

# RECENT HIPAA ENFORCEMENT: KEY ISSUES TO CONSIDER



KIM C. STANGER

(11-20)

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.

# WRITTEN MATERIALS

- .ppts slides
- Articles:
  - *HIPAA Enforcement: Lessons from the OCR's Recent Settlements*
  - *Complying With HIPAA: A Checklist for Covered Entities*
    - *HIPAA Security Policy Checklist*
    - *HIPAA Privacy Policy Checklist*
  - *Encrypt Your Devices or Face HIPAA Penalties*
  - *Disclosing Employee's COVID-19 Status to Employer*
  - *HIPAA, E-mails, and Texts to Patients or Others*
  - *Checklist for HIPAA Business Associate Agreements*
  - *HIPAA Breach Notification: When and How to Self-Report*
  - *Others*

Available at <https://www.hollandhart.com/healthcare>.

# QUESTIONS

- Submit using chat feature, or
- Contact me offline at [kcstanger@hollandhart.com](mailto:kcstanger@hollandhart.com).

# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (“HIPAA”)

- 45 CFR 164
  - .500: Privacy Rule (2003)
  - .300: Security Rule (2005)
  - .400: Breach Notification Rule (2010)
- HITECH Act
  - Modified HIPAA
  - Implemented by HIPAA Omnibus Rule (2013)
- No new regulations since 2013, but there has been guidance, litigation, and settlements.

# REMEMBER OTHER LAWS



**More  
restrictive law**

**HIPAA**

**Less restrictive  
law**

- HIPAA preempts less restrictive laws.
- Comply with more restrictive law, e.g.,
  - Federally assisted substance use disorder programs (42 CFR part 2)
  - Others?



# 1. INCREASED ENFORCEMENT OVER PAST YEAR

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost paper records of 2,000+, but failed to timely report  |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |

# INCREASED ENFORCEMENT: RIGHT TO ACCESS INITIATIVE

| Settlement | Facts  |
|------------|--|
| \$25,000   | Psychiatric group failed to provide records despite requests and prior OCR guidance; claimed records contained psychotherapy notes |
| \$100,000  | Neurology practice failed to provide complete records despite repeated requests  |
| \$160,000  | Hospital failed to provide complete records despite repeated requests  |
| \$38,000   | HIV/AIDS clinic failed to provide records despite prior guidance from OCR  |
| \$15,000   | Multi-specialty clinic failed to provide records despite requests  |
| \$3,500    | Small psych practice failed to provide records despite prior OCR guidance  |
| \$10,000   | Psych practice failed to provide records to personal rep despite OCR guidance  |
| \$70,000   | SUD provider failed to provide personal representative with records  |
| \$85,000   | Provider failed to provide records to 3 <sup>rd</sup> party in format and overcharged despite OCR guidance                         |
| \$85,000   | Hospital failed to provide mother with records of unborn child despite repeated requests   |
| \$15,000   | Physician failed to provide access despite multiple requests.  |



# HIPAA CIVIL PENALTIES

| Conduct  | Penalty   |
|--|---|
| Did not know and should not have known of violation        | <ul style="list-style-type: none"> <li>• \$119* to \$59,522* per violation</li> <li>• Up to \$25,630* per type per year</li> <li>• <b>No penalty if correct w/in 30 days</b></li> <li>• OCR may waive or reduce penalty</li> </ul>    |
| Violation due to reasonable cause                          | <ul style="list-style-type: none"> <li>• \$1,191* to \$59,522* per violation</li> <li>• Up to \$102,522* per type per year</li> <li>• <b>No penalty if correct w/in 30 days</b></li> <li>• OCR may waive or reduce penalty</li> </ul> |
| <b>Willful neglect,</b><br>but correct w/in 30 days        | <ul style="list-style-type: none"> <li>• \$11,904* to \$59,522* per violation</li> <li>• Up to \$256,305* per type per year</li> <li>• <b>Penalty is mandatory</b></li> </ul>   |
| <b>Willful neglect,</b><br>but do not correct w/in 30 days | <ul style="list-style-type: none"> <li>• At least \$59,522* per violation</li> <li>• Up to \$1,754,698* per type per year</li> <li>• <b>Penalty is mandatory</b></li> </ul>   |

(45 CFR 102.3, 160.404; 85 FR 2879)

HOLLAND & HART<sup>LLP</sup>



# ADDITIONAL CONSEQUENCES OF HIPAA VIOLATIONS

- State attorney general can bring lawsuit.
  - \$25,000 fine per violation + fees and costs
- In future, individuals may recover percentage of penalties.
- Must sanction employees who violate HIPAA.
- Must self-report breaches of unsecured protected health info
  - To affected individuals.
  - To HHS.
  - To media if breach involves > 500 persons.
- Possible lawsuits by affected individuals or others.
- Compromise of health data...

## 2. AVOIDING HIPAA CIVIL PENALTIES

You can likely avoid HIPAA civil penalties if you:

- Have required policies and safeguards in place.
- Execute business associate agreements.
- Train personnel and document training.
- Respond immediately to mitigate and correct any violation.
- Timely report breaches if required.

*No “willful neglect” =  
No penalties if  
correct violation  
within 30 days.*



# 3. CYBERSECURITY

The image is a screenshot of a web browser displaying an NBC News article. The browser's address bar shows the URL: <https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254>. The browser's menu bar includes 'File', 'Edit', 'View', 'Favorites', 'Tools', and 'Help'. The page header features the NBC News logo and navigation links: 'NEWS', 'NBC NEWS NOW', 'NIGHTLY NEWS', 'MEET THE PRESS', 'DATELINE', 'MSNBC', and 'TODAY'. The article title is 'Major hospital system hit with cyberattack, potentially largest in U.S. history'. Below the title is a sub-headline: 'Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend.' The article is dated 'Sept. 28, 2020, 11:07 AM MDT / Updated Sept. 28, 2020, 2:04 PM MDT' and is written by 'Kevin Collier'. A 'Sponsored Stories' section is visible on the right, featuring a photo of a dog.

