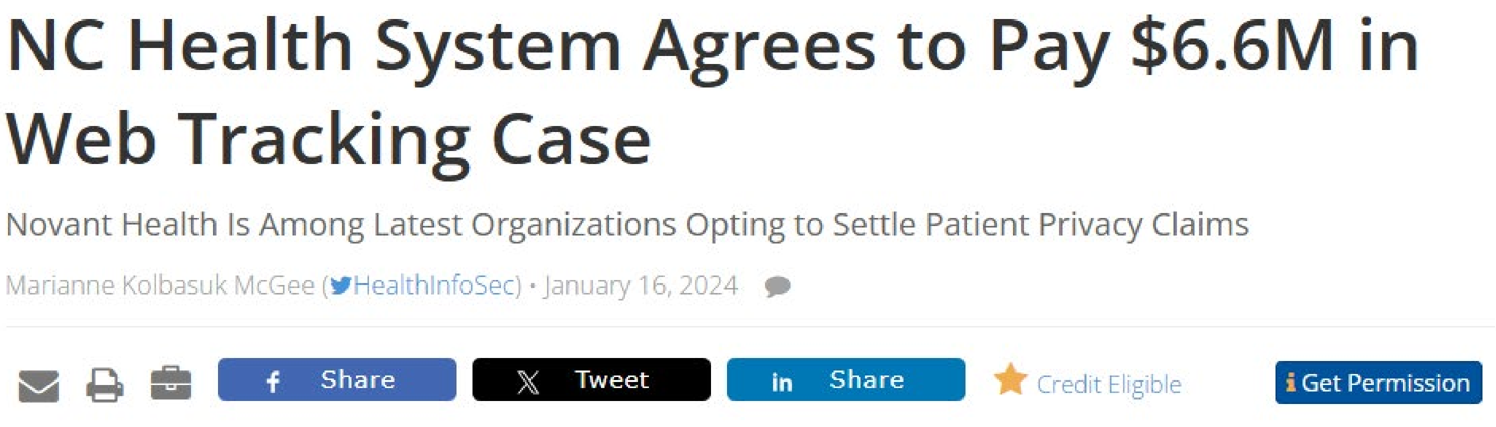
✓Comply with security rule when using or preventing tracking technologies.

- "OCR is prioritizing compliance with the HIPAA Security Rule in investigations into the use of online tracking technologies."
- Include tracking technology in risk assessment.
- Include required administrative, technical and physical safeguards (e.g., encrypting ePHI; enable appropriate authentication; access controls; audits; etc.).

✓Notify patients and OCR of breaches per breach reporting rule.

(https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html)

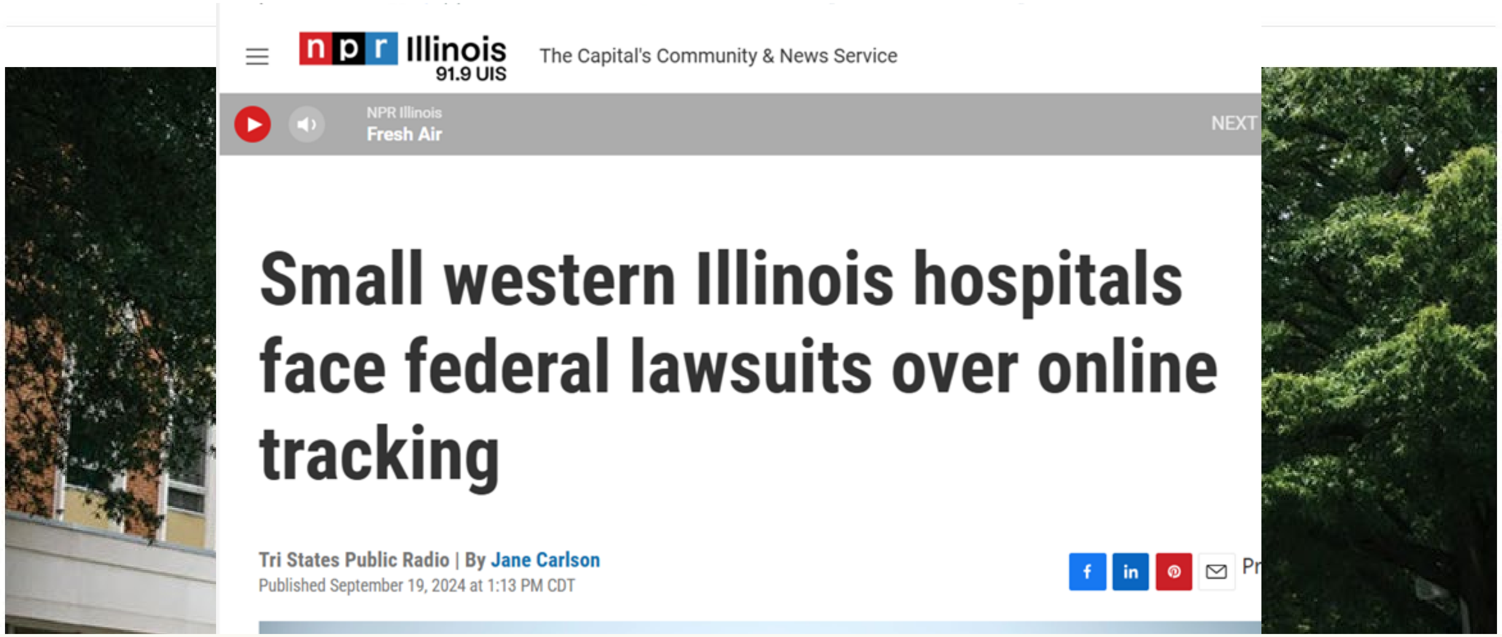
Online Tracking Lawsuits



NC Health System Agrees to Pay $6.6M in Web Tracking Case

Novant Health Is Among Latest Organizations Opting to Settle Patient Privacy Claims

Marianne Kolbasuk McGee (HealthInfoSec) • January 16, 2024



Small western Illinois hospitals face federal lawsuits over online tracking

Tri States Public Radio | By Jane Carlson
Published September 19, 2024 at 1:13 PM CDT

Possible Theories

- Negligence per se based on violation of statute
- Unfair or deceptive trade practices acts
- Federal and state wire-tapping laws
- Negligent misrepresentation
- Invasion of privacy
- Breach of contract
- Others?

Holland & Hart

Breach Notification Rule
(45 CFR 164.400 - .420)

Breach Notification

- If there is “breach” of “unsecured PHI”,
  - Covered entity must notify:
    - Each individual whose unsecured PHI has been or reasonably believed to have been accessed, acquired, used, or disclosed.
    - HHS.
    - Local media, if breach involves > 500 persons in a state.
  - Business associate must notify covered entity.

(45 CFR 164.400 et seq.)

"Breach" of Unsecured PHI

- Acquisition, access, use or disclosure of PHI in violation of privacy rule is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the info has been compromised based on a risk assessment of the following factors:
  - nature and extent of PHI involved;
  - unauthorized person who used or received the PHI;
  - whether PHI was actually acquired or viewed; and
  - extent to which the risk to the PHI has been mitigated,

– unless an exception applies.

(45 CFR 164.402)

Not a "Breach" of Unsecured PHI

- Loss of "secured" data, e.g., properly encrypted.
- Incidental disclosure, i.e., disclosure that is incidental to permissible disclosure so long as covered entity implemented reasonable safeguards.

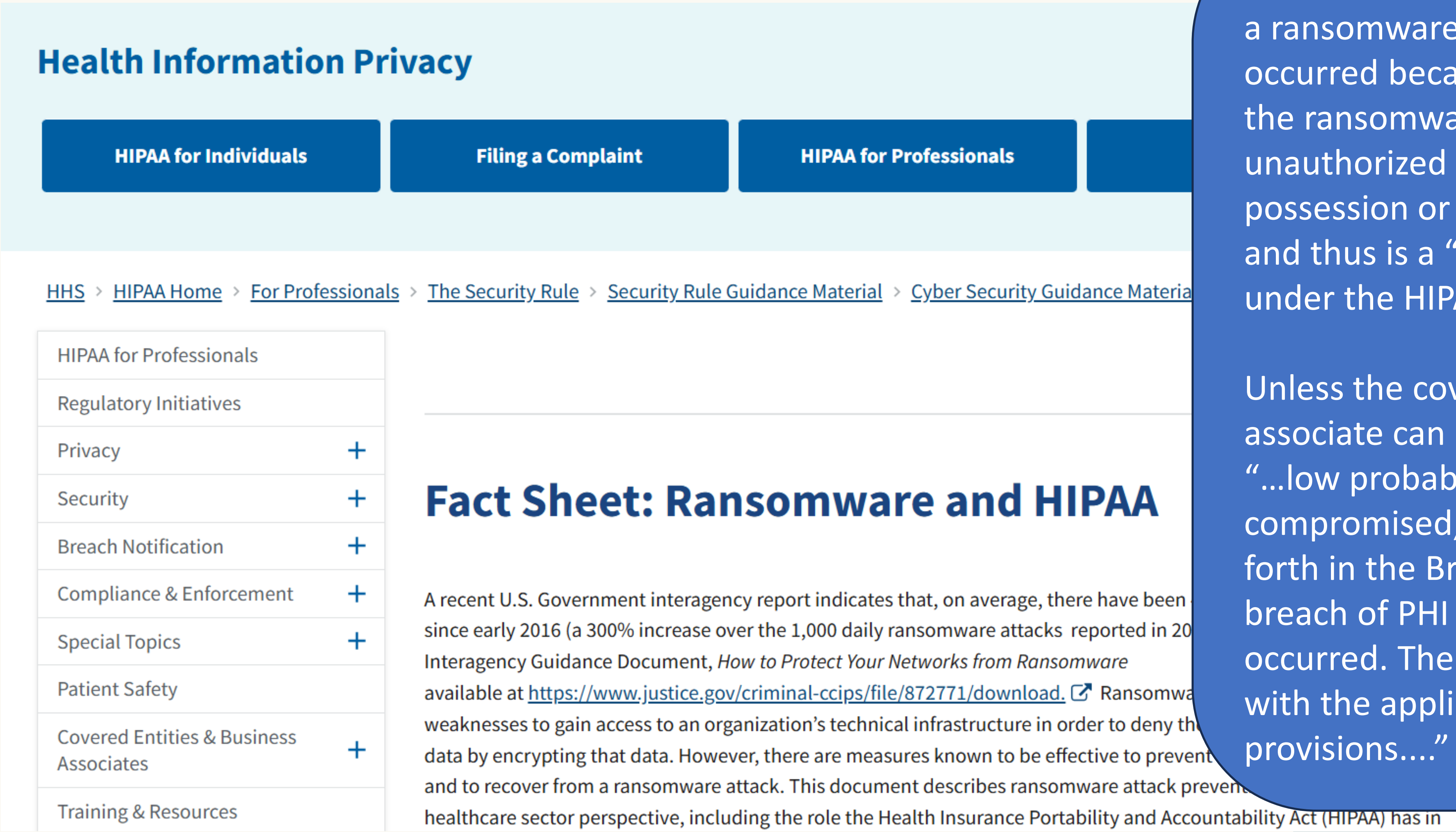
(45 CFR 164.502(a)(1)(iii))

- "Breach" defined to exclude:
  - Unintentional acquisition, access or use by workforce member if made in good faith, within scope of authority, and PHI not further disclosed in violation of privacy rule.
  - Inadvertent disclosure by authorized person to another authorized person at same covered entity, and PHI not further used or disclosed in violation of privacy rule.
  - Disclosure of PHI where covered entity has good faith belief that unauthorized person receiving info would not be able to retain info.

