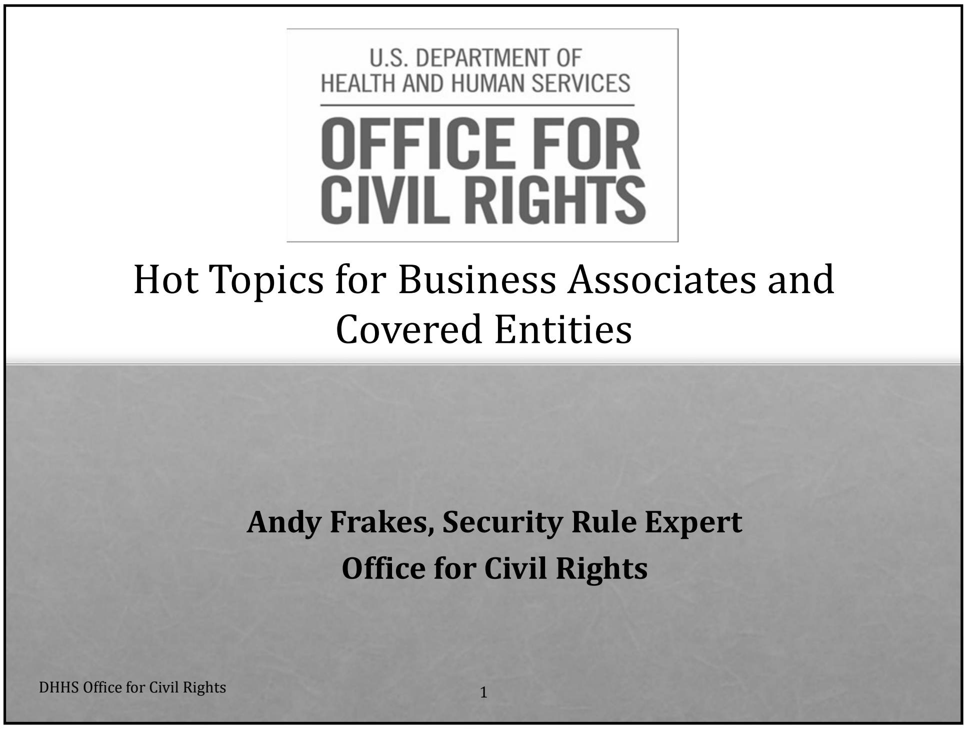


U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

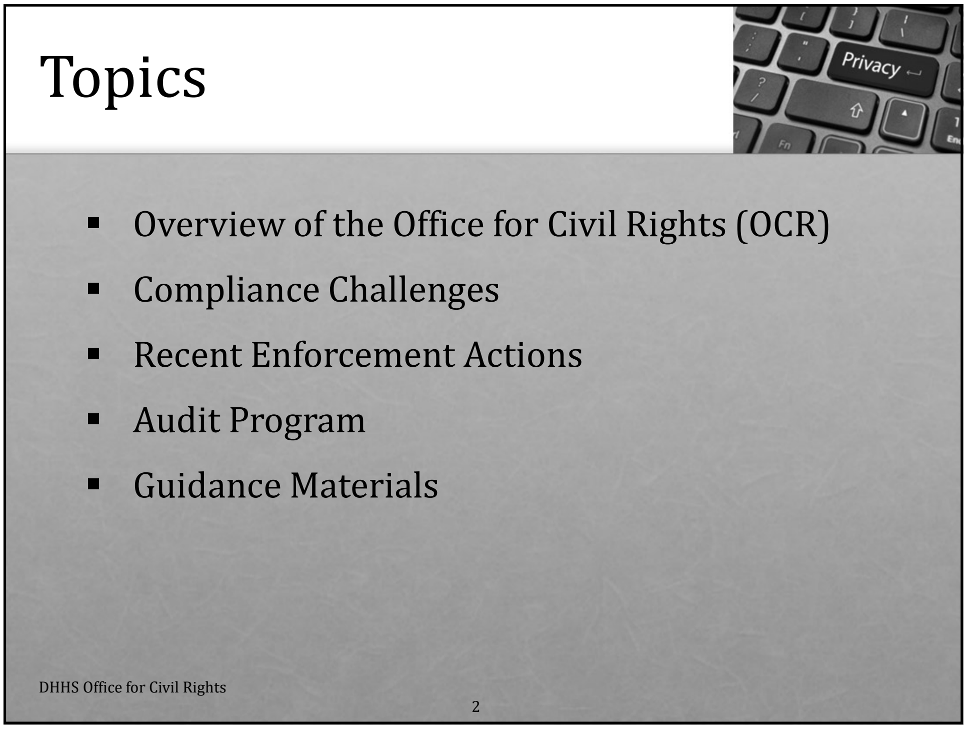
OFFICE FOR CIVIL RIGHTS

Hot Topics for Business Associates and Covered Entities

Andy Frakes, Security Rule Expert

Office for Civil Rights

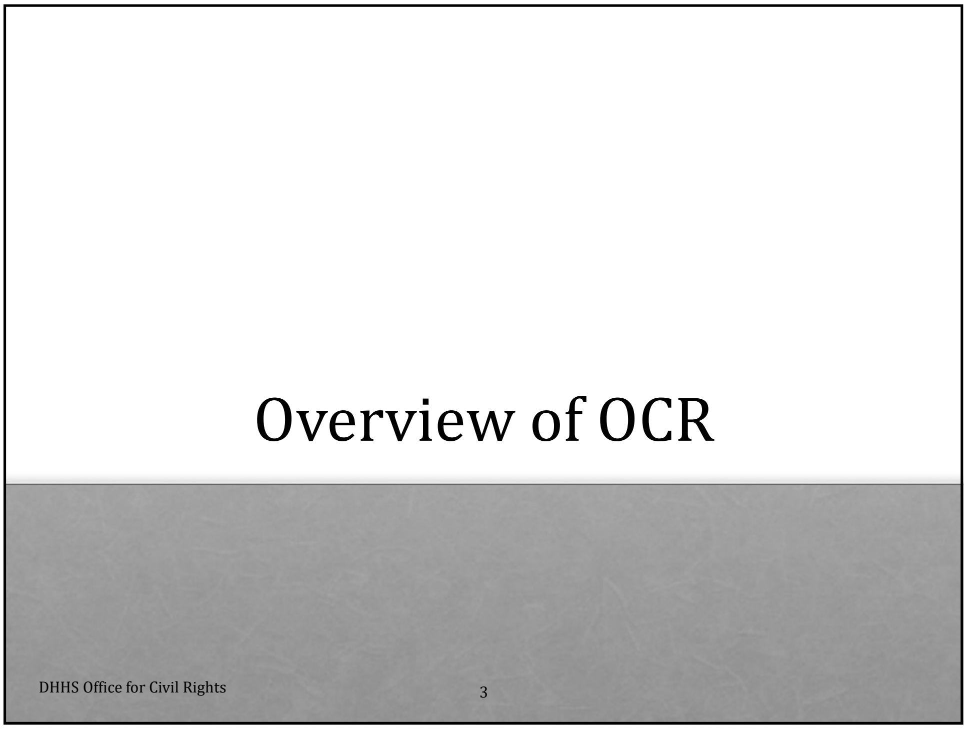
1



Topics

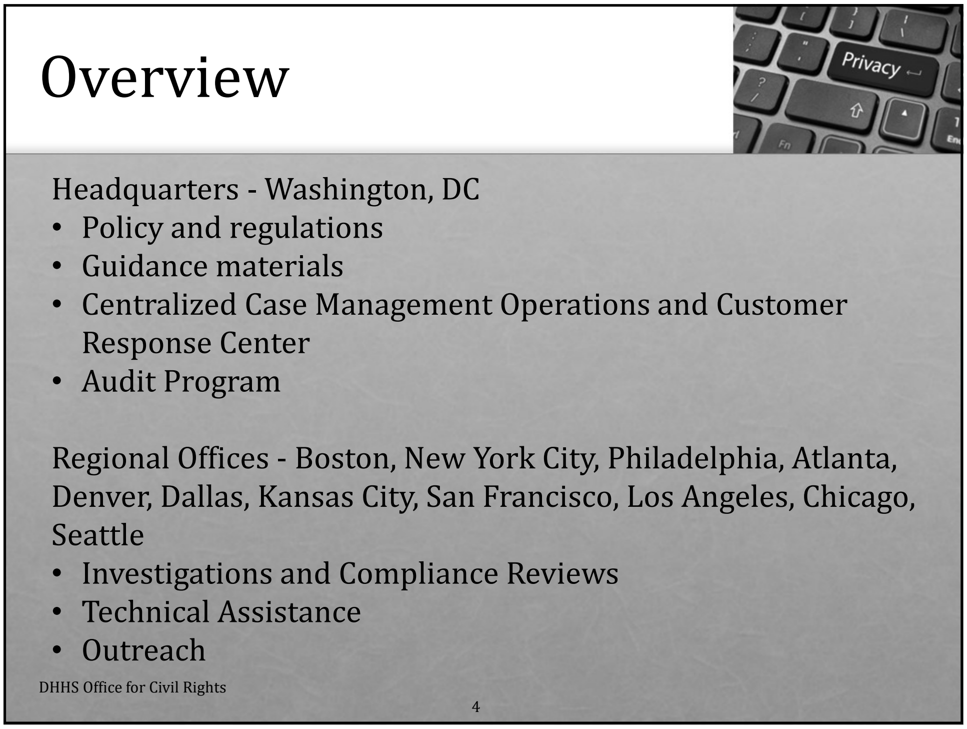
- Overview of the Office for Civil Rights (OCR)
- Compliance Challenges
- Recent Enforcement Actions