NEWS NBC NEWS NOW NIGHTLY NEWS MEET THE PRESS DATELINE MSNBC TODAY

**NEWS** Major hospital system hit with cyberattack, potentially largest in U.S. history SHARE THIS – f t e

## Major hospital system hit with cyberattack, potentially largest in U.S. history


Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend.

Sept. 28, 2020, 11:07 AM MDT / Updated Sept. 28, 2020, 2:04 PM MDT

**By Kevin Collier**

A major hospital chain has been hit by what appears to be one of the largest medical cyberattacks in United States history.

**Sponsored Stories** by Taboola



# CYBERSECURITY SETTLEMENTS

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost paper records of 2,000+, but failed to timely report  |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |

# 10/29/20: HHS/FBI WARNING "IMMINENT THREAT" TO HEALTHCARE INDUSTRY

Cyber Alert: Ransomware Activity Targeting the Healthcare and Public Health Sector - Message (HTML)

File Message Help Mimecast Tell me what you want to do

Mark Unread Find Zoom Save Attachments Properties Where Used

iManage E-Mail Management

Search for Workspaces (shortcut) - (Ctrl+9) File Delete Print Private Save Attachments

## Cyber Alert: Ransomware Activity Targeting the Healthcare and Public Health Sector



OCR HIPAA Privacy Rule information distribution <OCR-PRIVACY-LIST@LIST.NIH.GOV> on behalf of OS OCR PrivacyList, OCR (HHS)  
To: OCR-PRIVACY-LIST@LIST.NIH.GOV

Reply Reply All Forward

Thu 10/29/2020 9:18 AM

Retention Policy Inbox 120 Days - Remove Items (4 months)

Expires 2/26/2021

### HHS Office for Civil Rights in Action



October 29, 2020

## Cyber Alert: Ransomware Activity Targeting the Healthcare and Public Health Sector

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Department of Health and Human Services (HHS) have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.

CISA, FBI, and HHS have released [AA20-302A Ransomware Activity Targeting the Healthcare and Public Health Sector](#) that details both the threat and practices that healthcare organizations should continuously engage in to help manage the risk posed by ransomware and other cyber threats. The advisory references the [joint CISA MS-ISAC Ransomware Guide](#) that provides a ransomware response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans.

In addition to these materials regarding the most recent ransomware threat to the Healthcare and Public Health Sector, the HHS Office for Civil Rights' Fact Sheet: Ransomware and HIPAA

# [HTTPS://US-CERT.CISA.GOV/NCAS/ALERTS/AA20-302A](https://us-cert.cisa.gov/ncas/alerts/aa20-302a)

Browser address bar: <https://us-cert.cisa.gov/ncas/alerts/aa20-302a>

Browser tabs: Ransomware Activity Targeti...

Browser menu: File Edit View Favorites Tools Help

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



Search input field

Services button

Report button

[Alerts and Tips](#) [Resources](#) [Industrial Control Systems](#)

[National Cyber Awareness System](#) > [Alerts](#) > Ransomware Activity Targeting the Healthcare and Public Health Sector

## Alert (AA20-302A)

[More Alerts](#)

### Ransomware Activity Targeting the Healthcare and Public Health Sector

Original release date: October 28, 2020 | Last revised: November 02, 2020

Print | Tweet | Send | Share

#### Summary

*This advisory was updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.*

Windows taskbar: Start button, Search, Task View, File Explorer, Chrome, Edge, Outlook, Word, PowerPoint, System tray (Network, Volume, Power), Time: 10:51 PM 11/6/2020

# [HTTPS://WWW.HHS.GOV/SITES/DEFAULT/FILES/RANSOMWAREFACTSHEET.PDF](https://www.hhs.gov/sites/default/files/ransomwarefactsheet.pdf)

FACT SHEET: Ransomware and HI x +

← → ↻ 🏠 🔒 <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

According to OCR, ransomware attack is a presumptive HIPAA breach requiring:

- Investigation
- Notice to
  - Individuals
  - HHS
  - Media, if > 500 persons
- Fallout from govt investigation and adverse PR

## 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).<sup>1</sup> 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 assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

### 1. What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates<sup>2</sup> data, or ransomware in conjunction with other malware that does so.

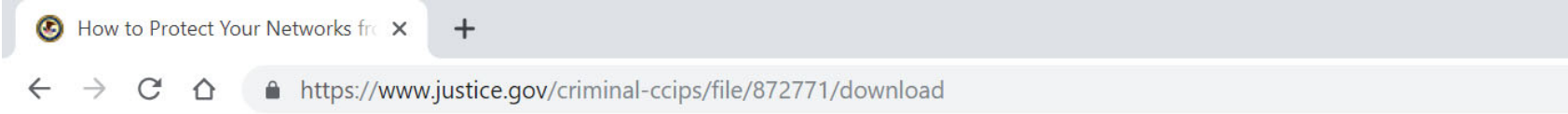
### 2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks:



[HTTPS://WWW.JUSTICE.GOV/CRIMINAL-CCIPS/FILE/872771/DOWNLOAD](https://www.justice.gov/criminal-ccips/file/872771/download)



1. Best practices for protecting your network
  - Educate personnel
  - Preventative measures
  - Business continuity
2. Suggestions for responding to ransomware
3. Law enforcement assistance

How to Protect Your Networks from  
**RANSOMWARE**

This document is a U.S. Government interagency technical guidance document aimed to inform Chief Information Officers and Chief Information Security Officers at critical infrastructure entities, including small, medium, and large organizations. This document provides an aggregate of already existing Federal

[HTTPS://WWW.PHE.GOV/PREPAREDNESS/PLANNING/405D/DOCUMENTS/HICP-MAIN-508.PDF](https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf)

## Top 5 Cyberthreats to Healthcare Industry

1. E-mail phishing attacks
  2. Ransomware attacks
  3. Loss or theft of equipment or data
  4. Insider, accidental or intentional data loss
  5. Attacks against connected medical devices that may affect patient safety
- Best practices
  - Sample Forms
  - Resources

w/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

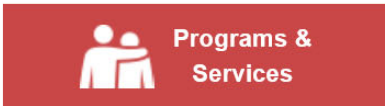
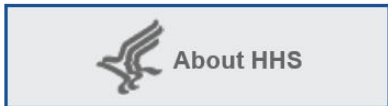
## Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

# [HTTPS://WWW.HHS.GOV/ABOUT/AGENCIES/ASA/OCIO/HC3/INDEX.HTML](https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html)

Browser navigation bar showing the URL <https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html> and a search field. The browser tab is titled "HC3 Home Page | HHS.gov".