(45 CFR 164.402)

OCR Ransomware Guidance

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html



Health Information Privacy
HIPAA for Individuals
Filing a Complaint
HIPAA for Professionals
HHS › HIPAA Home › For Professionals › The Security Rule › Security Rule Guidance Material › Cyber Security Guidance Materia
HIPAA for Professionals
Regulatory Initiatives
Privacy +
Security +
Breach Notification +
Compliance & Enforcement +
Special Topics +
Patient Safety
Covered Entities & Business Associates +
Training & Resources

Fact Sheet: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 20 Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download. Ransomwa weaknesses to gain access to an organization's technical infrastructure in order to deny th data by encrypting that data. However, there are measures known to be effective to prevent and to recover from a ransomware attack. This document describes ransomware attack preven healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in

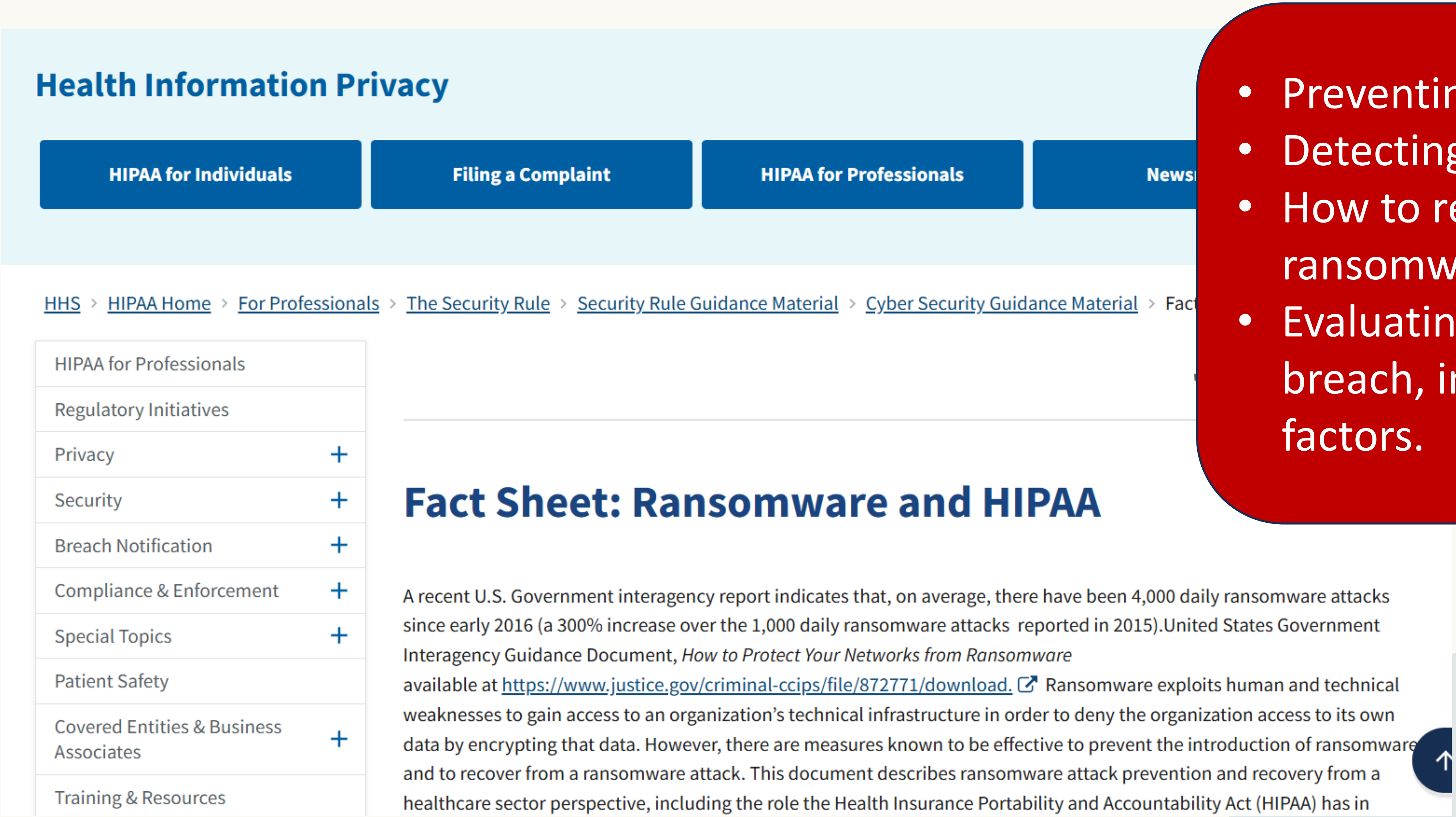
"When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions…."

OCR Ransomware Guidance

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html

- Preventing ransomware.
- Detecting ransomware.
- How to respond to ransomware.
- Evaluating if there is breach, including risk factors.

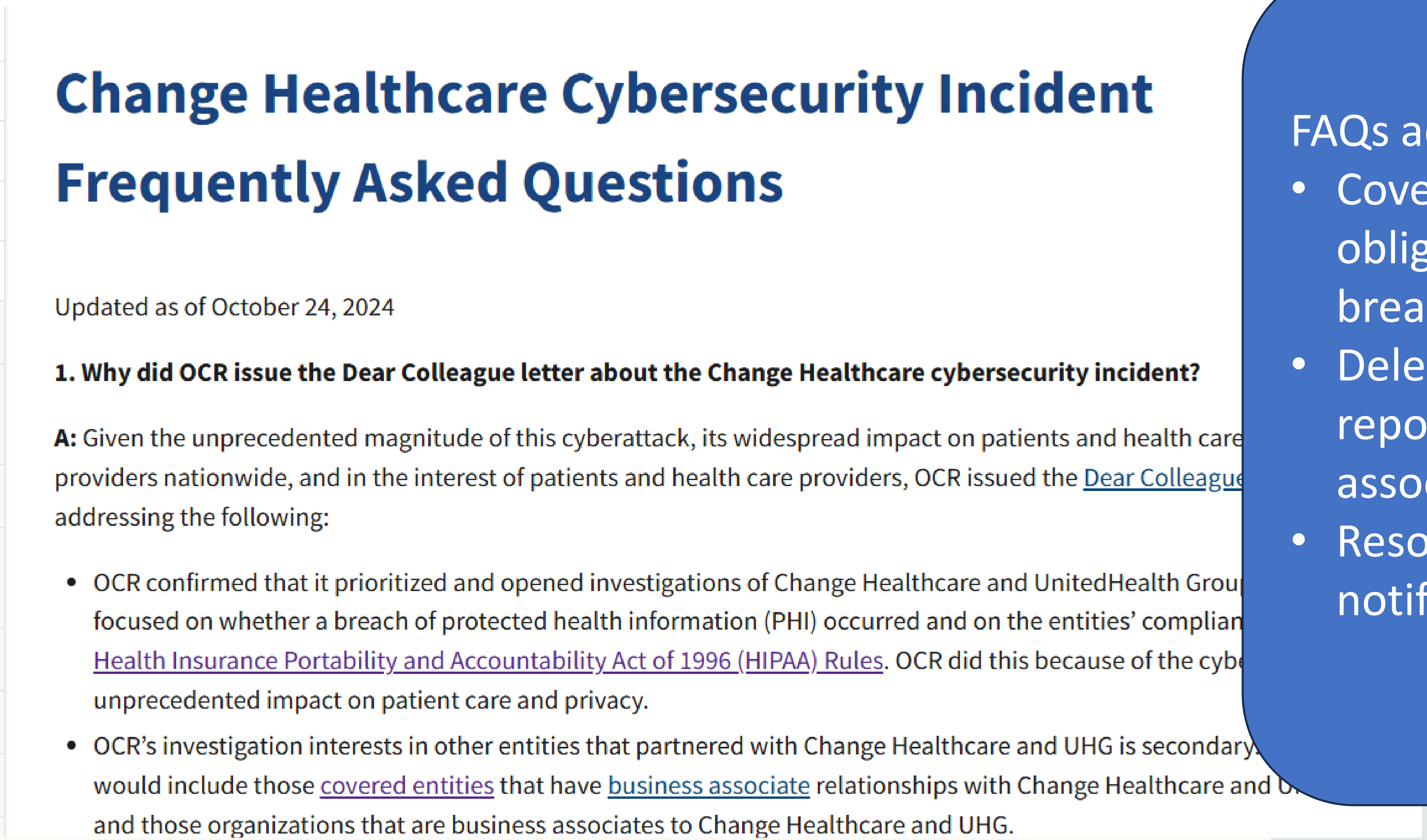


Fact Sheet: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download. Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in

Change Cyberbreach

https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html



Change Healthcare Cybersecurity Incident Frequently Asked Questions

Updated as of October 24, 2024

1. Why did OCR issue the Dear Colleague letter about the Change Healthcare cybersecurity incident?

A: Given the unprecedented magnitude of this cyberattack, its widespread impact on patients and health care providers nationwide, and in the interest of patients and health care providers, OCR issued the Dear Colleague addressing the following:

- OCR confirmed that it prioritized and opened investigations of Change Healthcare and UnitedHealth Grou focused on whether a breach of protected health information (PHI) occurred and on the entities' complian Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules. OCR did this because of the cybe unprecedented impact on patient care and privacy.
- OCR's investigation interests in other entities that partnered with Change Healthcare and UHG is secondary would include those covered entities that have business associate relationships with Change Healthcare and U and those organizations that are business associates to Change Healthcare and UHG.

FAQs address items such as:

- Covered entities' obligation to report the breach.
- Delegating breach reporting to its business associate (e.g., Change).
- Resolving breach notification with Change.

