An Update on HIPAA Policy and Enforcement

NCVHS

Rachel Seeger, MPA, MA
HHS Office for Civil Rights

May 15, 2018

HIPAA Policy Development

OCR Responds to Nation's Opioid Crisis

- Opioid abuse crisis and national health emergencies have heightened concerns about providers':

  - ability to notify patients' family and friends when a patient has overdosed

  - reluctance to share health information with patients' families in an emergency or crisis situation, particularly patients with serious mental illness and substance use disorder

  - uncertainty about HIPAA permissions for sharing information when a patient is incapacitated or presents a threat to self or others

New OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions
- New Materials for Professionals and Consumers
  - Fact Sheets for patients, families, and health care providers
  - Information-sharing Decision Charts

Dangerous Patients and Public Safety Disclosures

- Disclosures are permitted without the patient's authorization or permission to law enforcement, family, friends or others who are in a position to lessen the threatened harm—when disclosure "is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others."

- Disclosures must be consistent with applicable law.

Where to Find OCR's New Materials

- For professionals: https://www.hhs.gov/hipaa/for-professionals/index.html > Special Topics > Mental Health & Substance Use Disorders

- For consumers: https://www.hhs.gov/hipaa/for-individuals/index.html > Mental Health & Substance Use Disorders

- Mental Health FAQ Database: https://www.hhs.gov/hipaa/for professionals/faq/mental-health

- Future FERPA and HIPAA Joint Guidance

# Proposed Changes to HIPAA Privacy and Enforcement Rules

- NPRM on Presumption of Good Faith of Health Care Providers

- NPRM on Changing Requirement to Obtain Acknowledgment of Receipt of Notice of Privacy Practices

- Request for Information on Distribution of a Percentage of Civil Monetary Penalties or Monetary Settlements to Harmed Individuals

Future HIPAA Guidance

- Texting

- Social Media

- Encryption

RECENT HIPAA ENFORCEMENT AND BREACH HIGHLIGHTS

HIPAA Enforcement Highlights
April 14, 2003 – January 31, 2018

- Over 175,534 complaints received to date

- Over 25,742 cases resolved with corrective action and/or technical assistance

- Expect to receive 24,000 complaints this year

Enforcement, cont.

- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action during the investigation

- In some cases though, the nature or scope of indicated noncompliance warrants additional enforcement action

- Resolution Agreements/Corrective Action Plans

- 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts

- 3 civil money penalties

HIPAA Enforcement since April 2017

4/12/2017	Metro Community Provider Network	$400,000
4/21/2017	Center for Children's Digestive Health	$31,000
4/21/2017	CardioNet	$2,500,000
5/10/2017	Memorial Hermann Health System	$2,400,000
5/23/2017	St. Luke's-Roosevelt Hospital Center	$387,200
12/28/2017	21st Century Oncology	$2,300,000
2/1/2018	Fresenius Medical Care North America	$3,500,000
2/13/2018	FileFax	$100,000