[Home](#) > [About](#) > [Agencies](#) > [ASA](#) > [OCIO](#) > HC3 Home Page

- Assistant Secretary for Administration (ASA)
- About ASA
- EEO Compliance & Operations +
- Office of Business Management & Transformation (OBMT) +
- Office of Human Resources (OHR) +
- Office of the Chief Information Officer (OCIO) -
- About OCIO

Text Resize **A A A** | Print | Share

## HC3 Home Page

### A Prescription for Health Sector Cybersecurity

Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH).



### HC3 Products



# OCR DIRECTOR SEVERINO

- "Hacking is the number one source of large health care data breaches."  
(<https://www.hhs.gov/about/news/2020/09/21/orthopedic-clinic-pays-1.5-million-to-settle-systemic-noncompliance-with-hipaa-rules.html>)
- "If [covered entities] don't invest the time and effort to identify their security vulnerabilities, be they technical or human, hackers surely will."  
(<https://www.hhs.gov/about/news/2020/09/25/health-insurer-pays-6-85-million-settle-data-breach-affecting-over-10-4-million-people.html>)
- "The health care industry is a known target for hackers and cyberthieves. The failure to implement the security protections required by the HIPAA Rules ... is inexcusable." (<https://www.hhs.gov/about/news/2020/09/23/hipaa-business-associate-pays-2.3-million-settle-breach.html> )

# 4. SECURITY RULE

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost records of paper records of 2,000+, but failed to timely report   |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |

# SECURITY RULE

- Risk assessment
- Implement safeguards.
  - Administrative
  - Technical, including encryption
  - Physical
- Execute business associate agreements.

(45 CFR 164.300-.314)

- Protect ePHI:
- Confidentiality
  - Integrity
  - Availability

# RISK ASSESSMENT

## Requirement

- Must conduct and document an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.  
(45 CFR 164.308(a)(1))
- Ongoing process.

## Elements

- Scope includes all ePHI in any format, including hard drives, portable media, mobile devices, servers, transmission, storage, networks, etc.
- Track flow of ePHI
- Identify threats and vulnerabilities
- Assess current security measures
- Assess likelihood of threat
- Determine level of risk
- Confirm and implement plan

# [HTTPS://WWW.HEALTHIT.GOV/TOPIC/PRIVACY-SECURITY-AND-HIPAA/SECURITY-RISK-ASSESSMENT-TOOL](https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool)

Security Risk Assessment Tool | H x +

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

NEW: Health IT Feedback Portal

Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

HealthIT.gov

TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC

Search

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 +

## Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities and its business associates conduct a risk assessment of their health information. A risk assessment helps your organization ensure it is compliant with HIPAA's technical safeguards. A risk assessment also helps reveal areas where your organization's health information (PHI) could be at risk. To learn more about the assessment process and the 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 and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program.

Updated Tool  
2020



# SECURITY RULE SAFEGUARDS

| Administrative   | Physical  | Technical  |
|--|---|--|
| <ul style="list-style-type: none"><li>• Security management process, e.g., risk analysis, sanctions, review system activity</li><li>• Assigned security responsibility</li><li>• Workforce security</li><li>• Information access management</li><li>• Security awareness and training</li><li>• Security incident procedures</li><li>• Contingency plan</li><li>• Evaluation</li></ul> | <ul style="list-style-type: none"><li>• Facility access controls, e.g., contingency operations, validation, maintenance records</li><li>• Workstation use</li><li>• Workstation security</li><li>• Device and media controls, e.g., disposal, re-use, accountability, data backup and storage</li></ul> | <ul style="list-style-type: none"><li>• Access control, e.g., unique user ID, emergency access, auto logoff, encryption</li><li>• Audit controls</li><li>• Integrity, e.g., authentication</li><li>• Person or entity authentication</li><li>• Transmission security, e.g., integrity controls, encryption</li></ul> |

(45 CFR 164.308-.312)

# [HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SECURITY/GUIDANCE/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html)

/hipaa/for-professionals/security/guidance/index.html

HHS.gov Health Information Privacy

U.S. Department of Health & Human Services

I'm looking for...



HHS A-Z Index



HIPAA for Individuals



Filing a Complaint



HIPAA for Professionals



Newsroom

[HHS Home](#) > [HIPAA](#) > [For Professionals](#) > [Security](#) > Security Rule Guidance Material

HIPAA for Professionals

Privacy



Security



Summary of the Security Rule

Guidance

Combined Text of All Rules

Breach Notification



Compliance & Enforcement



Special Topics



Patient Safety



Covered Entities & Business

Text Resize A A A



Share



## Security Rule Guidance Material

In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).

[Security Risks to Electronic Health Information from Peer-to-Peer File Sharing Applications](#)-The Federal Trade Commission (FTC) has developed a guide to Peer-to-Peer (P2P) security issues for businesses that collect and store sensitive information.

[Safeguarding Electronic Protected Health Information on Digital Copiers](#)-The Federal Trade Commission (FTC) has tips on how to safeguard sensitive data stored on the hard drives of digital copiers.