- Audit Program
- Guidance Materials

2



Overview of OCR

3



Overview

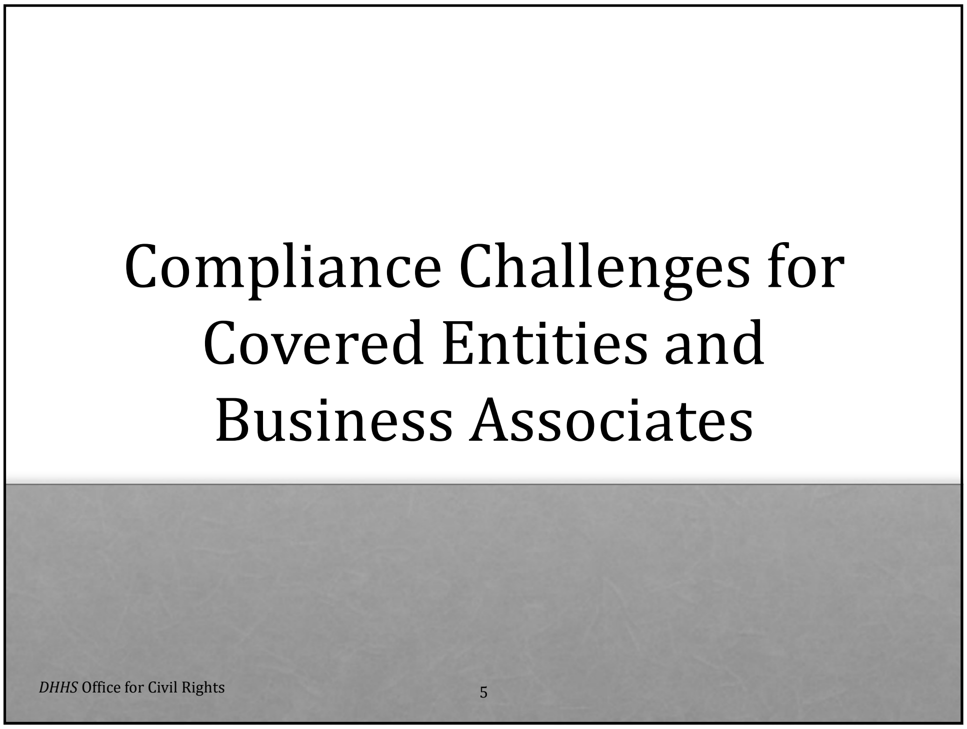
Headquarters - Washington, DC

- Policy and regulations
- Guidance materials
- Centralized Case Management Operations and Customer Response Center
- Audit Program

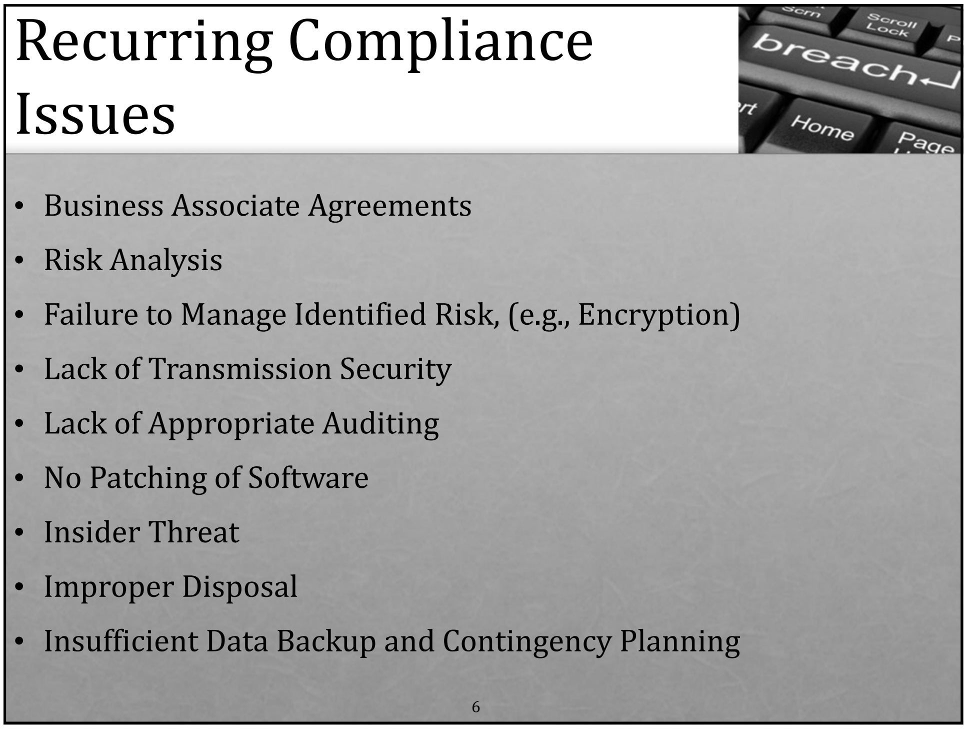
Regional Offices - Boston, New York City, Philadelphia, Atlanta, Denver, Dallas, Kansas City, San Francisco, Los Angeles, Chicago, Seattle