Cybersecurity

HHS Strategy Paper

https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

HEALTHCARE SECTOR CYBERSECURITY

Introduction to the Strategy of the U.S. Department of Health and Human Services

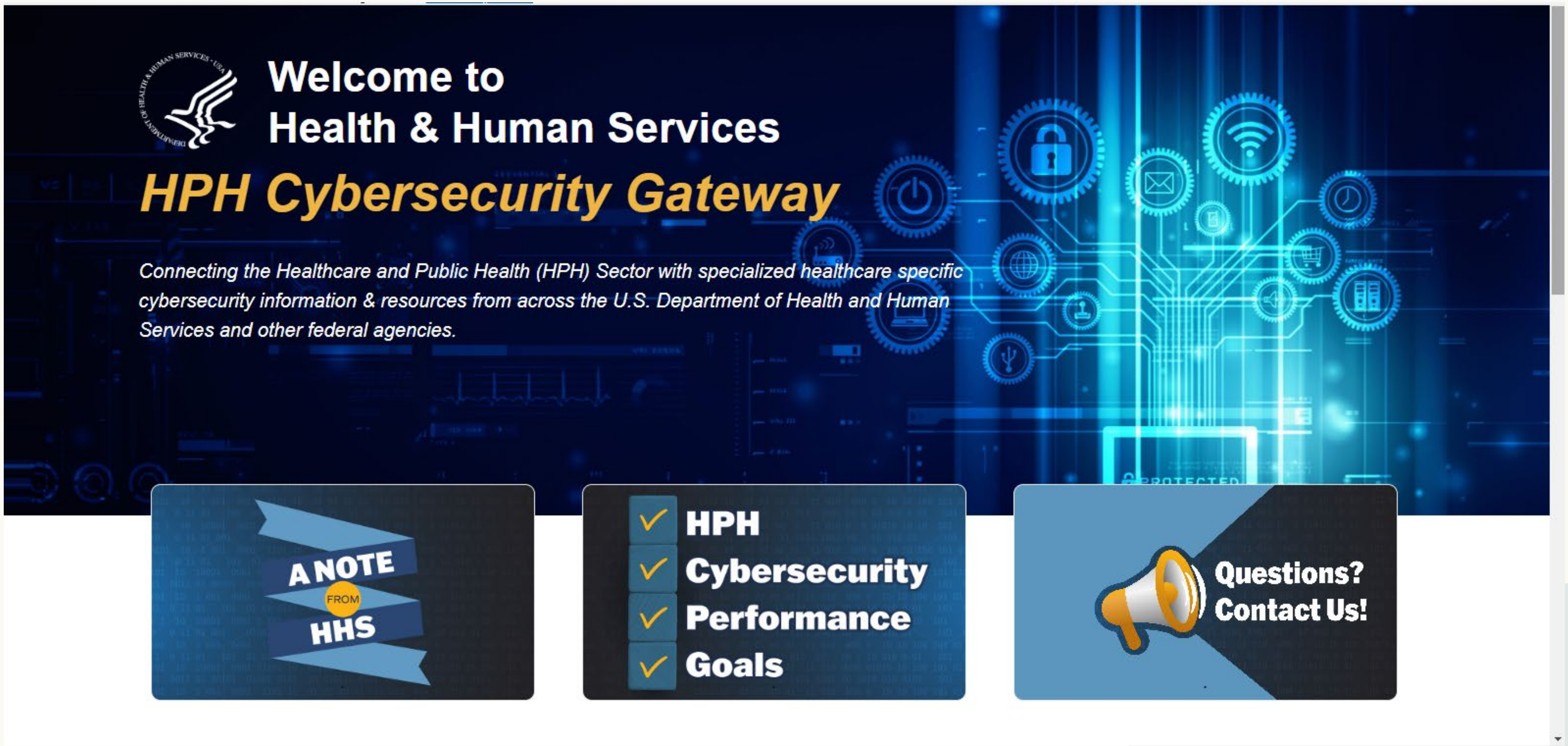
Coming Soon?

On 12/6/23, HHS published strategy for strengthening cybersecurity for healthcare industry.

1. Establish voluntary cybersecurity performance goals.
2. Provide resources to incentivize and implement cybersecurity practices.
3. Greater enforcement and accountability.
   - Cybersecurity requirements for hospitals through Medicare/Medicaid.
   - Update HIPAA Security Rule to include new cybersecurity rule requirements.
   - Increase civil penalties.
   - Increase resources for audits and investigation.
4. HHS to provide one-stop shop for healthcare cybersecurity resources.

HPH Cybersecurity Gateway

https://hphcyber.hhs.gov/



Welcome to
Health & Human Services

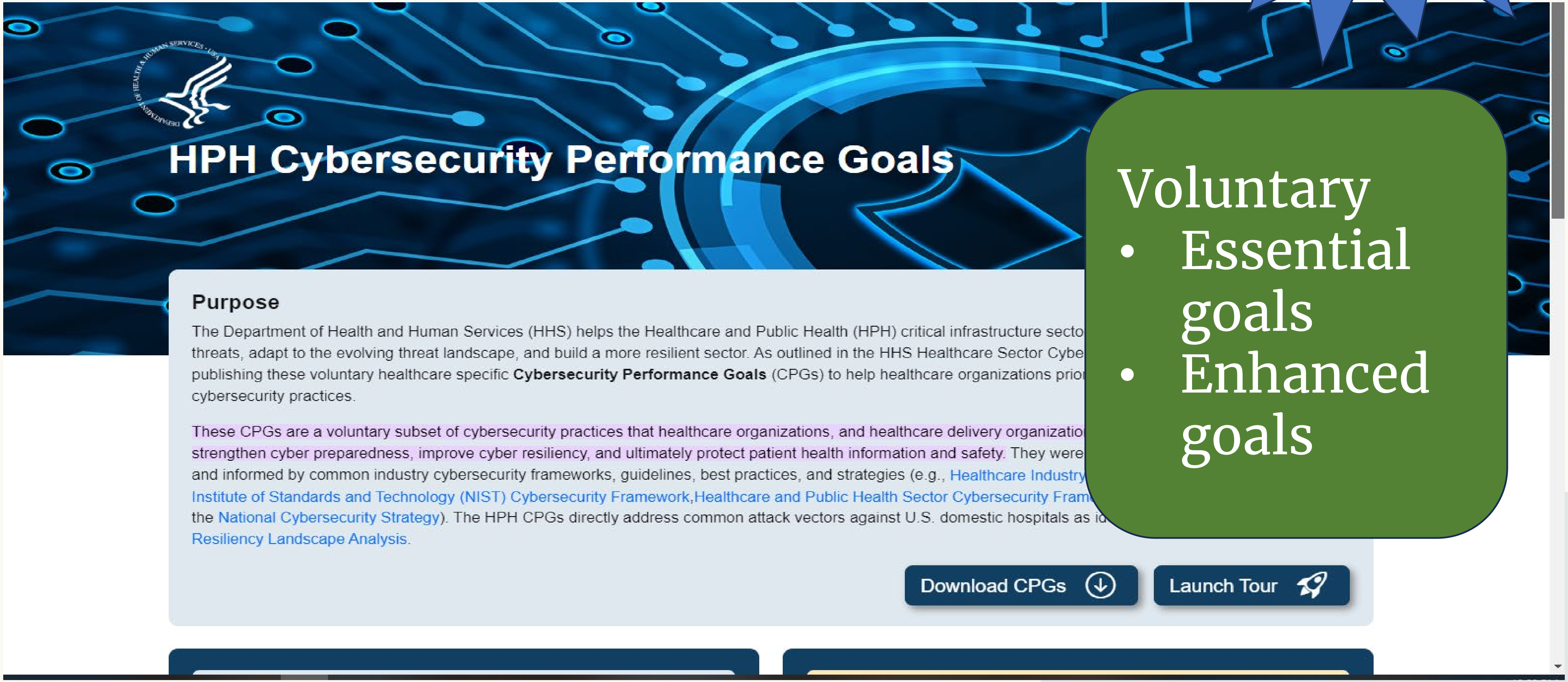
HPH Cybersecurity Gateway

Connecting the Healthcare and Public Health (HPH) Sector with specialized healthcare specific cybersecurity information & resources from across the U.S. Department of Health and Human Services and other federal agencies.

HHS Cybersecurity Performance Goals

https://hphcyber.hhs.gov/documents/cybersecurity-performance-goals.pdf

1/24/24



HPH Cybersecurity Performance Goals

Purpose

The Department of Health and Human Services (HHS) helps the Healthcare and Public Health (HPH) critical infrastructure secto threats, adapt to the evolving threat landscape, and build a more resilient sector. As outlined in the HHS Healthcare Sector Cybe publishing these voluntary healthcare specific **Cybersecurity Performance Goals** (CPGs) to help healthcare organizations prio cybersecurity practices.

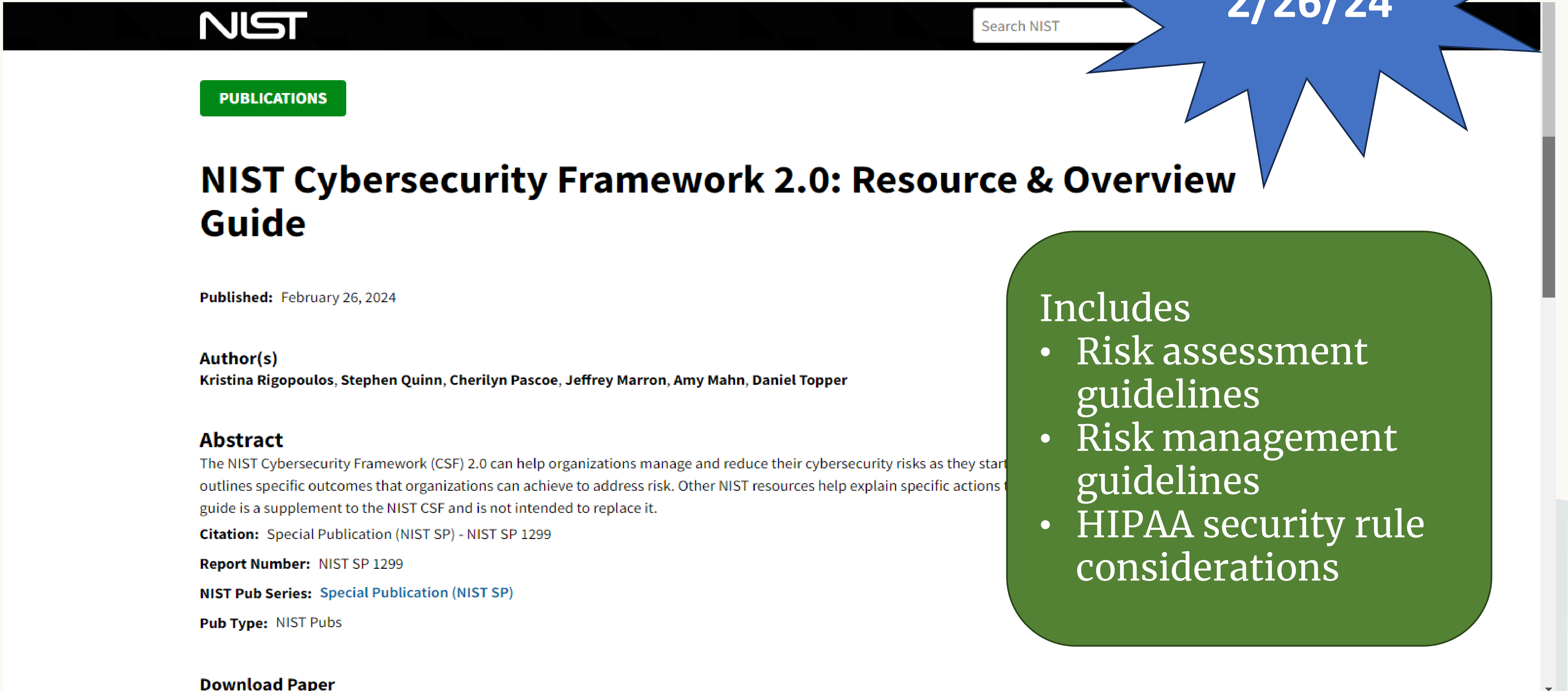
These CPGs are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizatio strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They were and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare Industry Institute of Standards and Technology (NIST) Cybersecurity Framework,Healthcare and Public Health Sector Cybersecurity Fram the National Cybersecurity Strategy). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as id Resiliency Landscape Analysis.