Total $11,618,200

HIPAA Resolution Agreements and Civil Monetary Penalties
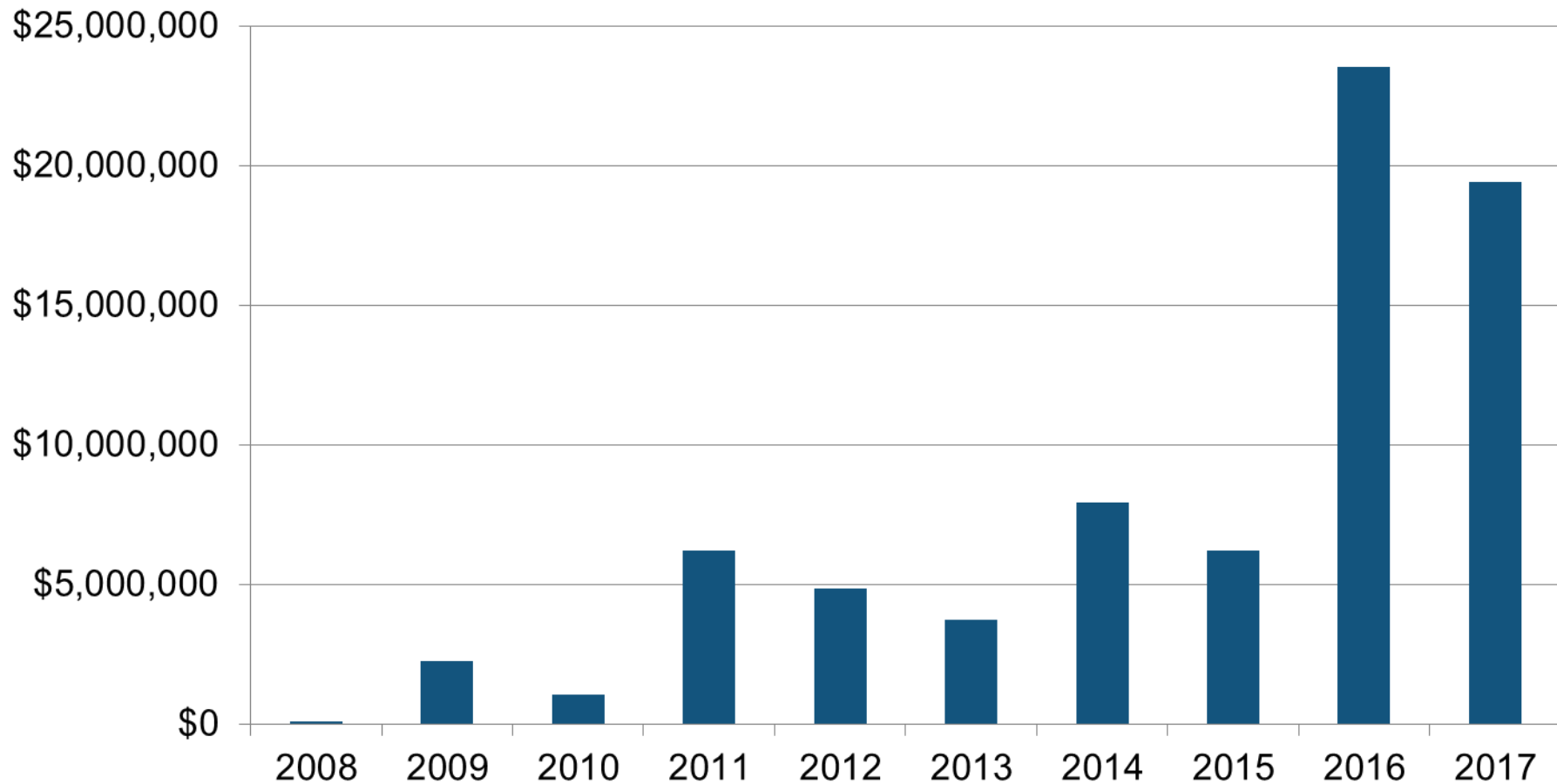
50 settlement agreements and 3 civil money penalties through 2017

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

New HIPAA Breach Reporting Tool

- The revised web tool still publicly reports all breaches involving 500 or more records – but presents that information in a more understandable way.

- The HBRT also features improved navigation for both those looking for information on breaches and ease-of-use for organizations reporting incidents.

- The tool helps educate industry on the types of breaches that are occurring, industry-wide or within particular sectors, and how breaches are commonly resolved following investigations launched by OCR, which can help industry improve the security posture of their organizations.

Key Improvements

Indicates active cases under investigation within last 24 months

Help for consumers provides tools on identity theft

Archive tab takes users to OCR's database of all breach cases

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

# Advanced Search Functions

Latest Breach Reporting Highlights

September 2009 through February 28, 2018

- Approximately 2,222 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 46% of large breaches
  - Hacking/IT now account for 19% of incidents
  - Laptops and other portable storage devices account for 25% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 177,298,024

- Approximately 341,002 reports of breaches of PHI affecting fewer than 500 individuals