- Investigations and Compliance Reviews
- Technical Assistance
- Outreach

4



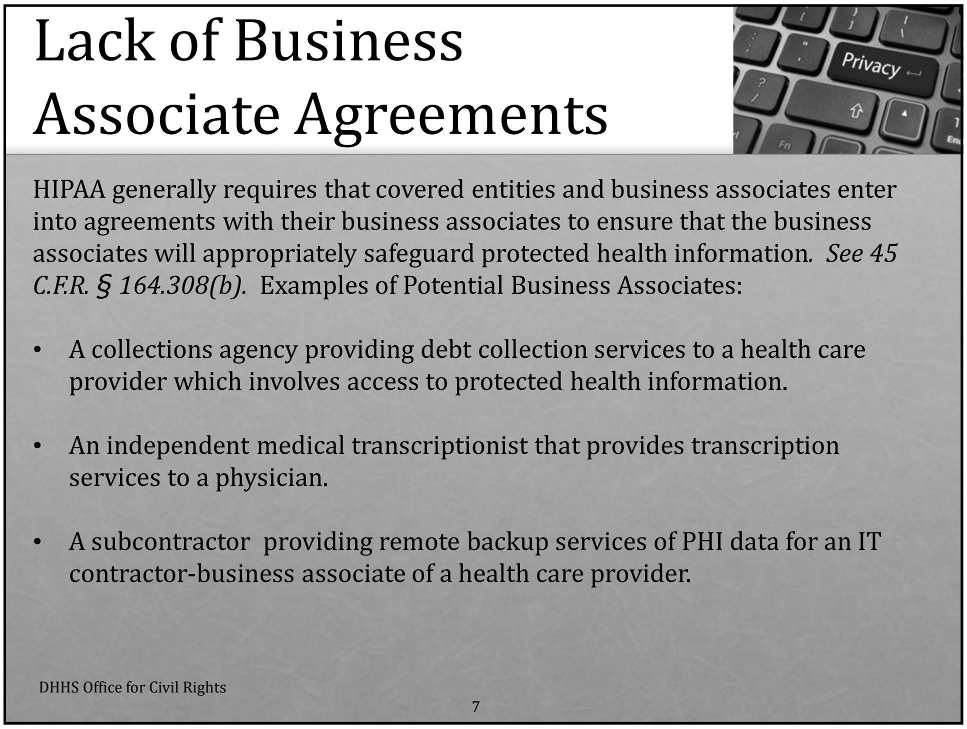
Compliance Challenges for Covered Entities and Business Associates



Scroll Lock
breach
Home
Page

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, (e.g., Encryption)
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning



Lack of Business Associate Agreements

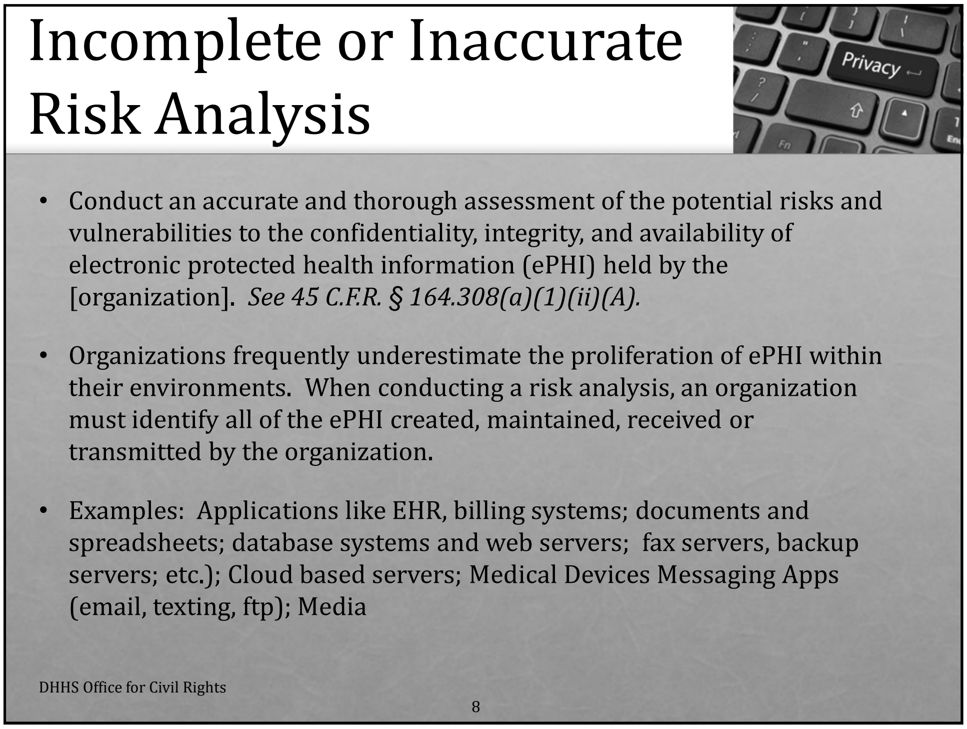
HIPAA generally requires that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information*. See 45 C.F.R. § 164.308(b).* Examples of Potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involves access to protected health information.
- An independent medical transcriptionist that provides transcription services to a physician.
- A subcontractor providing remote backup services of PHI data for an IT contractor-business associate of a health care provider.

DHHS Office for Civil Rights

7

7



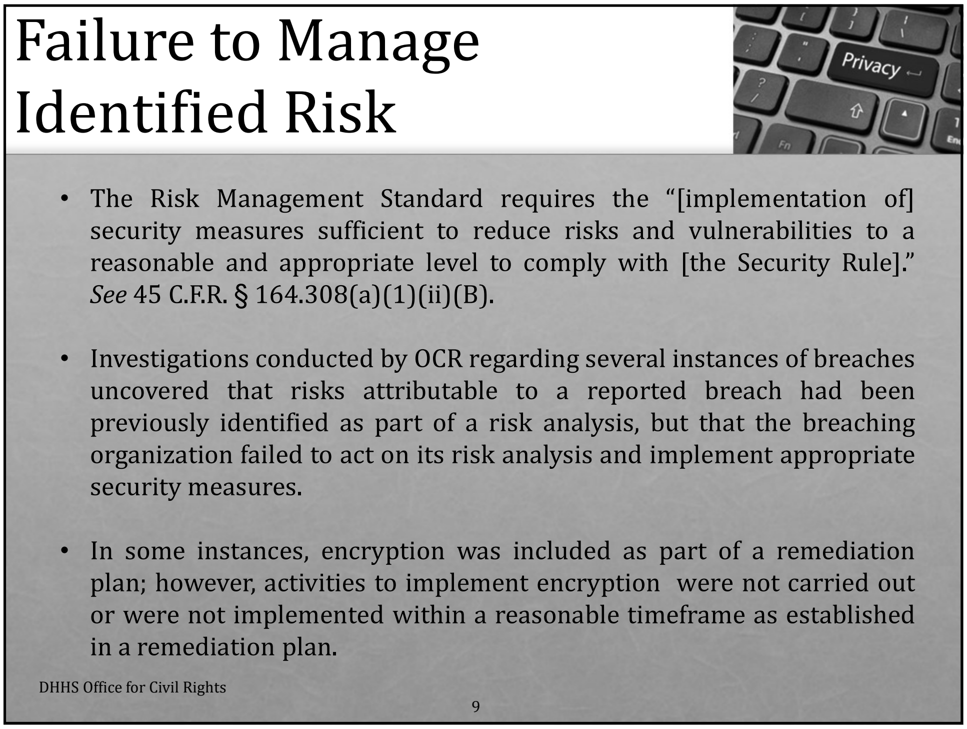
Incomplete or Inaccurate Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the [organization]. *See 45 C.F.R. § 164.308(a)(1)(ii)(A).*
- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.
- Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.); Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); Media

DHHS Office for Civil Rights

8

8



Failure to Manage Identified Risk

- The Risk Management Standard requires the "[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]." *See* 45 C.F.R. § 164.308(a)(1)(ii)(B).