Voluntary
- Essential goals
- Enhanced goals

NIST Cybersecurity Framework 2.0

https://www.nist.gov/publications/nist-cybersecurity-framework-20-resource-overview-guide

2/26/24



PUBLICATIONS

NIST Cybersecurity Framework 2.0: Resource & Overview Guide

Published: February 26, 2024

Author(s)

Kristina Rigopoulos, Stephen Quinn, Cherilyn Pascoe, Jeffrey Marron, Amy Mahn, Daniel Topper

Abstract

The NIST Cybersecurity Framework (CSF) 2.0 can help organizations manage and reduce their cybersecurity risks as they start
outlines specific outcomes that organizations can achieve to address risk. Other NIST resources help explain specific actions t
guide is a supplement to the NIST CSF and is not intended to replace it.

Citation: Special Publication (NIST SP) - NIST SP 1299

Report Number: NIST SP 1299

NIST Pub Series: Special Publication (NIST SP)

Pub Type: NIST Pubs

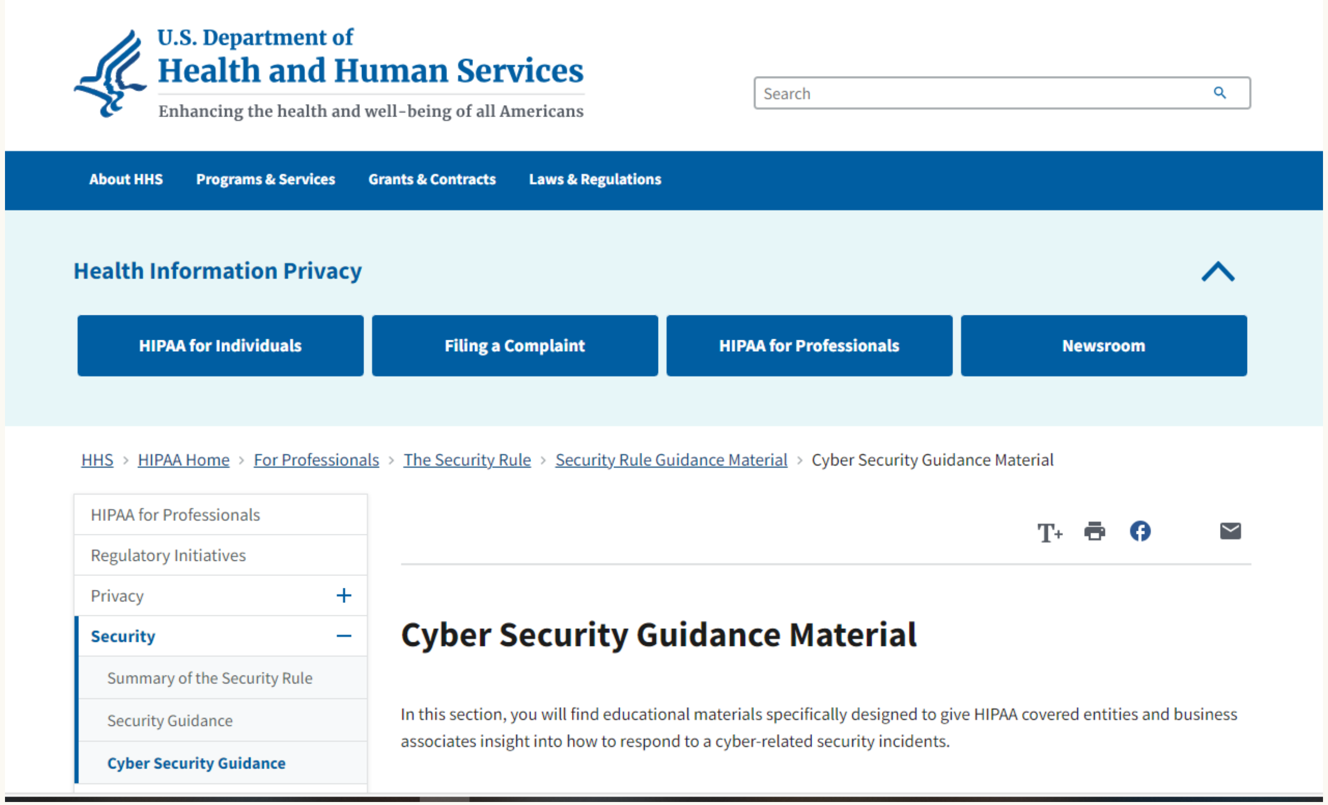
Download Paper

Includes

- Risk assessment guidelines
- Risk management guidelines
- HIPAA security rule considerations

OCR Cybersecurity Guidance

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html



Cyber Security Guidance Material

In this section, you will find educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to a cyber-related security incidents.

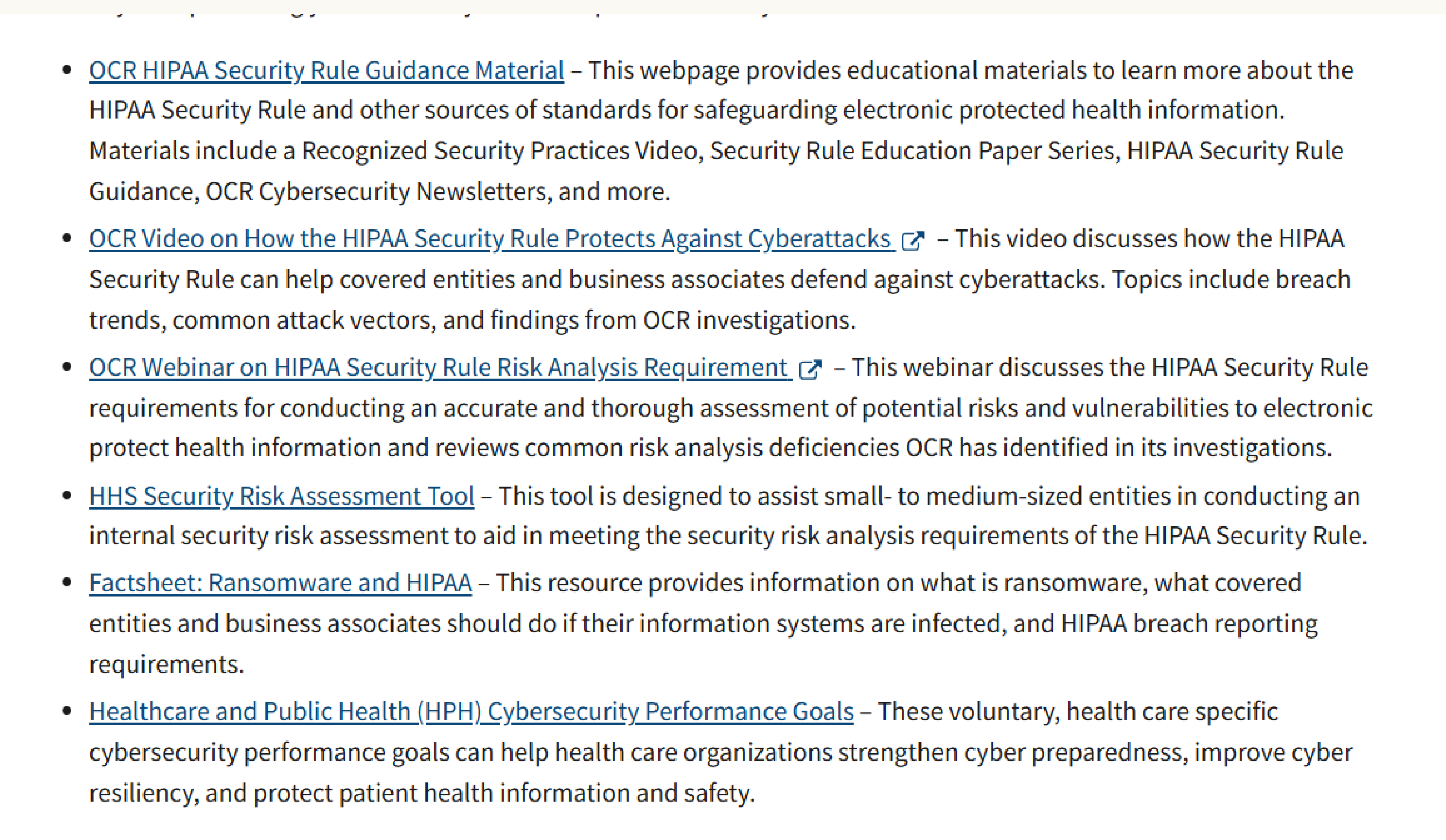
- Cybersecurity Resources
- Cybersecurity Newsletters
  - Sanction policies (10/23)
  - Authentication (6/23)
  - Security rule incident procedures (10/22)
  - Defending against common cyber attacks (3/22)
  - Others
- Cyber incident response checklist

Sign up for OCR listserv at
https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html?language=es