## 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](#)

# [HTTPS://WWW.HEALTHIT.GOV/TOPIC/PRIVACY-SECURITY-AND-HIPAA/HEALTH-IT-PRIVACY-AND-SECURITY-RESOURCES-PROVIDERS](https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers)

The screenshot shows a web browser window displaying the HealthIT.gov website. The browser's address bar shows the URL: <https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers>. The website header includes the HealthIT.gov logo, the text "Official Website of The Office of the National Coordinator for Health Information Technology (ONC)", and navigation links for "CONTACT" and "EMAIL UPDATES". Below the header is a blue navigation bar with links for "TOPICS", "HOW DO I?", "BLOG", "NEWS", and "ABOUT ONC", along with a search bar. The main content area features a breadcrumb trail: "Home > Topics > Privacy, Security, and HIPAA > Privacy & Security Resources & Tools > Resources and Tools for Providers". On the left side, there is a sidebar menu with expandable sections: "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" (which is currently expanded), "Security Risk Assessment Tool", "Privacy & Security Training Games", and "Model Privacy Notice (MPN)". The main content area is titled "Health IT Privacy and Security Resources for Providers" and contains a paragraph explaining that 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 resources to help providers integrate HIPAA and other federal health information privacy and security into their practice. Below this paragraph is a section titled "Tools and Templates" which lists five resources: "Sync for Science (S4S) API Privacy and Security", "Guide to Privacy and Security of Electronic Health Information", "Security Risk Assessment (SRA) Tool", "Security Risk Analysis Guidance", and "HIPAA Security Toolkit Application". The Windows taskbar at the bottom shows the time as 1:33 PM on 3/9/2019.

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.

# HTTPS://WWW.HEALTHIT.GOV/TOPIC/PRIVACY-SECURITY-AND-HIPAA/YOUR-MOBILE-DEVICE-AND-HEALTH-INFORMATION-PRIVACY-AND-SECURITY

Browser address bar: <https://www.healthit.gov/topic/privacy-security-and-hipaa/your-mobile-device-and-health-information-privacy-and-security>

HealthIT.gov logo | **NEW: Health IT Feedback Portal** | CONTACT | EMAIL

Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

Connect with us: [in](#) [Twitter](#) [YouTube](#) [RSS](#)

TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC

Search

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

## Your Mobile Device and Health Information Privacy and Security

*Secure your mobile devices, e.g., laptops, USBs, etc.!*

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

Worried About Usin...

### MOBILE DEVICE RISKS

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



to you when using mobile devices.

# OCR DIRECTOR SEVERINO

- “All health care providers, large and small, need to take their HIPAA obligations seriously.... The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the health care industry.”  
(<https://www.hhs.gov/about/news/2020/03/03/health-care-provider-pays-100000-settlement-ocr-failing-implement-hipaa.html> )
- “Laptops, cellphones, and other mobile devices are stolen every day, that’s the hard reality. Covered entities can best protect their patients’ data by encrypting mobile devices to thwart identity thieves.”  
(<https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html> )
- “Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk.”  
(<https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html>).

# COMMUNICATING BY E-MAIL OR TEXT

- General rule: must be secure, i.e., encrypted.
- To patients: may communicate via unsecure e-mail or text if warned patient and they choose to receive unsecure.

(45 CFR 164.522(b); 78 FR 5634)

- To providers, staff or other third parties: must use secure platform.

(45 CFR 164.312; CMS letter dated 12/28/17)

- Orders: Medicare Conditions of Participation and Conditions for Coverage generally prohibit texting orders.

(CMS letter dated 12/28/17)

# 5. COMPLY WITH USE AND DISCLOSURE RULES

Must have:

- Disclosure for treatment, payment and healthcare operations.
- Disclosures to family members and others involved in patient's care if patient doesn't object.
- Exceptions for public safety and govt functions.
- HIPAA compliant authorization

(45 CFR 164.502-.512)

# PRIVACY RULE SETTLEMENTS

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost paper records of 2,000+, but failed to timely report  |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |



# TREATMENT, PAYMENT OR HEALTHCARE OPERATIONS

- May use/disclose PHI without patient's authorization for your own:
  - Treatment;
  - Payment; or
  - Health care operations.
- May disclose PHI to another covered entity for other entity's:
  - Treatment;
  - Payment; or
  - Certain healthcare operations if both have relationship with patient.
- Exception: psychotherapy notes.
  - Requires specific authorization for use by or disclosures to others.

(45 CFR 164.506, 164.508 and 164.522)

➤ Don't agree to restrictions!

# FAMILY AND PERSONS INVOLVED IN CARE

- May/must disclose to personal representatives.
- May use or disclose PHI to family or others involved in patient's care or payment for care:
  - If patient present, may disclose if:
    - Patient agrees to disclosure or has chance to object and does not object, or
    - Reasonable to infer agreement from circumstances.
  - If patient unable to agree, may disclose if:
    - Patient has not objected; and
    - You determine it is in the best interest of patient.
  - Limit disclosure to scope of person's involvement.
- Applies to disclosures after the patient is deceased.

(45 CFR 164.510)

# [HTTPS://WWW.HHS.GOV/SITES/DEFAULT/FILES/PROVIDER\\_FFG.PDF](https://www.hhs.gov/sites/default/files/provider_ffg.pdf)

provider\_ffg.pdf

[https://www.hhs.gov/sites/default/files/provider\\_ffg.pdf](https://www.hhs.gov/sites/default/files/provider_ffg.pdf)



## A HEALTH CARE PROVIDER'S GUIDE TO THE HIPAA PRIVACY RULE:



### Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care

U.S. Department of Health and Human Services • Office for Civil Rights

This guide explains when a health care provider is allowed to share a patient's health information with the patient's family members, friends, or others identified by the patient as involved in the patient's care under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HIPAA is a Federal law that sets national standards for how health plans, health care clearinghouses, and most health care providers are to protect the privacy of a patient's health information.<sup>1</sup>

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for care. This guide is intended to clarify these HIPAA requirements so that health care providers do not unnecessarily withhold a patient's health information from these persons. This guide includes common questions and a table that summarizes the relevant requirements.<sup>2</sup>

#### COMMON QUESTIONS ABOUT HIPAA

- 1. If the patient is present and has the capacity to make health care decisions, when does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?**

If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care.