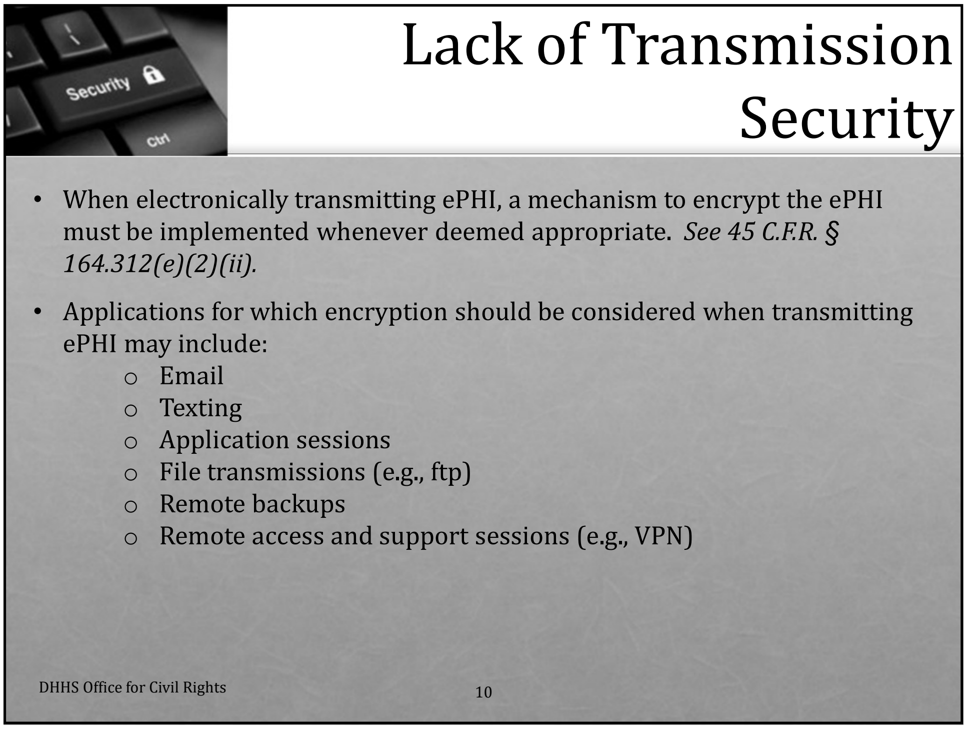
- Investigations conducted by OCR regarding several instances of breaches uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the breaching organization failed to act on its risk analysis and implement appropriate security measures.

- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.

DHHS Office for Civil Rights

9

9



Lack of Transmission Security

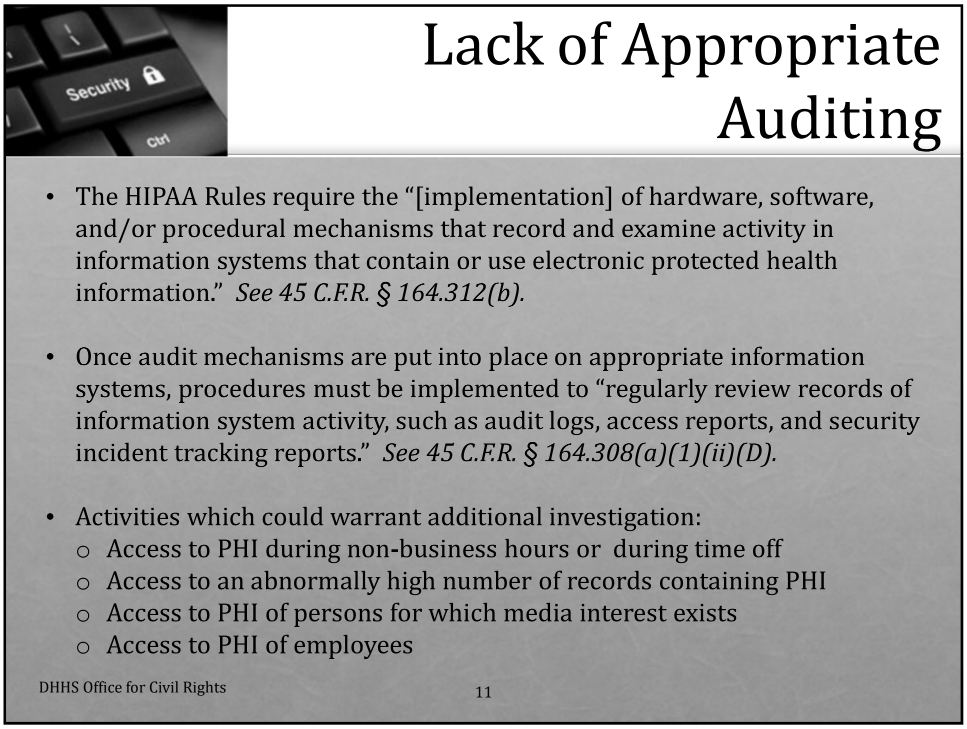
- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. *See 45 C.F.R. § 164.312(e)(2)(ii).*

- Applications for which encryption should be considered when transmitting ePHI may include:
  - o Email
  - o Texting
  - o Application sessions
  - o File transmissions (e.g., ftp)
  - o Remote backups
  - o Remote access and support sessions (e.g., VPN)

DHHS Office for Civil Rights

10

10



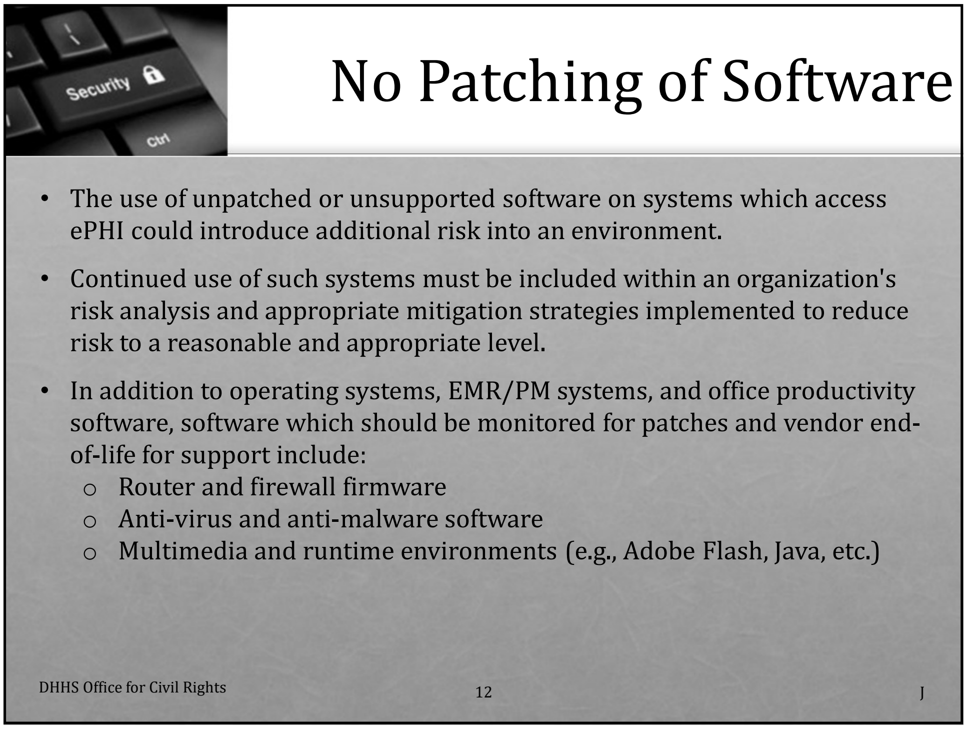
Lack of Appropriate Auditing

- The HIPAA Rules require the "[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." *See 45 C.F.R. § 164.312(b).*

- Once audit mechanisms are put into place on appropriate information systems, procedures must be implemented to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." *See 45 C.F.R. § 164.308(a)(1)(ii)(D).*

- Activities which could warrant additional investigation:
  - Access to PHI during non-business hours or during time off
  - Access to an abnormally high number of records containing PHI
  - Access to PHI of persons for which media interest exists
  - Access to PHI of employees