500+ Breaches by Type of Breach from September 2009 through February 28, 2018

Pie chart:
- Theft 38%
- Unauthorized Access/Disclosure 28%
- Hacking/IT 19%
- Loss 8%
- Other 4%
- Improper Disposal 3%
- Unknown 1%
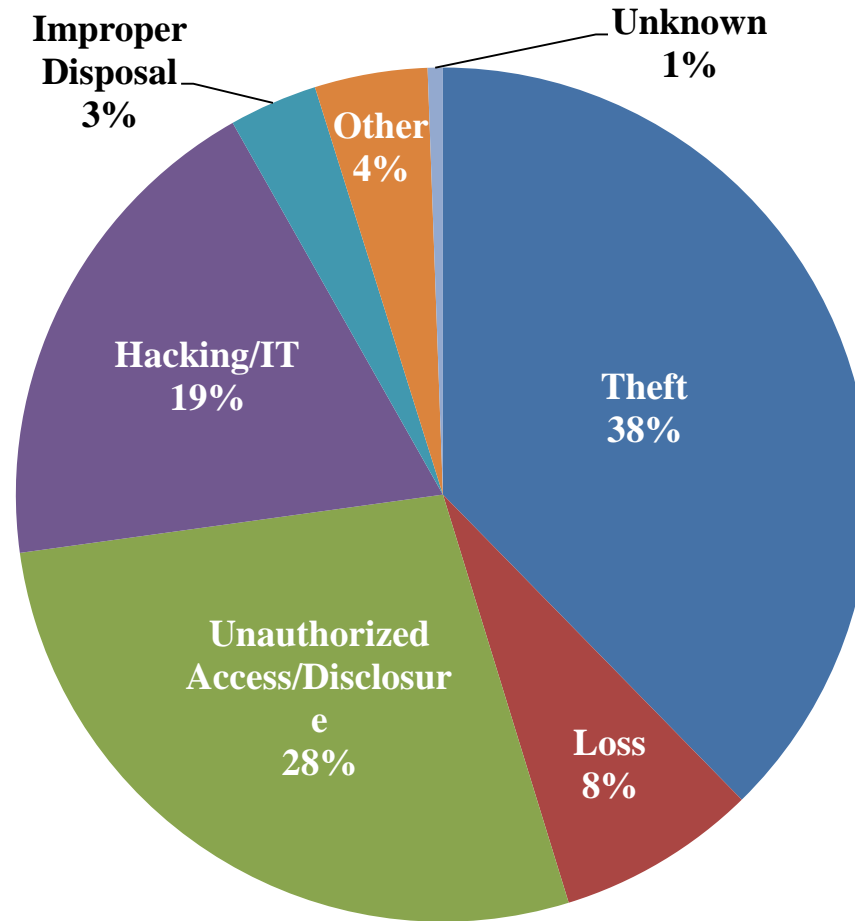
500+ Breaches by Type of Breach from March 1, 2015 – February 28, 2018
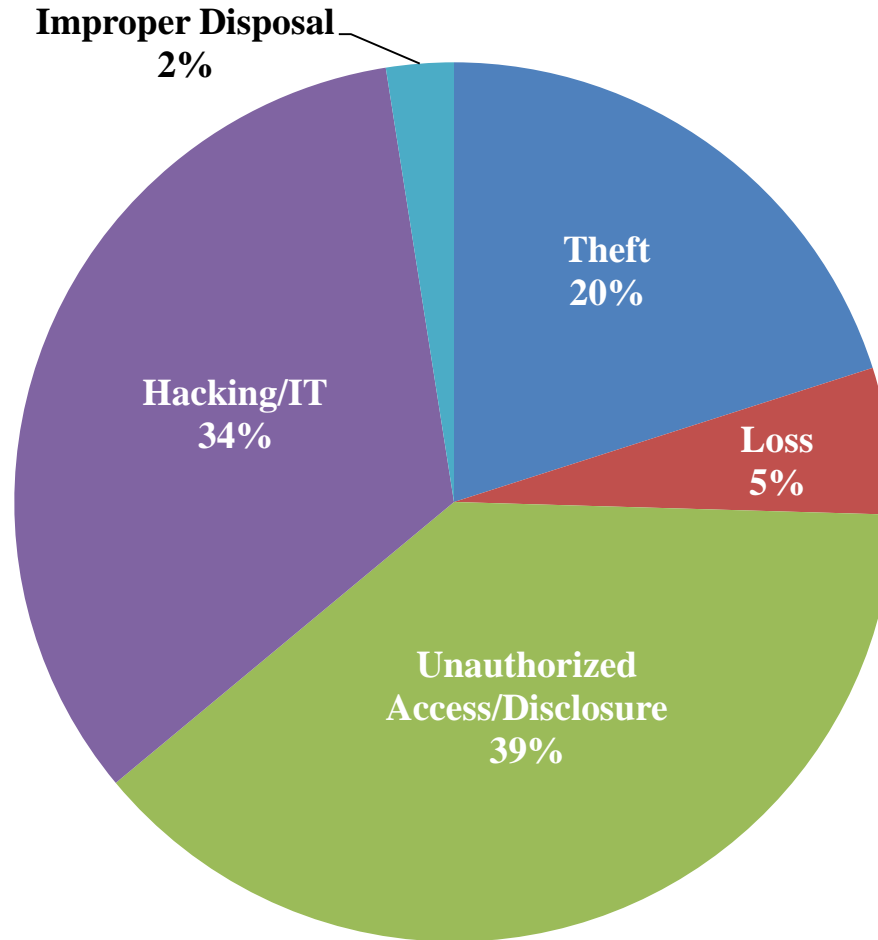
Improper Disposal
2%