Here are some examples:

- An emergency room doctor may discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.

# EXCEPTIONS FOR PUBLIC HEALTH OR GOVERNMENT FUNCTIONS

- Another law requires disclosures
- Disclosures to prevent serious and imminent harm.
- Public health activities
- Health oversight activities
- Judicial or administrative proceedings
  - Court order or warrant
  - Subpoenas
- Law enforcement
  - Must satisfy specific requirements
- Workers compensation  
(45 CFR 164.512)

Ensure you  
comply with  
specific  
regulatory  
requirements

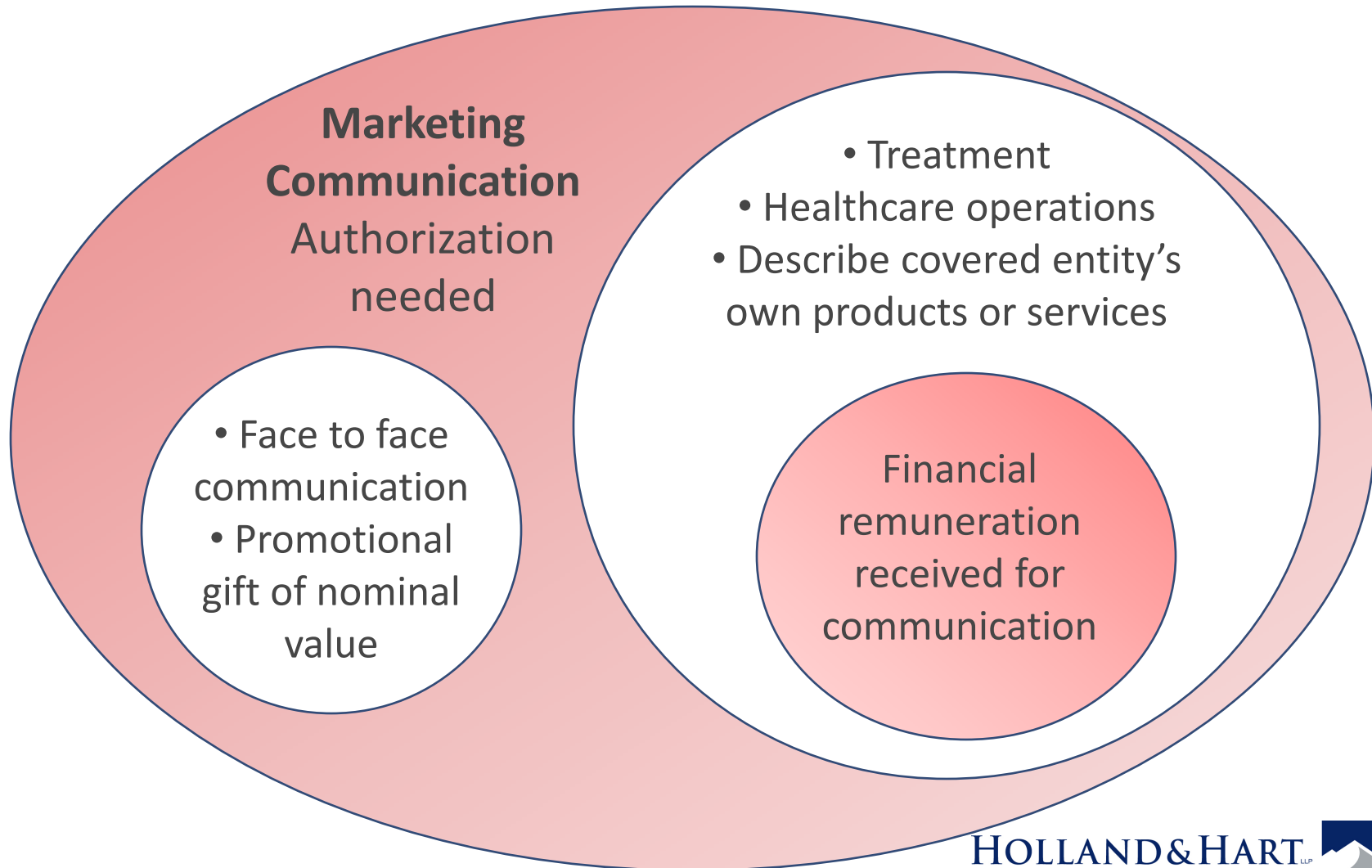
# MARKETING

- Generally need authorization if communication is about a product or service that encourages recipient to purchase or use product or service except:
  - To describe product or service provided by the covered entity,
  - For treatment of patient, or
  - For case management, care coordination, or to direct or recommend alternative treatment, therapies, providers, or setting,

unless covered entity receives financial remuneration from third party for making the communication.

(45 CFR 164.501 and .508(a)(3))

MARKETING = COMMUNICATION ABOUT PRODUCT OR SERVICE THAT ENCOURAGES RECIPIENT TO PURCHASE OR USE PRODUCT OR SERVICE



# MINIMUM NECESSARY STANDARD

- Cannot use or disclose more PHI than is reasonably necessary for intended purpose.
- Minimum necessary standard does not apply to disclosures to:
  - Patient.
  - Provider for treatment.
  - Per individual's authorization.
  - As required by law.
- May rely on judgment of:
  - Another covered entity.
  - Professional within the covered entity.
  - Business associate for professional services.
  - Public official for permitted disclosure.
- Must have role-based policies limiting access to functions.

(45 CFR 164.502 and .514)

## 6. COVID WAIVERS—NOT!

- HIPAA privacy and rule still apply despite COVID.
  - Generally may not disclose without—
    - Patient’s or personal rep’s authorization, or
    - HIPAA exception, e.g.,
      - Treatment, payment or authorizations
      - To avert serious and imminent threat of harm
      - Required by law
      - To public health agency
  - Beware media access.