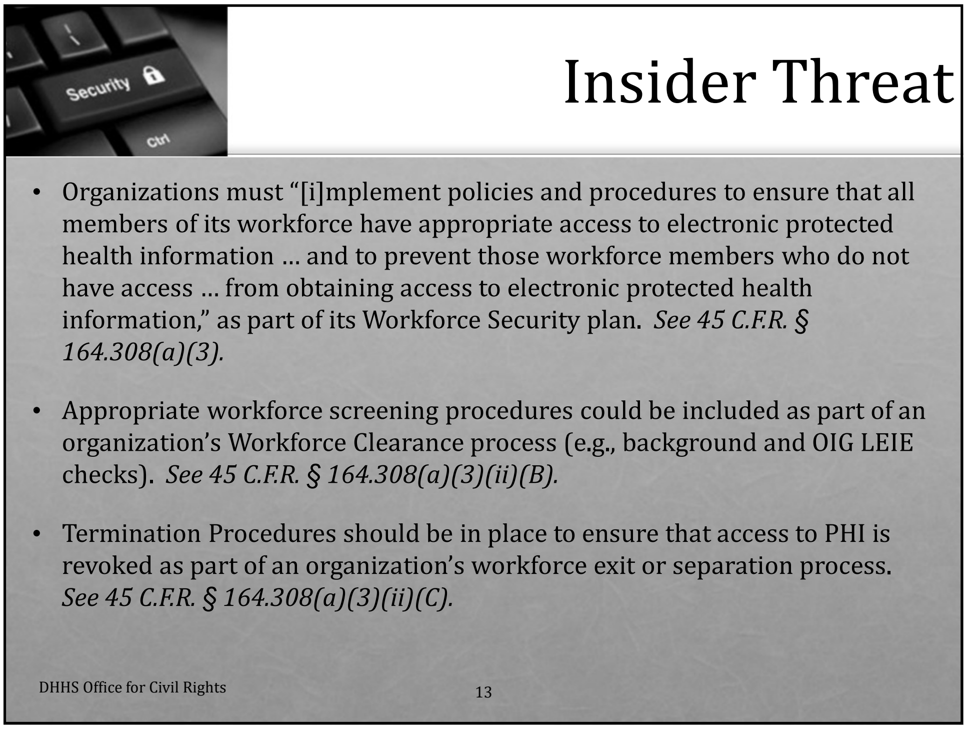
11



No Patching of Software

- The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software which should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

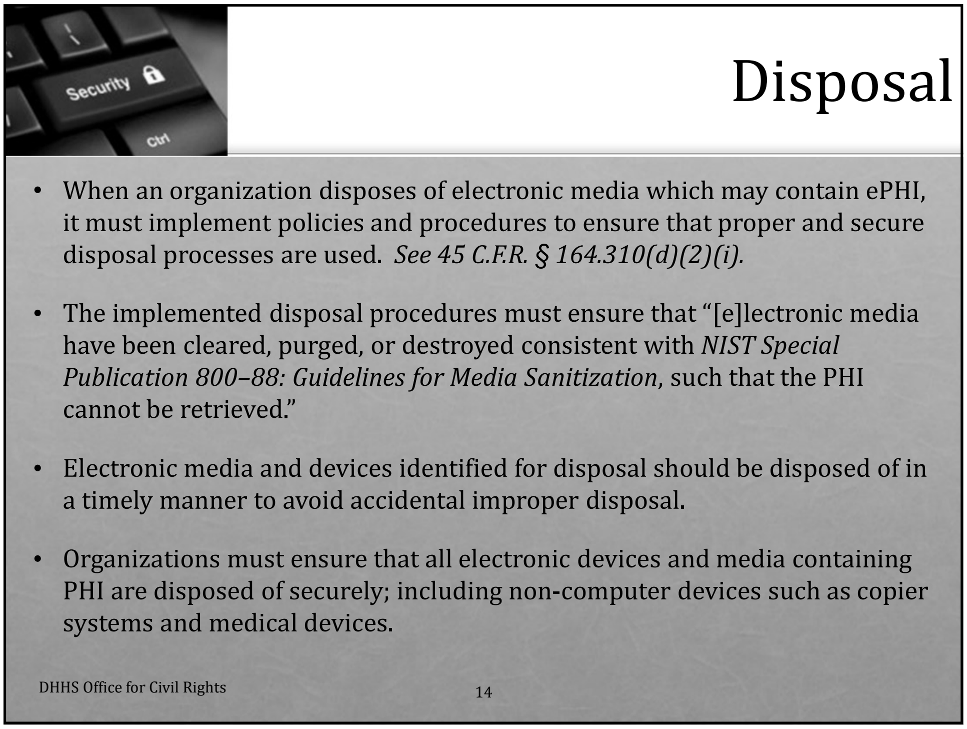
12



Insider Threat

- Organizations must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information," as part of its Workforce Security plan. *See 45 C.F.R. § 164.308(a)(3).*
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). *See 45 C.F.R. § 164.308(a)(3)(ii)(B).*
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. *See 45 C.F.R. § 164.308(a)(3)(ii)(C).*

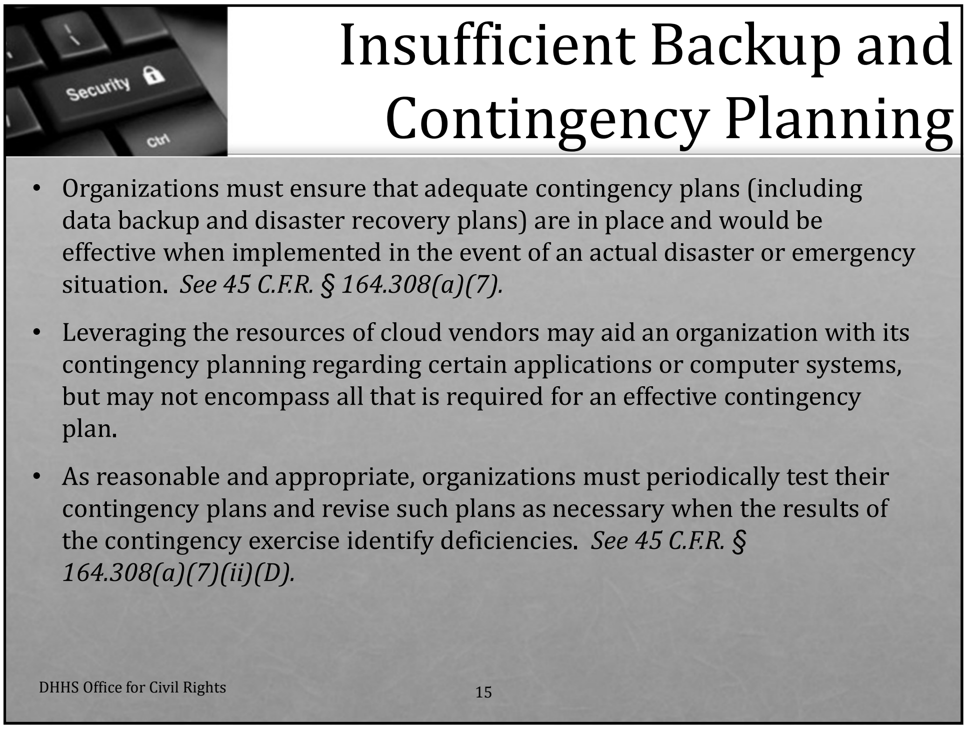
13



Disposal

- When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used. *See 45 C.F.R. § 164.310(d)(2)(i).*
- The implemented disposal procedures must ensure that "[e]lectronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800–88: Guidelines for Media Sanitization*, such that the PHI cannot be retrieved."
- Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.
- Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