Holland & Hart

OCR Cybersecurity Resources

https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html



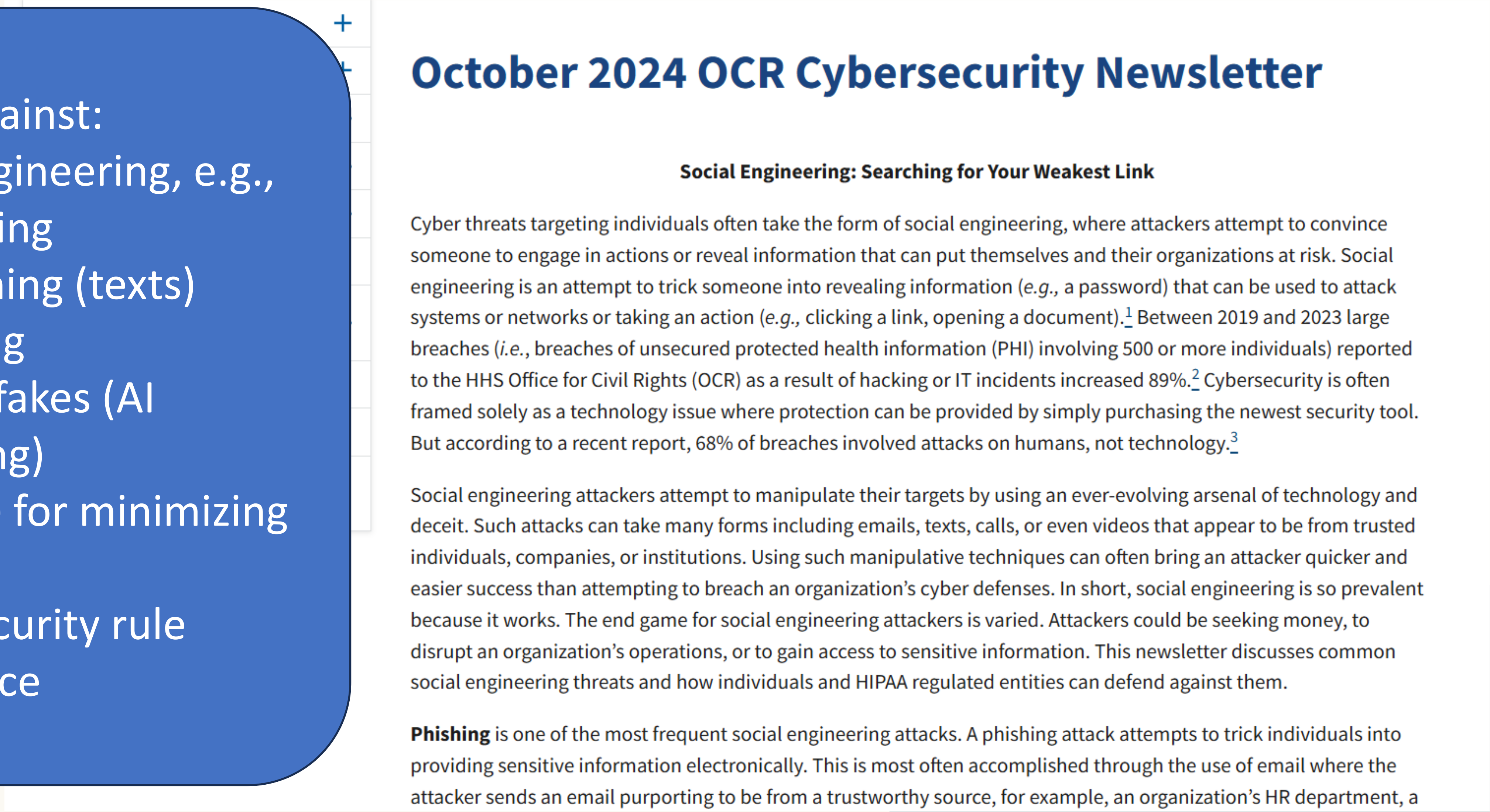
- OCR HIPAA Security Rule Guidance Material – This webpage provides educational materials to learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information. Materials include a Recognized Security Practices Video, Security Rule Education Paper Series, HIPAA Security Rule Guidance, OCR Cybersecurity Newsletters, and more.
- OCR Video on How the HIPAA Security Rule Protects Against Cyberattacks – This video discusses how the HIPAA Security Rule can help covered entities and business associates defend against cyberattacks. Topics include breach trends, common attack vectors, and findings from OCR investigations.
- OCR Webinar on HIPAA Security Rule Risk Analysis Requirement – This webinar discusses the HIPAA Security Rule requirements for conducting an accurate and thorough assessment of potential risks and vulnerabilities to electronic protect health information and reviews common risk analysis deficiencies OCR has identified in its investigations.
- HHS Security Risk Assessment Tool – This tool is designed to assist small- to medium-sized entities in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule.
- Factsheet: Ransomware and HIPAA – This resource provides information on what is ransomware, what covered entities and business associates should do if their information systems are infected, and HIPAA breach reporting requirements.
- Healthcare and Public Health (HPH) Cybersecurity Performance Goals – These voluntary, health care specific cybersecurity performance goals can help health care organizations strengthen cyber preparedness, improve cyber resiliency, and protect patient health information and safety.

OCR Cybersecurity Newsletter (10/24)

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2024/index.html

Cautions against:

- Social engineering, e.g.,
  - Phishing
  - Smishing (texts)
  - Baiting
  - Deepfakes (AI cloning)
- Guidance for minimizing exposure
- HIPAA security rule compliance



October 2024 OCR Cybersecurity Newsletter

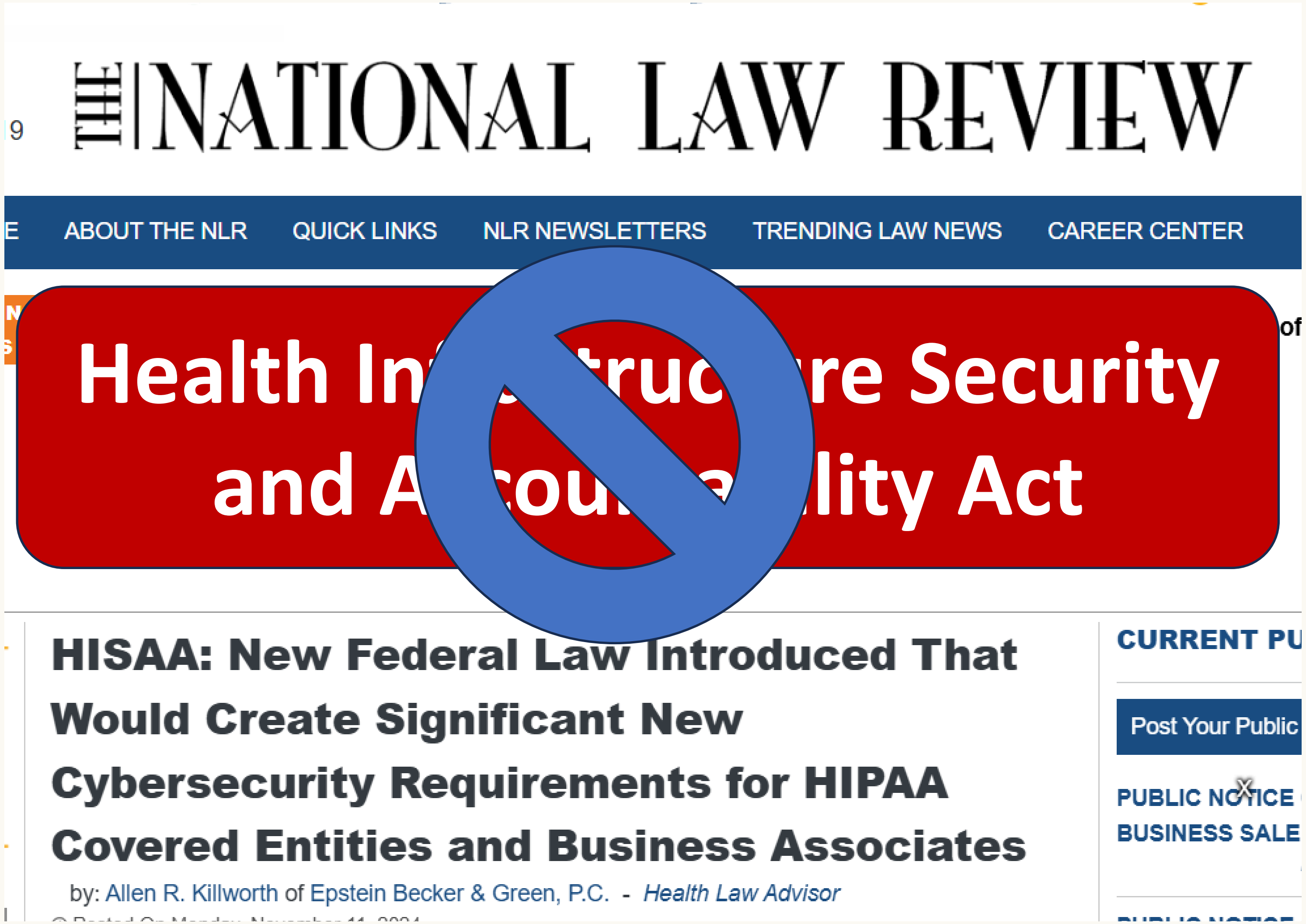
Social Engineering: Searching for Your Weakest Link

Cyber threats targeting individuals often take the form of social engineering, where attackers attempt to convince someone to engage in actions or reveal information that can put themselves and their organizations at risk. Social engineering is an attempt to trick someone into revealing information (*e.g.,* a password) that can be used to attack systems or networks or taking an action (*e.g.,* clicking a link, opening a document).[1] Between 2019 and 2023 large breaches (*i.e.*, breaches of unsecured protected health information (PHI) involving 500 or more individuals) reported to the HHS Office for Civil Rights (OCR) as a result of hacking or IT incidents increased 89%.[2] Cybersecurity is often framed solely as a technology issue where protection can be provided by simply purchasing the newest security tool. But according to a recent report, 68% of breaches involved attacks on humans, not technology.[3]

Social engineering attackers attempt to manipulate their targets by using an ever-evolving arsenal of technology and deceit. Such attacks can take many forms including emails, texts, calls, or even videos that appear to be from trusted individuals, companies, or institutions. Using such manipulative techniques can often bring an attacker quicker and easier success than attempting to breach an organization's cyber defenses. In short, social engineering is so prevalent because it works. The end game for social engineering attackers is varied. Attackers could be seeking money, to disrupt an organization's operations, or to gain access to sensitive information. This newsletter discusses common social engineering threats and how individuals and HIPAA regulated entities can defend against them.