(<https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf>)



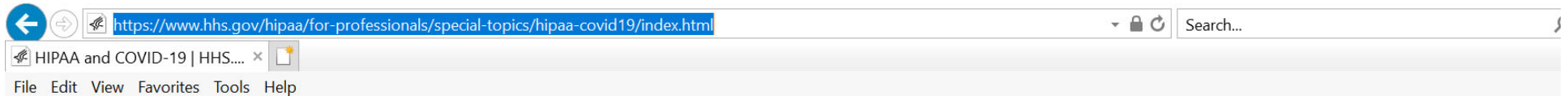
# COVID WAIVERS—KIND OF

- HHS waived sanctions against hospitals for:
  - Requirement to obtain patient consent to speak with family or friends
  - Requirement to honor request to opt out of facility directory
  - Distribute notice of privacy practices
  - Patient’s right to request privacy restrictions
  - Patient’s right to request confidential communications

(<https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf>)

- HHS will exercise enforcement discretion re:
  - Community based testing sites
  - Business associate’s use of PHI for public health purposes
  - Telehealth technology

# [HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SPECIAL-TOPICS/HIPAA-COVID19/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html)



- Emergency Response
- Health Information Technology
- Health Apps
- Patient Safety** +
- Covered Entities & Business Associates** +
- Training & Resources
- FAQs for Professionals
- Other Administrative Simplification Rules

## OCR HIPAA Announcements Related to COVID-19:

- [Trump Administration Adds Health Plans to June 2020 Plasma Donation Guidance](#) - August 24, 2020
- [OCR Issues Guidance on How Health Care Providers Can Contact Former COVID-19 Patients About Blood and Plasma Donation Opportunities](#) - June 12, 2020
- [OCR Issues Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities](#) - May 5, 2020
- [OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency](#) - April 9, 2020
- [OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency](#) - April 2, 2020
- [OCR Issues Bulletin on Civil Rights Laws and HIPAA Flexibilities That Apply During the COVID-19 Emergency](#) - March 28, 2020
- [OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19](#) - March 24, 2020
- [OCR Issues Guidance on Telehealth Remote Communications Following Its Notification of Enforcement Discretion](#) - March 20, 2020



# REPORTING TEST RESULTS FOR EMPLOYMENT OR SIMILAR PURPOSES

- HIPAA generally applies to tests performed for employment or similar purposes, e.g., COVID tests, drug tests, school physicals, independent medical exams, etc.
  - Obtain patient's authorization to disclose before providing service.
  - Provider may condition exam on authorization.
  - Employer may condition employment on authorization.

(65 FR 82592 and 82640)

- Generally may not use PHI obtained in capacity as healthcare provider for employment-related decisions.

(67 FR 53191-92)

- Possible exceptions:
  - Disclosure to avoid serious and imminent threat of harm.
  - Disclosures required by law, e.g., disclosure to public health authorities, OSHA, MSHA, etc.

## 7. BEWARE BUSINESS ASSOCIATES

- May disclose PHI to business associates if have valid business associate agreement (“BAA”).
    - Business associates = entities whom you engage to create, access, maintain or disclosure your PHI
  - Failure to execute BAA = HIPAA violation
    - May subject you to HIPAA fines.
    - May expose you to liability for business associate’s misconduct.
  - BAAs must contain required terms and statements, e.g.,
    - Identify permissible uses
    - Require cooperation and notice to covered entity
    - Pass limits to business associate and subcontractors
- (45 CFR 164.314, 164.504(e))

# BUSINESS ASSOCIATE SETTLEMENTS

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost paper records of 2,000+, but failed to timely report  |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |

# [HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/COVERED-ENTITIES/SAMPLE-BUSINESS-ASSOCIATE-AGREEMENT-PROVISIONS/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html)

Business Associate Contr x

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

HIPAA for Professionals

Privacy



Security



Breach Notification



Compliance & Enforcement



Special Topics



Patient Safety



Covered Entities & Business Associates



Business Associates

Business Associate Contracts

Training & Resources

## 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 functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to

top

# 8. RIGHT TO ACCESS PHI

OCR Settles Eleventh Investigatio x +

hhs.gov/about/news/2020/11/12/ocr-settles-eleventh-investigation-hipaa-right-access-initiative.html



About HHS



Programs &  
Services



Grants &  
Contracts



Laws &  
Regulations

[Home](#) > [About](#) > [News](#) > OCR Settles Eleventh Investigation in HIPAA Right of Access Initiative

Search News Releases

Search

Text Resize A A A

Print

Share

**FOR IMMEDIATE RELEASE**  
November 12, 2020

Contact: HHS Press Office  
202-690-6343  
[media@hhs.gov](mailto:media@hhs.gov)

OCR "Right to  
Access" Initiative

## OCR Settles Eleventh Investigation in HIPAA Right of Access Initiative

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) announces its eleventh settlement of an enforcement action in its HIPAA Right of Access Initiative. OCR announced this initiative as an enforcement priority in 2019 to support individuals' right to timely access to their health records at a reasonable cost under the HIPAA Privacy Rule.

Dr. Rajendra Bhayani, who is a private practitioner specializing in otolaryngology in Regal Park, New York, has agreed to take corrective actions and pay \$15,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard.

In September 2018, OCR received a complaint alleging that Dr. Bhayani failed to provide a patient with access to her medical records following her request in July 2018. OCR responded by providing Dr.