14

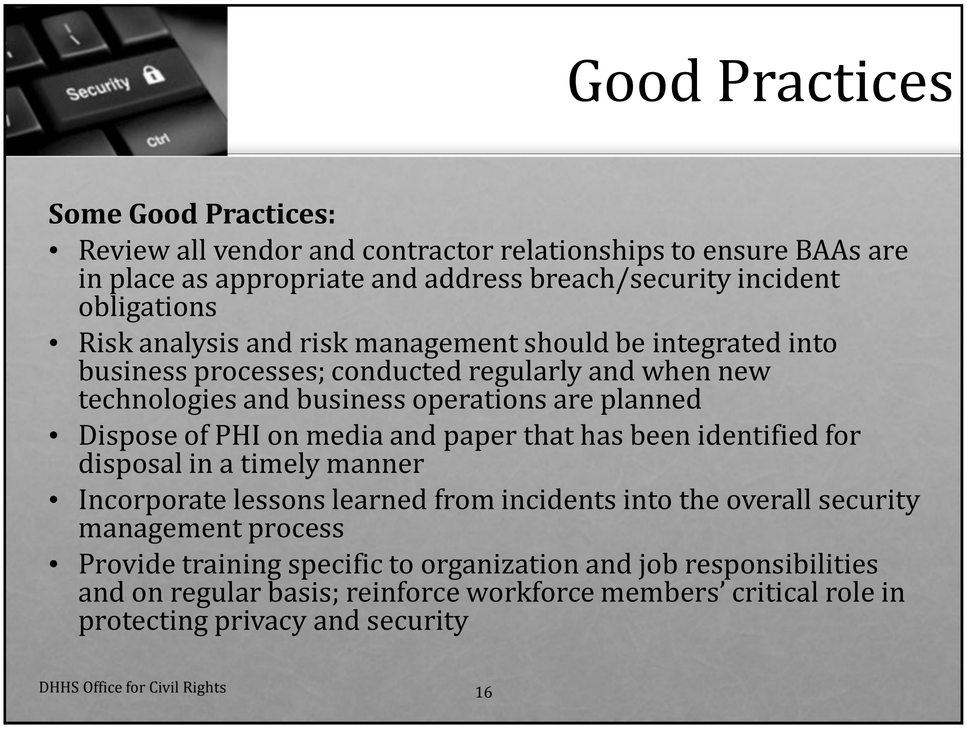


Insufficient Backup and Contingency Planning

- Organizations must ensure that adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented in the event of an actual disaster or emergency situation. *See 45 C.F.R. § 164.308(a)(7).*
- Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.
- As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies. *See 45 C.F.R. § 164.308(a)(7)(ii)(D).*

DHHS Office for Civil Rights 15

15



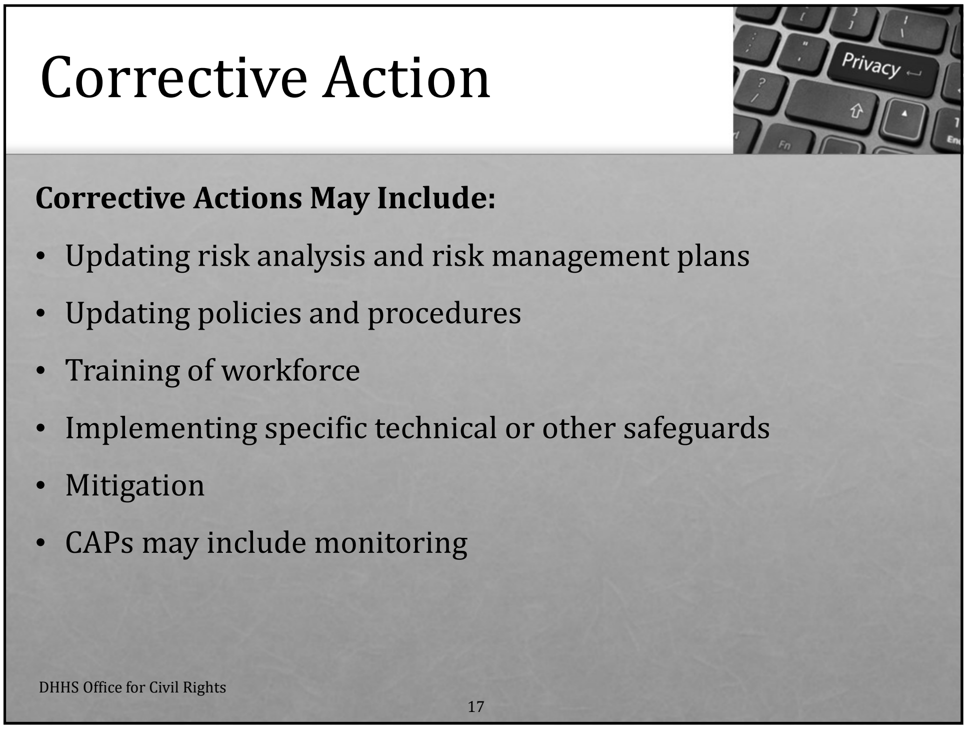
Good Practices

Some Good Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

DHHS Office for Civil Rights 16

16

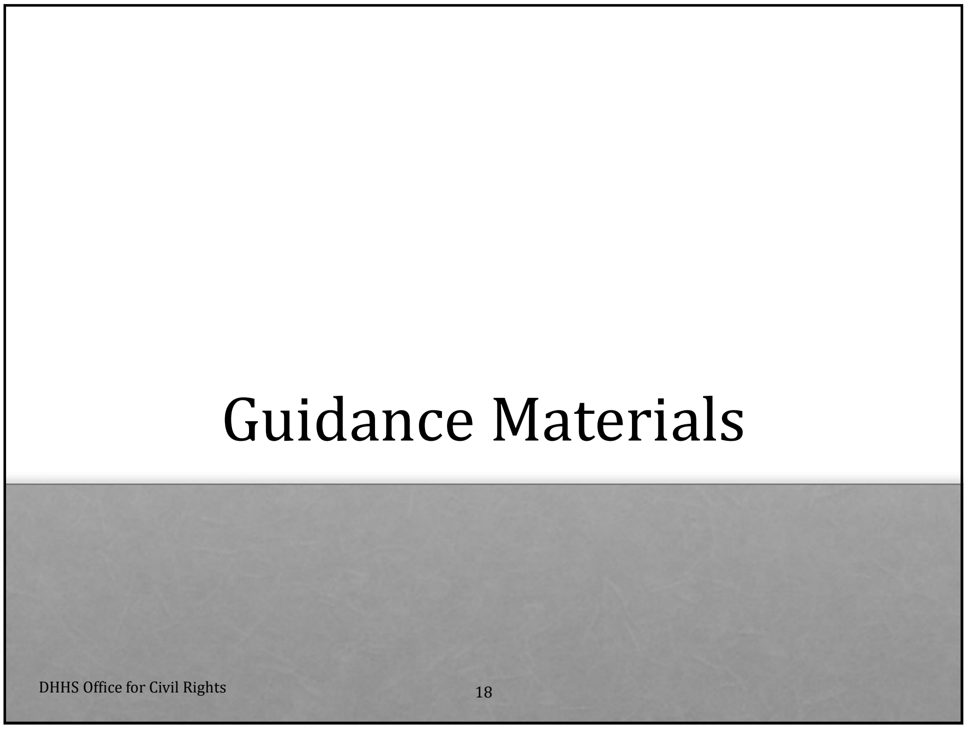


Corrective Action

Corrective Actions May Include:

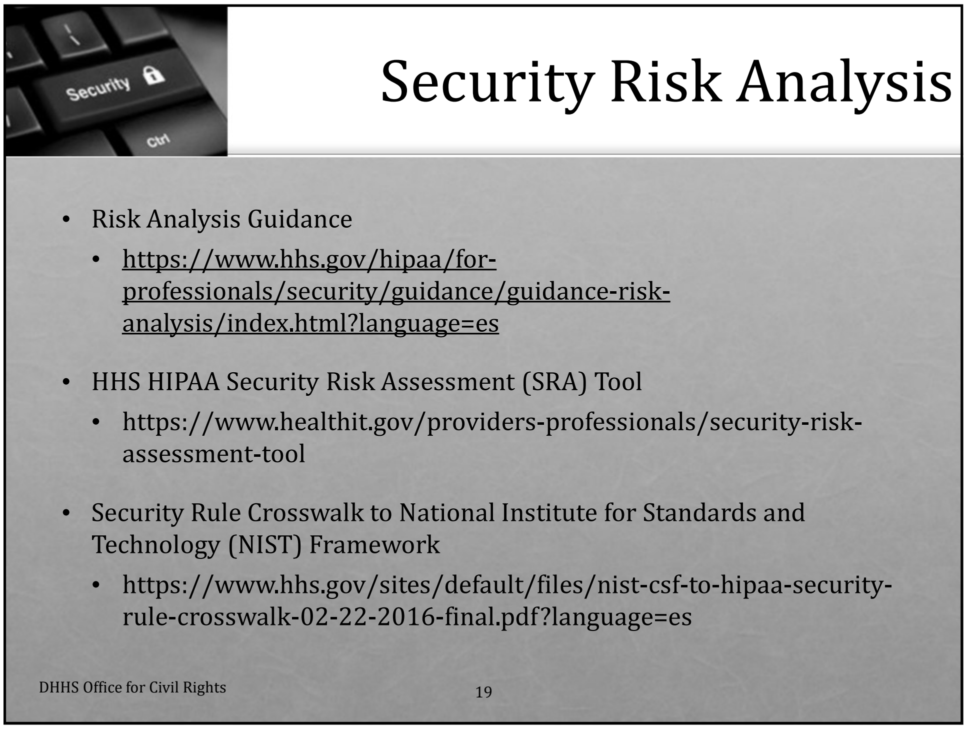
- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

17



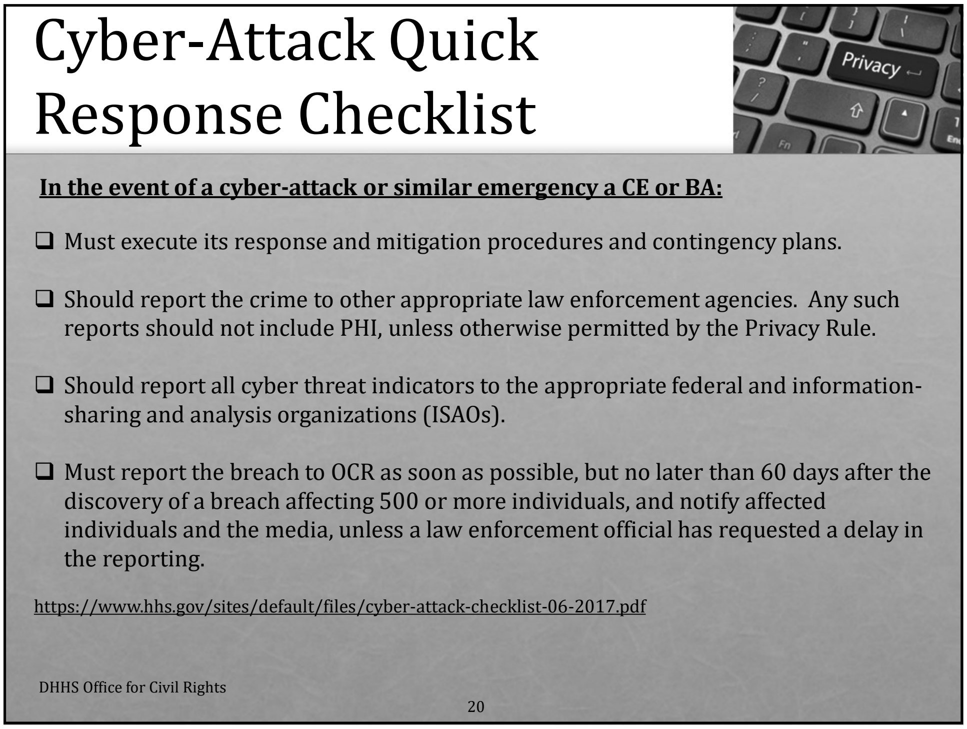
Guidance Materials

18



Security Risk Analysis

- Risk Analysis Guidance
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es
- HHS HIPAA Security Risk Assessment (SRA) Tool
  - https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- Security Rule Crosswalk to National Institute for Standards and Technology (NIST) Framework
  - https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es



Cyber-Attack Quick Response Checklist

In the event of a cyber-attack or similar emergency a CE or BA:

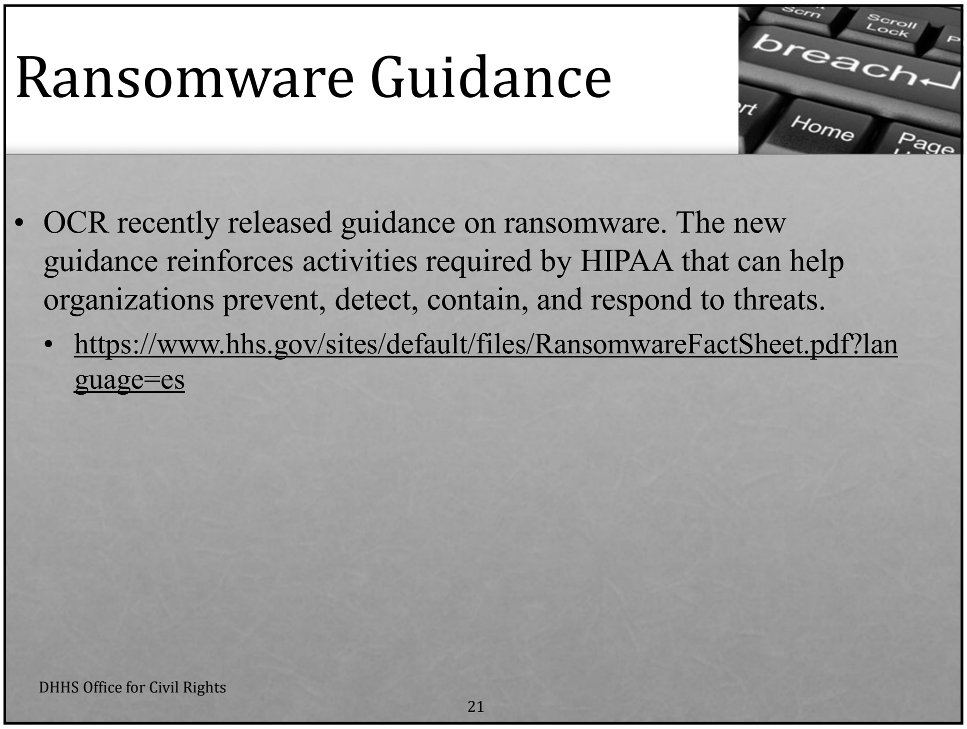
❑ Must execute its response and mitigation procedures and contingency plans.

❑ Should report the crime to other appropriate law enforcement agencies. Any such reports should not include PHI, unless otherwise permitted by the Privacy Rule.

❑ Should report all cyber threat indicators to the appropriate federal and information-sharing and analysis organizations (ISAOs).

❑ Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media, unless a law enforcement official has requested a delay in the reporting.