Phishing is one of the most frequent social engineering attacks. A phishing attack attempts to trick individuals into providing sensitive information electronically. This is most often accomplished through the use of email where the attacker sends an email purporting to be from a trustworthy source, for example, an organization's HR department, a

Proposed Legislation: HISAA?



Health In truc re Security and A cou lity Act

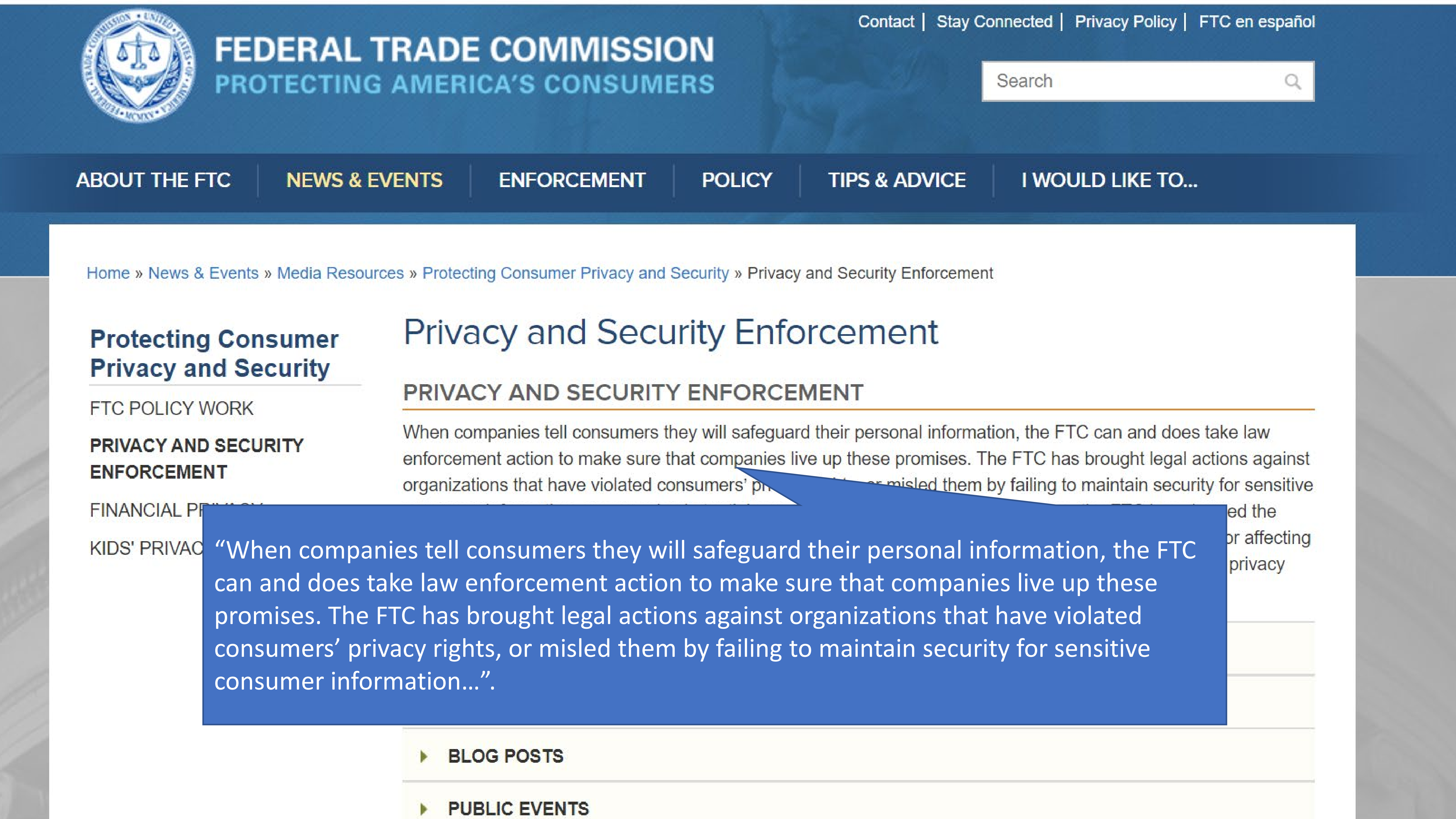
HISAA: New Federal Law Introduced That Would Create Significant New Cybersecurity Requirements for HIPAA Covered Entities and Business Associates

by: Allen R. Killworth of Epstein Becker & Green, P.C. - *Health Law Advisor*

HISAA would provide:

- Mandatory minimum cybersecurity standards for healthcare providers.
- Annual independent cybersecurity audits.
- HHS security audits.
- Top executives certify compliance annually.
- Eliminate statutory caps on HHS fines.
- Funded by user fees.

FTC and Data Security



Contact | Stay Connected | Privacy Policy | FTC en español
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Search
ABOUT THE FTC
NEWS & EVENTS
ENFORCEMENT
POLICY
TIPS & ADVICE
I WOULD LIKE TO...
Home » News & Events » Media Resources » Protecting Consumer Privacy and Security » Privacy and Security Enforcement
Protecting Consumer Privacy and Security
FTC POLICY WORK
PRIVACY AND SECURITY ENFORCEMENT
FINANCIAL PR
KIDS' PRIVAC
BLOG POSTS
PUBLIC EVENTS

Privacy and Security Enforcement

PRIVACY AND SECURITY ENFORCEMENT

When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' pr misled them by failing to maintain security for sensitive ed the or affecting privacy

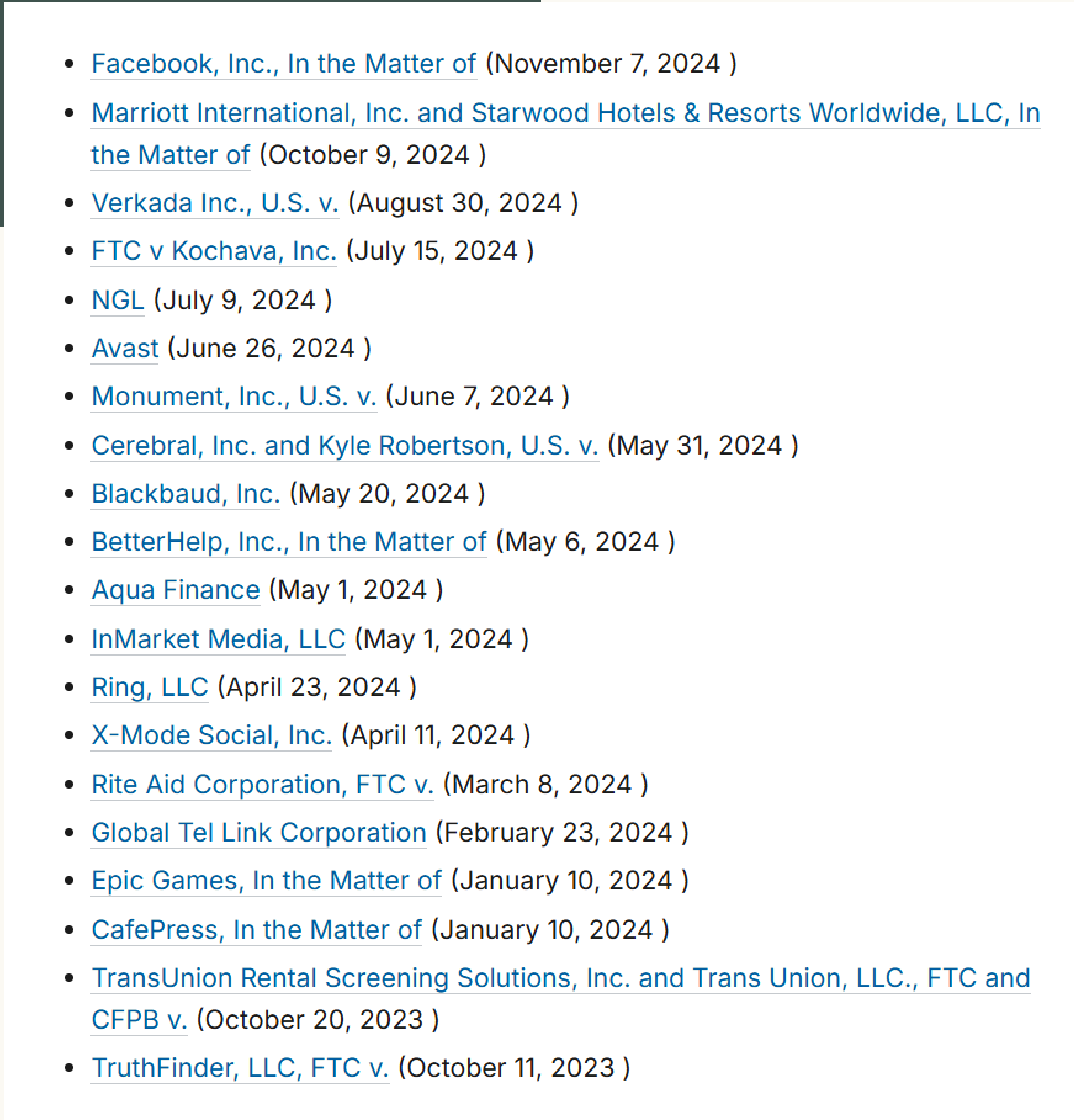
"When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information…".

FTC Enforcement of Privacy and Security

FTC is using FTCA § 5 to go after entities for data security breaches.

- Bars unfair and deceptive trade practices, e.g.,
  - Mislead consumers re security practices.
  - Misusing info or causing harm to consumers.

(https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement)



- Facebook, Inc., In the Matter of (November 7, 2024)
- Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC, In the Matter of (October 9, 2024)
- Verkada Inc., U.S. v. (August 30, 2024)
- FTC v Kochava, Inc. (July 15, 2024)
- NGL (July 9, 2024)
- Avast (June 26, 2024)
- Monument, Inc., U.S. v. (June 7, 2024)
- Cerebral, Inc. and Kyle Robertson, U.S. v. (May 31, 2024)
- Blackbaud, Inc. (May 20, 2024)
- BetterHelp, Inc., In the Matter of (May 6, 2024)
- Aqua Finance (May 1, 2024)
- InMarket Media, LLC (May 1, 2024)
- Ring, LLC (April 23, 2024)
- X-Mode Social, Inc. (April 11, 2024)
- Rite Aid Corporation, FTC v. (March 8, 2024)
- Global Tel Link Corporation (February 23, 2024)
- Epic Games, In the Matter of (January 10, 2024)
- CafePress, In the Matter of (January 10, 2024)
- TransUnion Rental Screening Solutions, Inc. and Trans Union, LLC., FTC and CFPB v. (October 20, 2023)
- TruthFinder, LLC, FTC v. (October 11, 2023)

Beware

HIPAA NOTICE OF PRIVACY PRACTICES

- Usually prepared by privacy officer or compliance.
- Must contain required terms.
- Describes permissible uses and disclosures.
- Prohibits others.