# RECENT “RIGHT TO ACCESS” SETTLEMENTS

| Settlement | Facts  |
|------------|--|
| \$25,000   | Psychiatric group failed to provide records despite requests and prior OCR guidance; claimed records contained psychotherapy notes |
| \$100,000  | Neurology practice failed to provide complete records despite repeated requests  |
| \$160,000  | Hospital failed to provide complete records despite repeated requests  |
| \$38,000   | HIV/AIDS clinic failed to provide records despite prior guidance from OCR  |
| \$15,000   | Multi-specialty clinic failed to provide records despite requests  |
| \$3,500    | Small psych practice failed to provide records despite prior OCR guidance  |
| \$10,000   | Psych practice failed to provide records to personal rep despite OCR guidance  |
| \$70,000   | SUD provider failed to provide personal representative with records  |
| \$85,000   | Provider failed to provide records to 3 <sup>rd</sup> party in format and overcharged despite OCR guidance                         |
| \$85,000   | Hospital failed to provide mother with records of unborn child despite repeated requests   |
| \$15,000   | Physician failed to provide access despite requests and OCR assistance   |



# RIGHT TO ACCESS PHI

- Patient or personal rep generally has right to inspect and obtain copy of PHI in “designated record set, i.e., documents used to make decisions concerning healthcare or payment.
- Must respond within 30 days.
- Must provide records in requested form if readily producible, including electronic form.
- May require written request.
- May charge reasonable cost-based fee, i.e., cost of actual labor and materials in making copies, not administrative or retrieval fee.
- Check with privacy officer or review 45 CFR 164.524 before denying request.

(45 CFR 164.524)

# OCR DIRECTOR SEVERINO

- "For too long, healthcare providers have slow-walked their duty to provide patients their medical records out of a sleepy bureaucratic inertia. We hope our shift to the imposition of corrective actions and settlements under our Right of Access Initiative will finally wake up healthcare providers to their obligations under the law." (<https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html>).
- "Doctor's offices, large and small, must provide patients their medical records in a timely fashion. We will continue to prioritize HIPAA Right of Access cases for enforcement until providers get the message." (<https://www.hhs.gov/about/news/2020/11/12/ocr-settles-eleventh-investigation-hipaa-right-access-initiative.html>)

# [WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/PRIVACY/GUIDANCE/ACCESS/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html)

nt under | x

ecure | <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/>

**HHS.gov**

U.S. Department of Health & Human Services

**Health Information Privacy**

I'm looking for...



[HHS A-Z Index](#)



**HIPAA for  
Individuals**



**Filing a  
Complaint**



**HIPAA for  
Professionals**



**Newsroom**

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance](#) > Individuals' Right under HIPAA to Access their Health Information

**HIPAA for Professionals**

**Privacy** -

[Summary of the Privacy Rule](#)

[Guidance](#)

[Combined Text of All Rules](#)

**Security** +

Text Resize **A A A**

Print

Share



## Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

[Newly Released FAQs on Access Guidance](#)

[New Clarification – \\$6.50 Flat Rate Option is Not a Cap on Fees for Copies of PHI](#)

### Introduction

Providing individuals with easy access to their health information empowers them to be more in control

# PERSONAL REPRESENTATIVES

- Under HIPAA, personal rep = patient.
  - Personal rep may exercise patient rights.
- Personal rep = persons with authority under state law to:
  - Make healthcare decisions for patient, or
  - Make decisions for deceased patient's estate.

(45 CFR 164.502(g))

- Not required to treat person as the personal rep of minor (i.e., do not disclose protected info to them) if:
  - Minor obtains care at the direction of a court or person appointed by the court.
  - Parent agrees that provider may have a confidential relationship.
  - Provider determines that treating personal rep as the patient is not in the best interest of patient, e.g., abuse.

(45 CFR 164.502(g))

# PSYCHOTHERAPY NOTES

- Must have authorization to use or disclose psych notes except for provider's use of own notes for treatment purposes.
  - “Psych notes” are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
  - “Psych notes” excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
- Psych authorization cannot be combined with any other authorization.

(45 CFR 164.508)

# PATIENT REQUESTS TO SEND PHI TO THIRD PARTY

On January 23, 2020, *Ciox* court modified OCR rules for disclosures per patient's request to send PHI to third party.

| ePHI IN EHR  | OTHER PHI   |
|--|---|
| Must send ePHI maintained in EHR to third party identified by patient. | <u>Not</u> required to send to third party per patient's request. |
| Part of patient's right to access, i.e., must respond within 30 days.  | N/A   |
| <u>Not</u> limited to reasonable cost-based fee ("patient rate")       | <u>Not</u> limited to reasonable cost-based fee ("patient rate")  |

(45 CFR 164.524; OCR *Guide to Patient Access*)

# 9. RESPOND PROMPTLY TO PROBLEMS AND VIOLATIONS

- Covered entities and business associates must:
  - “[R]espond to suspected or known security incidents;
  - “[M]itigate, to the extent practicable, harmful effects of security incidents that are known...

(45 CFR 164.308(a)(6))

- Covered entity must
  - “[M]itigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart ...

(45 CFR 164.530(f))

# FAILURE TO RESPOND

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected; reporter had warned clinic  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost paper records of 2,000+, but failed to timely report  |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |



# TECHNICAL ASSISTANCE

- “Principles for achieving compliance.
  - (a) Cooperation. The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.
  - (b) Assistance. The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.”

(45 CFR 160.304)

# FAILURE TO RESPOND

| Settlement | Facts  |
|------------|--|
| \$25,000   | Psychiatric group failed to provide records despite requests and prior OCR guidance; claimed records contained psychotherapy notes |
| \$100,000  | Neurology practice failed to provide complete records despite repeated requests  |
| \$160,000  | Hospital failed to provide complete records despite repeated requests  |
| \$38,000   | HIV/AIDS clinic failed to provide records despite prior guidance from OCR  |
| \$15,000   | Multi-specialty clinic failed to provide records despite requests  |
| \$3,500    | Small psych practice failed to provide records despite prior OCR guidance  |
| \$10,000   | Psych practice failed to provide records to personal rep despite OCR guidance  |
| \$70,000   | SUD provider failed to provide personal representative with records  |
| \$85,000   | Provider failed to provide records to 3 <sup>rd</sup> party in format and overcharged despite OCR guidance                         |
| \$85,000   | Hospital failed to provide mother with records of unborn child despite repeated requests   |
| \$15,000   | Physician failed to provide access despite requests and OCR assistance   |

# WILLFUL NEGLIGENCE

- “*Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.”