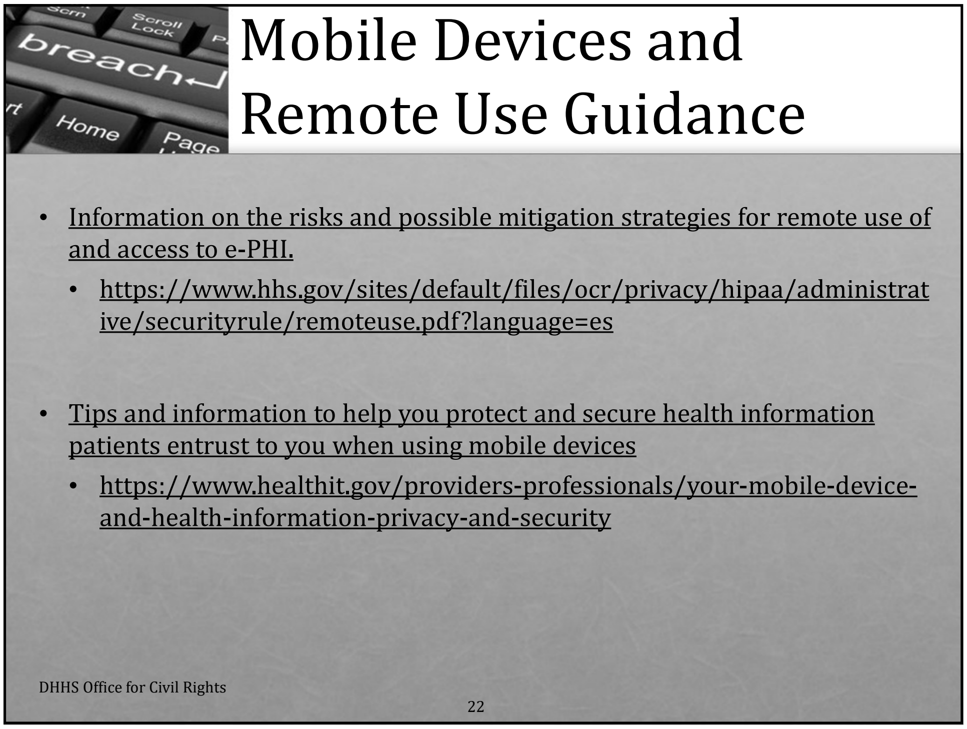
https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf



Ransomware Guidance

- OCR recently released guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
  - https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es

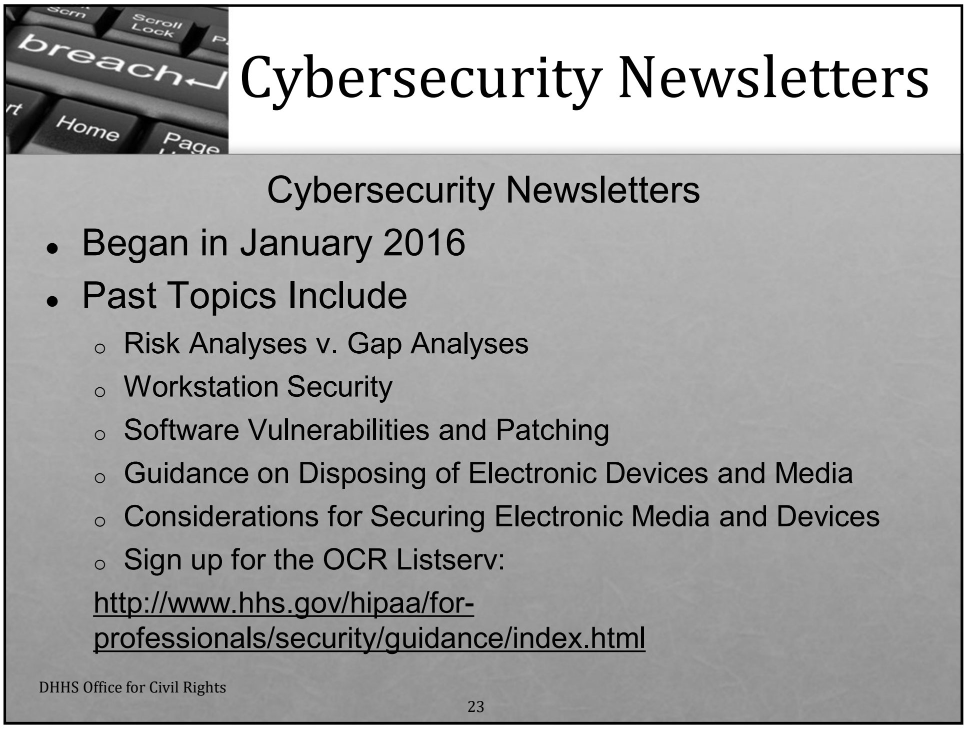
21



Mobile Devices and Remote Use Guidance

- Information on the risks and possible mitigation strategies for remote use of and access to e-PHI.
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf?language=es
- Tips and information to help you protect and secure health information patients entrust to you when using mobile devices
  - https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

22



Cybersecurity Newsletters

Cybersecurity Newsletters

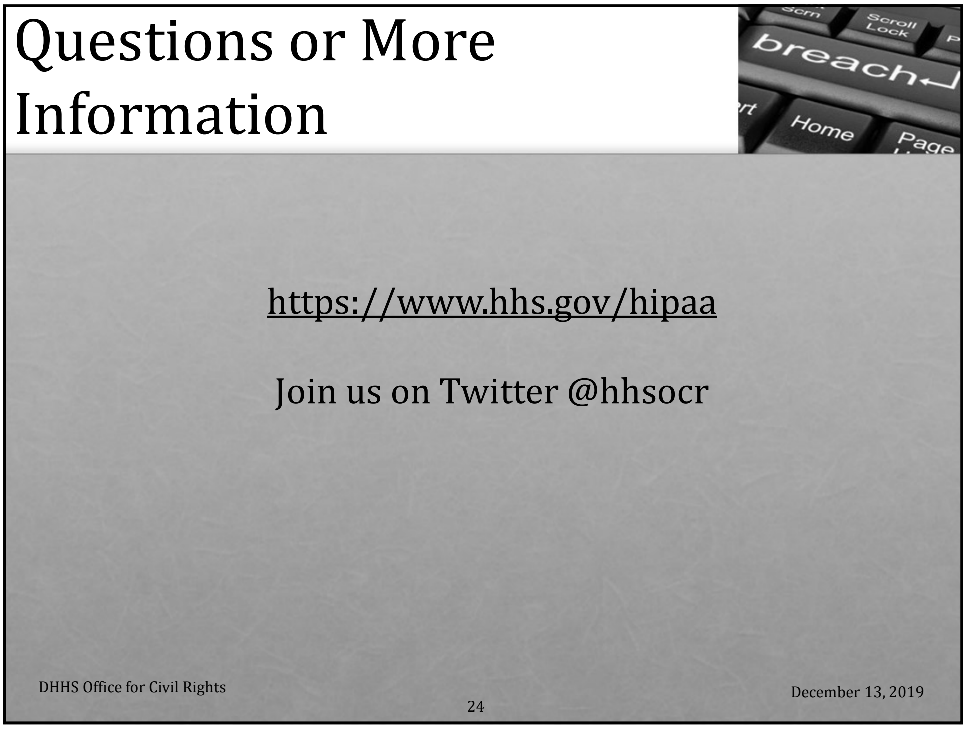
- Began in January 2016
- Past Topics Include
  - Risk Analyses v. Gap Analyses
  - Workstation Security
  - Software Vulnerabilities and Patching
  - Guidance on Disposing of Electronic Devices and Media
  - Considerations for Securing Electronic Media and Devices
  - Sign up for the OCR Listserv:

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

DHHS Office for Civil Rights

23

23



Questions or More Information

https://www.hhs.gov/hipaa

Join us on Twitter @hhsocr

DHHS Office for Civil Rights

24

December 13, 2019

24