Theft
20%

Loss
5%

Hacking/IT
34%

Unauthorized
Access/Disclosure
39%

500+ Breaches by Location of Breach from September 2009 through January 31, 2018

Pie chart: 500+ Breaches by Location of Breach

- Paper Records 21%
- Desktop Computer 10%
- Laptop 16%
- Portable Electronic Device 9%
- Network Server 17%
- Email 11%
- EMR 6%
- Other 10%

500+ Breaches by Location of Breach from September 2009 through January 31, 2018

Pie chart: Breaches by Location of Breach
- Paper Records 21%
- Desktop Computer 8%
- Laptop 9%
- Portable Electronic Device 6%
- Network Server 22%
- Email 16%
- EMR 9%
- Other 9%
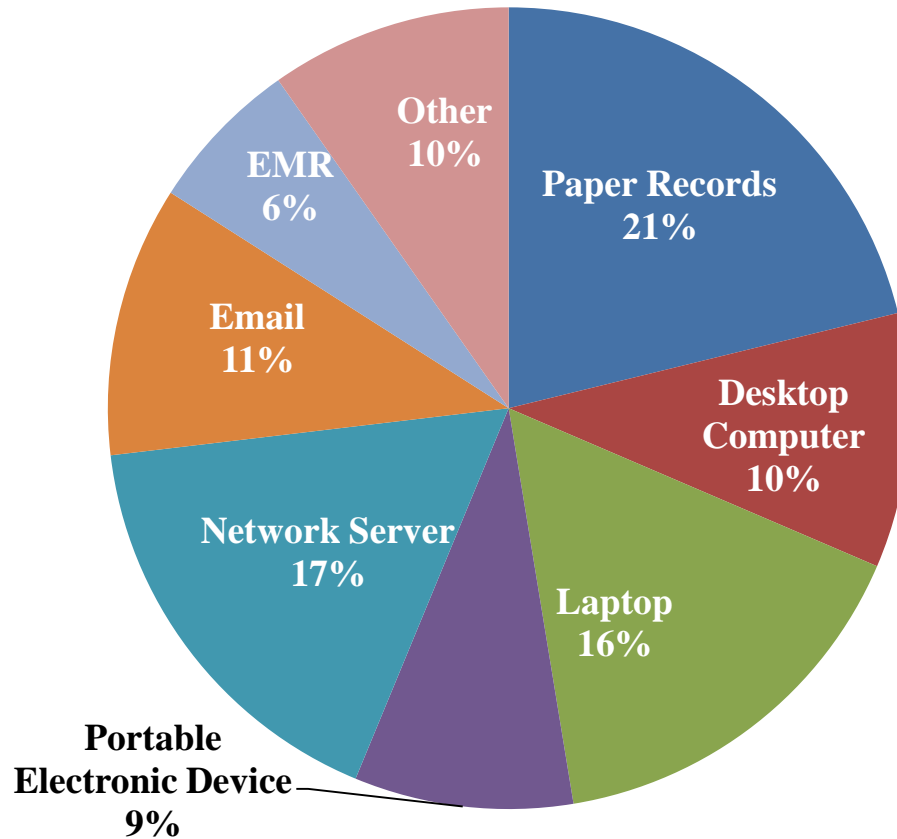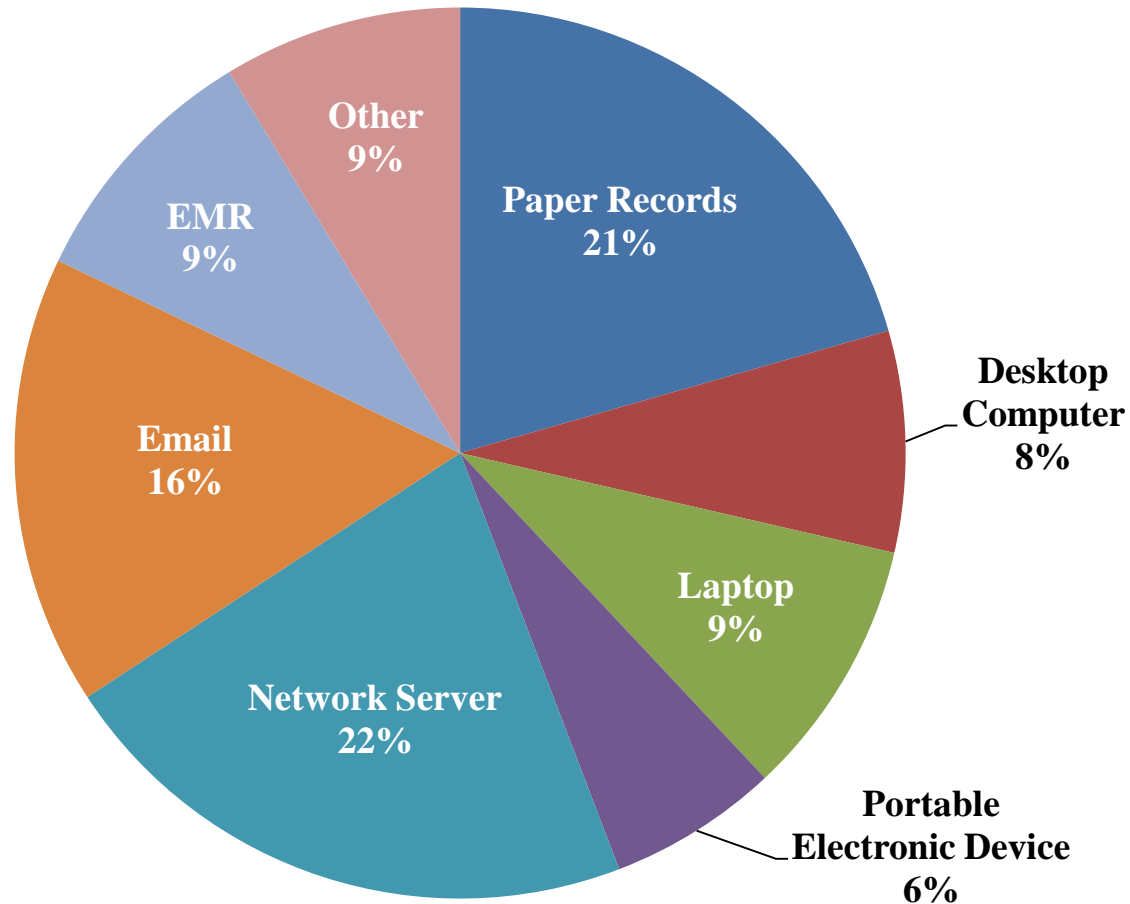
Cyber Security Guidance Material
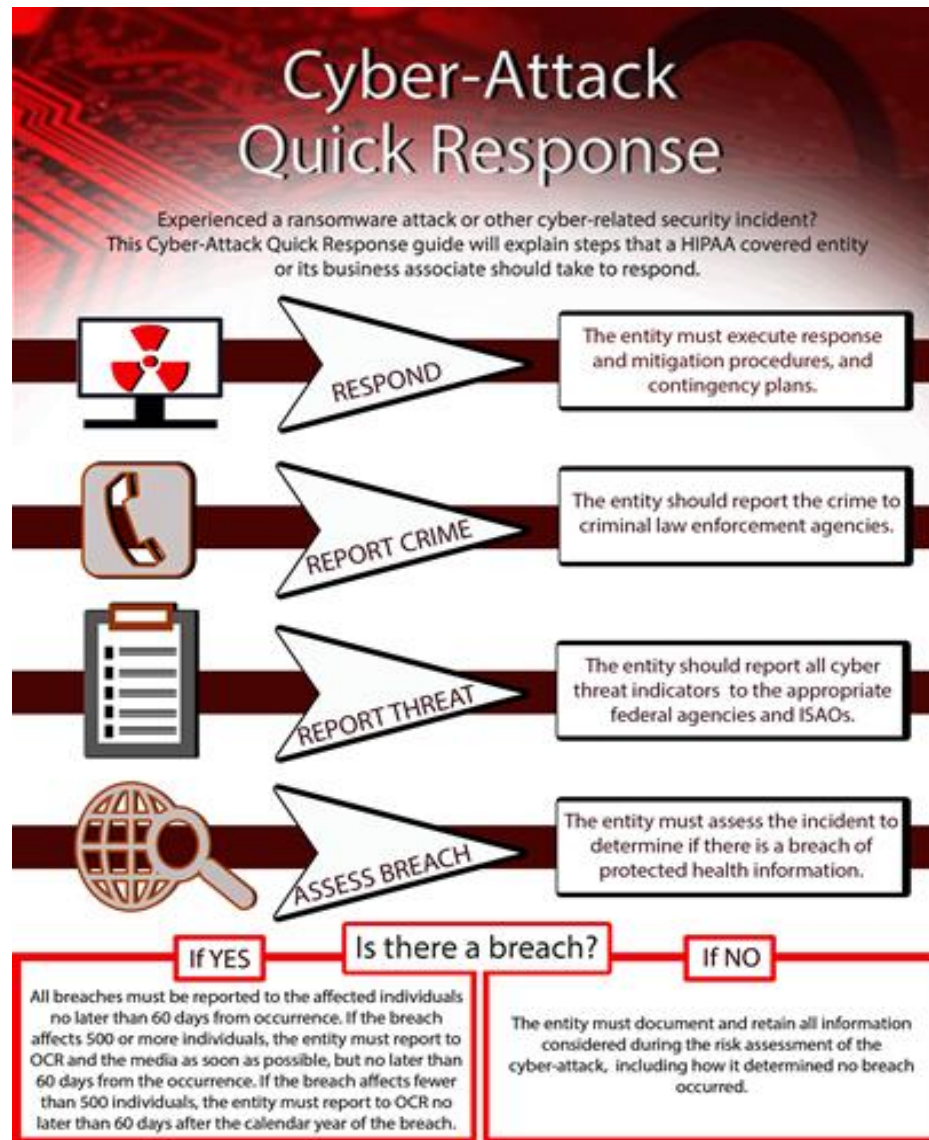
Ransomware

- Following the May 2017 WannaCry ransomware attack, HHS reminded organizations to adhere to the OCR ransomware guidance as part of strong cyber hygiene.

- OCR presumes a breach in the case of a ransomware attack.

FACT SHEET: Ransomware and HIPAA

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

"Maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack."

Cybersecurity Resources

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

- Health Information Technology Portal http://hipaaQsportal.hhs.gov

- Medscape
  http://www.medscape.org/viewarticle/876110

For More Information

http://www.hhs.gov/hipaa

Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/

Find us on Twitter @hhsocr