Compare

WEBSITE PRIVACY TERMS

- Often prepared by marketing, website developer or IT without considering HIPAA implications.
- May purportedly allow uses or disclosures that are not permitted by HIPAA.

FTC Health Breach Notification Rule (HBNR)

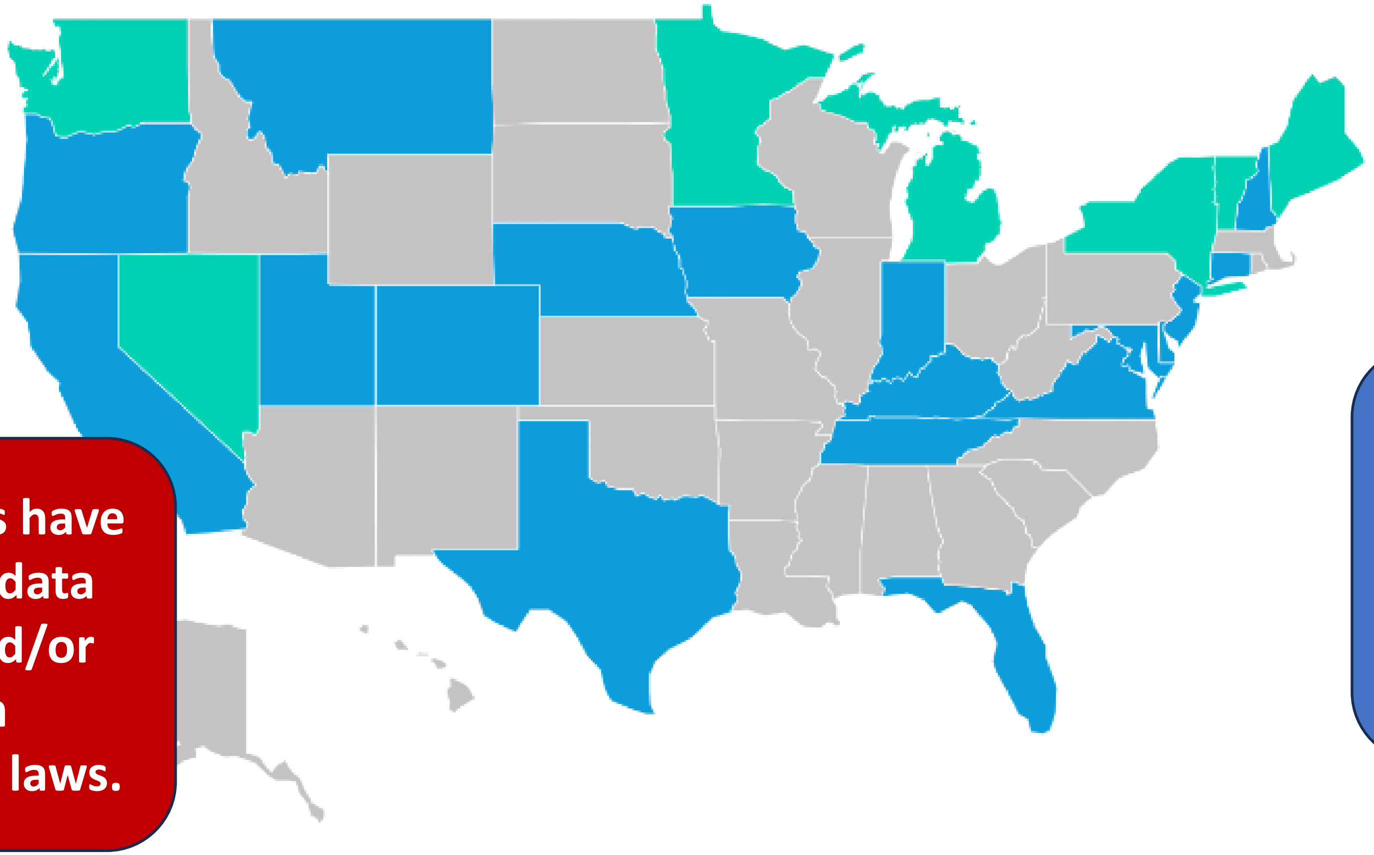
- Requires vendors of personal health info to provide notice of breach to consumers and FTC.
  - Generally, does not apply to entities covered by HIPAA (covered entities and business associates)
- Modified rule effective 7/29/24
  - Confirms HBNR applies to health apps, online services, and other technologies not covered by HIPAA.
  - "Breach of security" includes unauthorized acquisition of identifiable health info that occurs through data security breach or unauthorized disclosure.
  - Modifies required content of notice of breach.

(16 CFR part 316; 89 FR 47028)

- **GoodRx pays $1,500,000 for failing to report unauthorized disclosure of consumer health data to Facebook, Google, and others.**
- **Easy Healthcare (Premom ovulation tracking app) shared info with third parties, including AppsFlyer and Google.**

State Data Privacy Laws

U.S. states with consumer data privacy laws

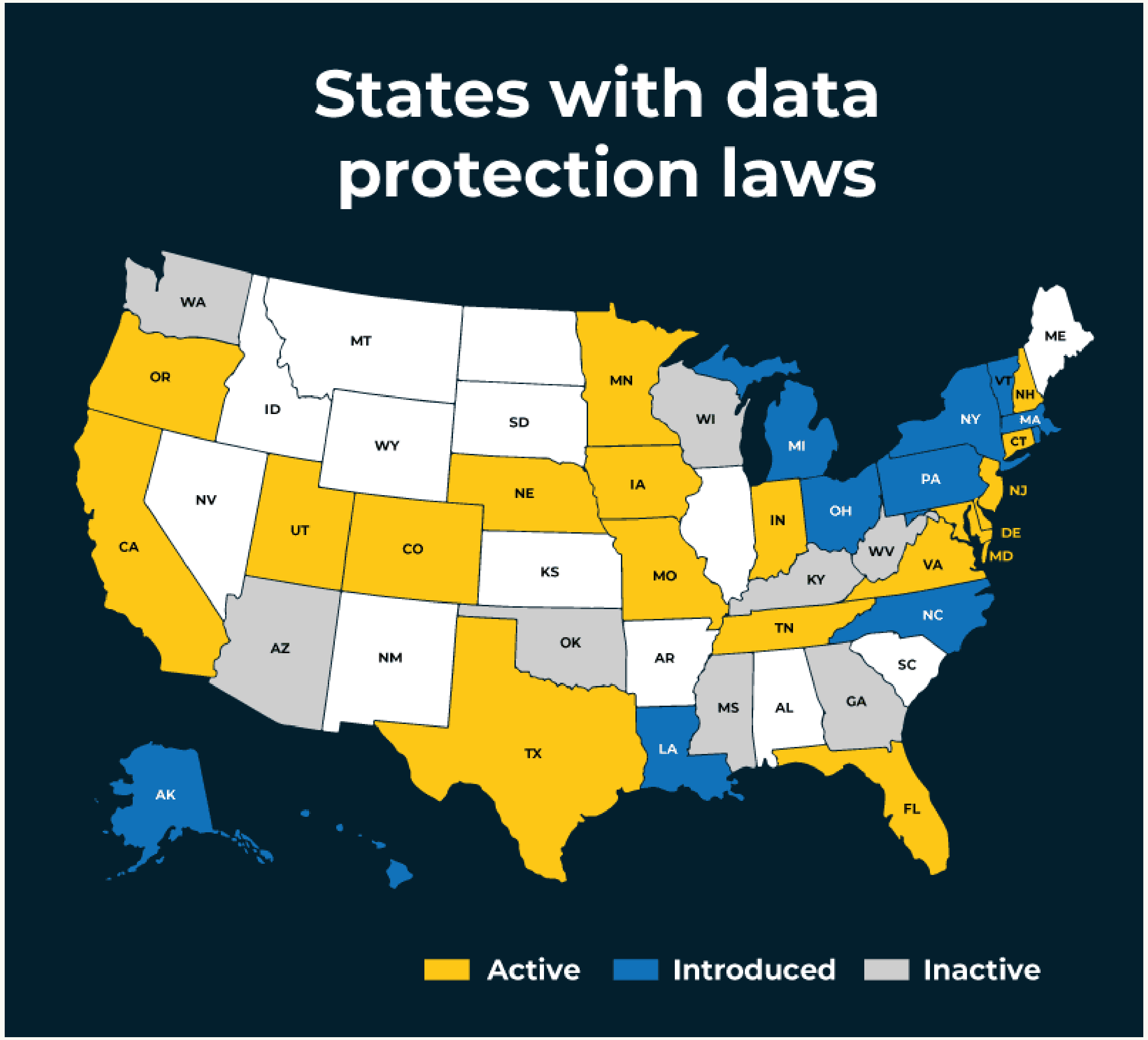


Many states have their own data privacy and/or breach notification laws.

Source: Bloomberg Law, https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#row-66725b4d4cdd5

Remember:
HIPAA requires you to comply with more restrictive law, including state laws.

State Data Privacy Laws



States with data protection laws

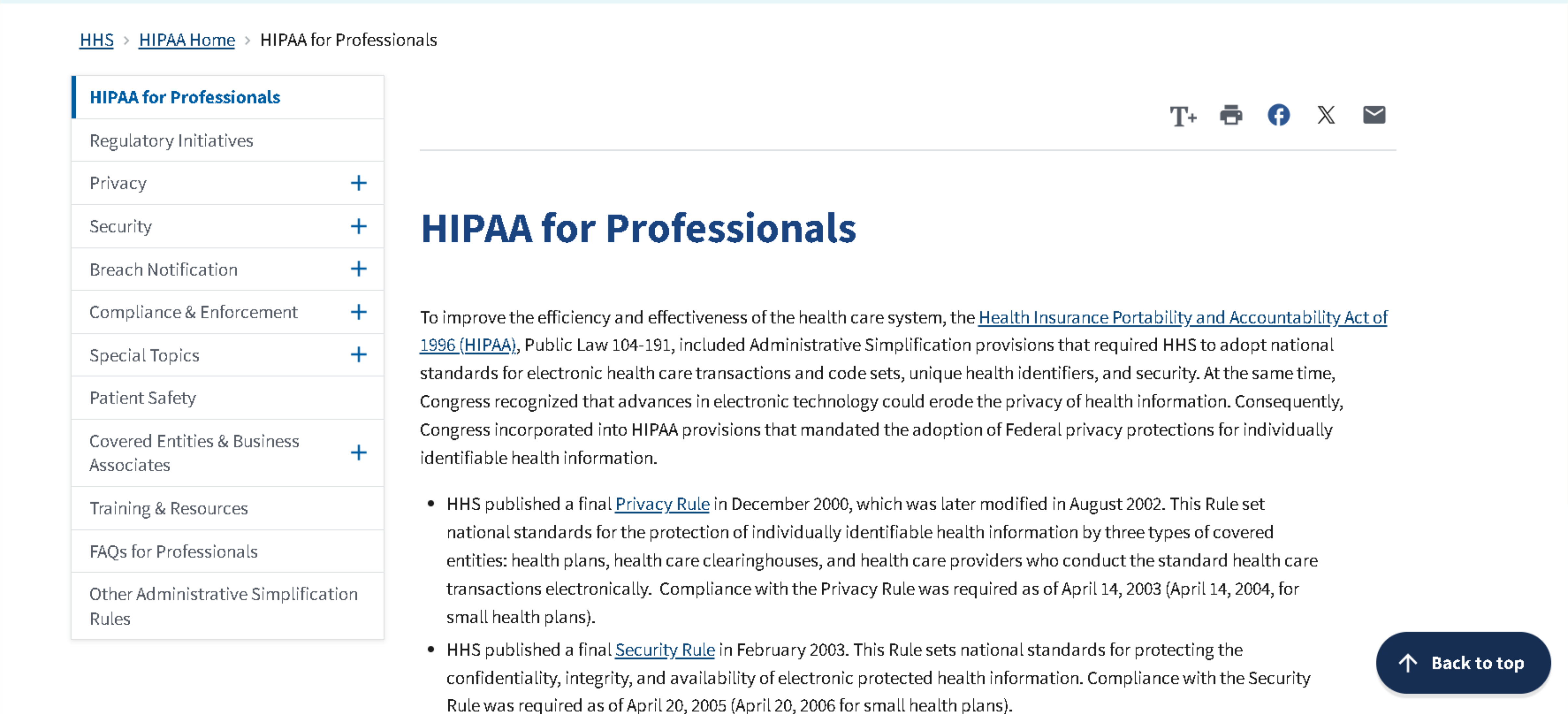
- *Beware telehealth and other situations in which you may be subject to laws in other states.*
- *Remember HIPAA requires that you comply with the most restrict laws.*

Source: https://www.securescan.com/articles/records-management/data-privacy-laws-and-compliance/

Additional Resources

OCR HIPAA Website

https://www.hhs.gov/hipaa/for-professionals/index.html

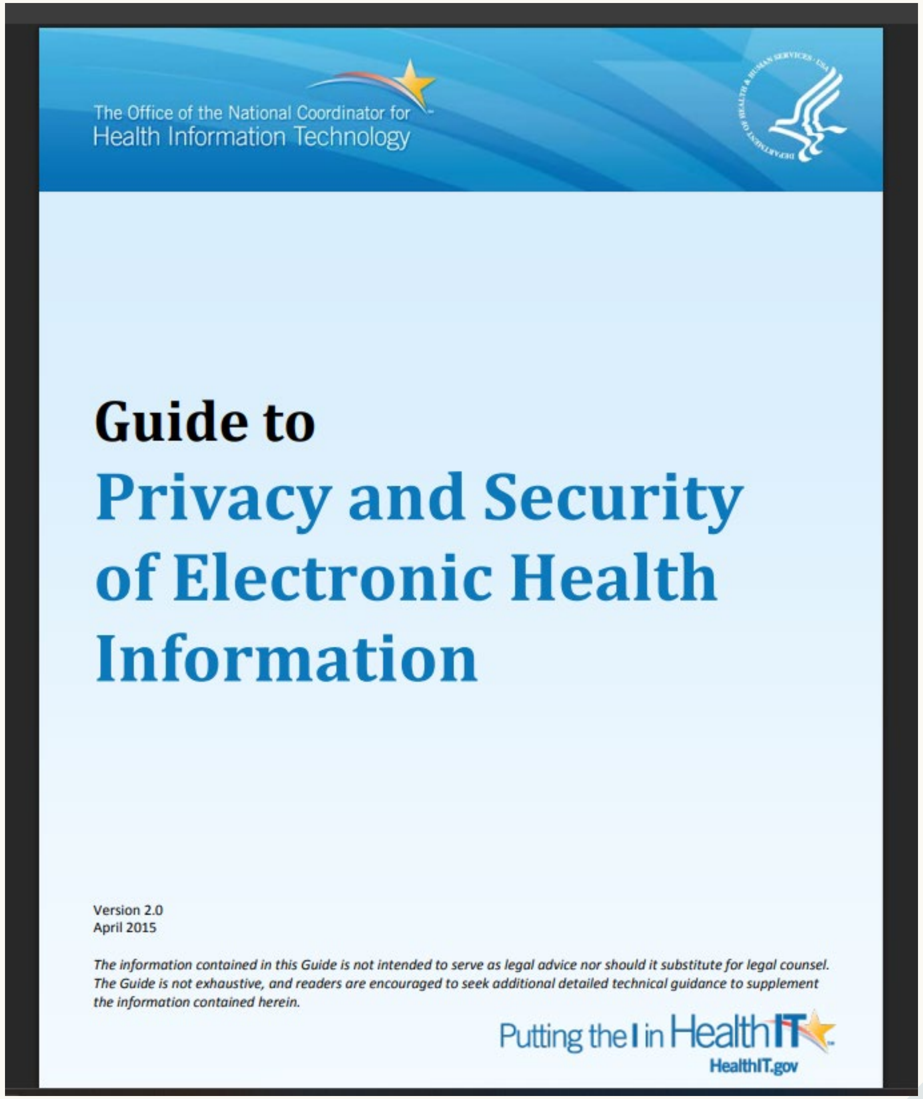


HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf



The Office of the National Coordinator for
Health Information Technology

Guide to Privacy and Security of Electronic Health Information

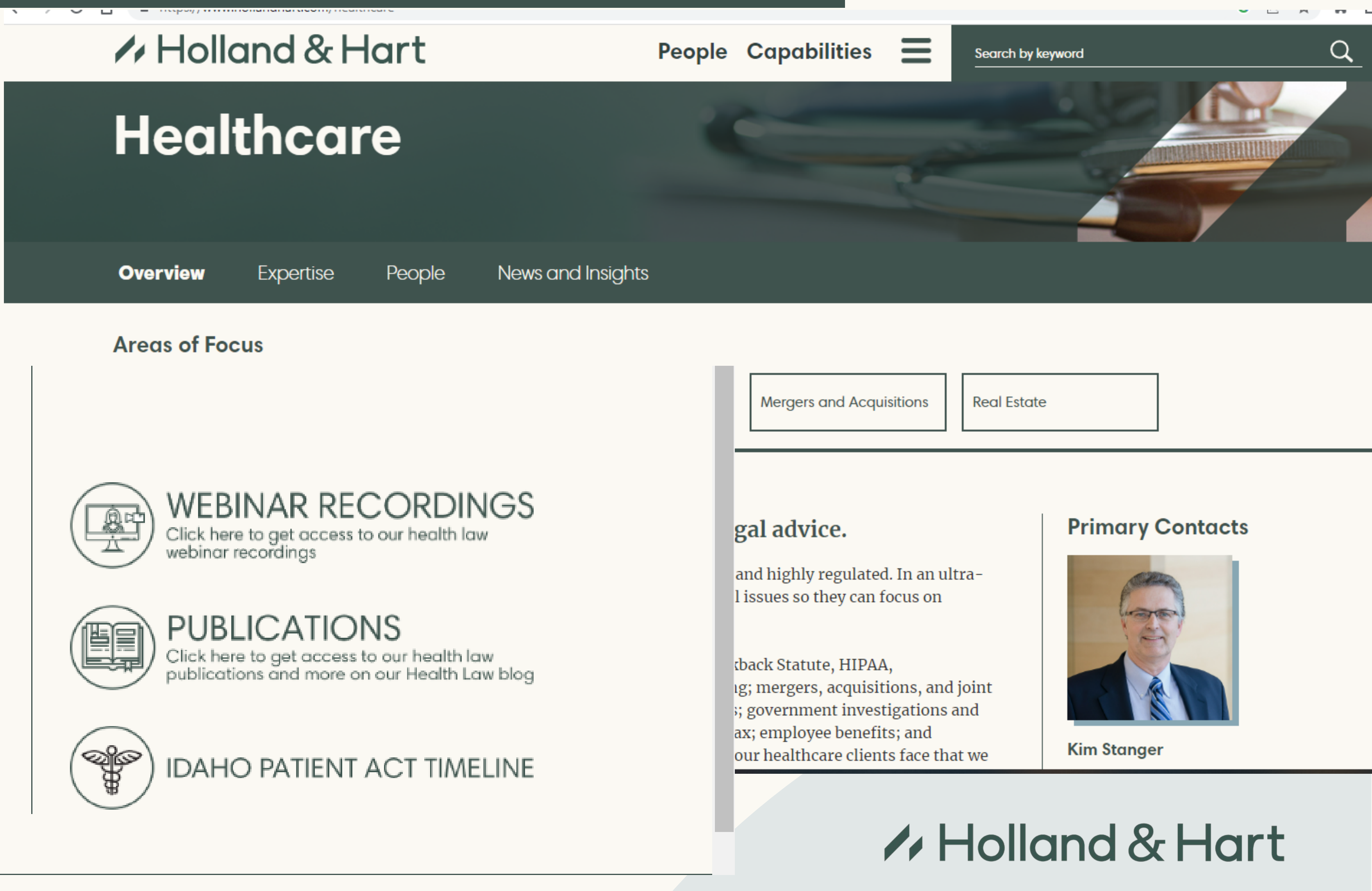
Version 2.0
April 2015

The information contained in this Guide is not intended to serve as legal advice nor should it substitute for legal counsel. The Guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in HealthIT
HealthIT.gov

HTTPS://WWW.HOLLANDHART.COM/HEALTHCARE

Free content:
- Recorded webinars
- Client alerts
- White papers
- Other



Holland & Hart

People Capabilities

Search by keyword

Healthcare

Overview Expertise People News and Insights

Areas of Focus

WEBINAR RECORDINGS
Click here to get access to our health law webinar recordings

PUBLICATIONS
Click here to get access to our health law publications and more on our Health Law blog

IDAHO PATIENT ACT TIMELINE

Mergers and Acquisitions

Real Estate

gal advice.

and highly regulated. In an ultra-
l issues so they can focus on

kback Statute, HIPAA,
ng; mergers, acquisitions, and joint
s; government investigations and
ax; employee benefits; and
our healthcare clients face that we

Primary Contacts

Kim Stanger

Holland & Hart

Questions?

Kim C. Stanger
Office: (208) 383-3913
Cell: (208) 409-7907
kcstanger@hollandhart.com