(45 CFR 160.401)

- Willful neglect =
  - Mandatory OCR investigations
  - Mandatory penalties
    - If correct within 30 days:
      - \$11,904\* to \$59,522\* per violation
      - Up to \$256,305\* per type per year
    - If fail to correct w/in 30 days:
      - At least \$59,522\* per violation
      - Up to \$1,754,698\* per type per year

(45 CFR 160.404)

# WILLFUL NEGLIGENCE

- “A covered entity disposed of several hard drives containing electronic protected health information in an unsecured dumpster, in violation of § 164.530(c) and § 164.310(d)(2)(i). HHS’s investigation reveals that the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process.”

(75 FR 40879)

✓ **Willful neglect**

# 10. HAVE REQUIRED POLICIES AND SAFEGUARDS

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost records of paper records of 2,000+, but failed to timely report   |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |

# REQUIRED POLICIES AND SAFEGUARDS

- Ensure you have policies covering required provisions:
  - Privacy Rule: 45 CFR 164.500 et seq.
  - Security Rule: 45 CFR 164.300 et seq.
  - Breach Notification Rule: 45 CFR 164.400 et seq.
- Ensure you have compliant forms
  - Notice of Privacy Practices
  - Business Associate Agreements
  - Authorizations
  - Designation of privacy and security officers
- Periodically review and update as necessary
  - Compliance with 2013 omnibus rule
  - Policies and forms have a tendency to morph over time

# REQUIRED POLICIES AND SAFEGUARDS

- “A hospital employee accessed the paper medical record of his ex-spouse while he was on duty to discover her current address for a personal reason, knowing that such access is not permitted by the Privacy Rule and contrary to the policies and procedures of the hospital. HHS’s investigation reveals that the covered entity had appropriate and reasonable safeguards regarding employee access to medical records, and that it had delivered appropriate training to the employee.”

(75 FR 40879)

✓ **Not willful neglect by the hospital.**

# REQUIRED POLICIES AND SAFEGUARDS



## HIPAA PRIVACY CHECKLIST

The following summarizes required and recommended privacy policies and forms per the HIPAA Privacy Rule. Additional policies are required by the HIPAA Security Rule. Covered entities and business associates should ensure that they have required policies in place to minimize or avoid penalties under the HIPAA regulations. The citations are to 45 CFR Part 164. For additional resources concerning Privacy Rule requirements and compliance assistance, see the Office of Civil Rights privacy website, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html>. The Privacy Rule is subject to periodic amendment. Users should review the current rule requirements to ensure continued compliance.

| Policies                                 |   |                        |
|--|---|------------------------|
| HIPAA Privacy Rule Reference             | Policy  | Status (Complete, N/A) |
| <b>Use and Disclosure: General Rules</b> |   |                        |
| 164.506                                  | Consent is implied for treatment, payment and health care operations; no written authorization is required except for psychotherapy notes.  |                        |
| 164.510                                  | Providing notice and chance for patient to agree or object is sufficient for certain disclosures, including disclosures to family members or others involved in the patient's care; for facility directories; and to provide notice in emergency situations.                  |                        |
| 164.512                                  | Certain disclosures may be made per regulatory exceptions subject to specific conditions, e.g., uses or disclosures required by law; to avert a serious and imminent health; for public health activities; in response to a court order or subpoena; to law enforcement, etc. |                        |
| 164.508                                  | Authorizations are generally required for all other uses or disclosures, including uses or disclosures of psychotherapy notes; for most marketing activities; sale of protected health information; etc. Include the elements for a valid authorization.                      |                        |
| <b>Use and Disclosure: Special Rules</b> |   |                        |
| 164.514(f)                               | Fund raising uses or disclosures generally require authorization except in limited circumstances.   |                        |
| 164.512(i)                               | Research generally requires authorization unless certain conditions are met.  |                        |
| 164.502(f)                               | Privacy protection continues after death for a period of 50 years.  |                        |
| 164.502(g)                               | Personal representatives and parents of unemancipated minors are generally entitled to access information and exercise other patient rights, subject to certain exceptions.   |                        |
| 164.514(h)                               | Covered entities should verify a requesting person's identity and authority before disclosing information.  |                        |

HIPAA PRIVACY CHECKLIST - 1  
Copyright © 2013, Holland & Hart LLP

HIPAA-Privacy-Checklist-HH.docx

Kim C. Stanger  
Phone (208) 383-3913  
[kstanger@hollandhart.com](mailto:kstanger@hollandhart.com)  
[www.hollandhart.com](http://www.hollandhart.com)



## 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) |
|----------------------------------|--|------------------------|
| <b>Administrative Safeguards</b> |  |                        |
| 164.308(a)(1)(i)                 | Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.   |                        |
| 164.308(a)(1)(i)(A)              | Has a risk analysis been completed using IAW NIST Guidelines? (R)  |                        |
| 164.308(a)(1)(i)(B)              | Has the risk management process been completed using IAW NIST Guidelines? (R)  |                        |
| 164.308(a)(1)(i)(C)              | Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)   |                        |
| 164.308(a)(1)(i)(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)(i)(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)(i)(B)              | Have you implemented procedures to determine the access of an employee to EPHI is appropriate? (A)   |                        |
| 164.308(a)(3)(i)(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.  |                        |

HIPAA SECURITY CHECKLIST - 1  
Copyright © 2013, Holland & Hart LLP

HIPAA-Security-Checklist-HH.docx

Kim C. Stanger  
Phone (208) 383-3913  
[kstanger@hollandhart.com](mailto:kstanger@hollandhart.com)  
[www.hollandhart.com](http://www.hollandhart.com)



# ADMINISTRATIVE REQUIREMENTS

- Implement written policies and procedures.
- Implement reasonable safeguards.
  - “Incidental disclosures” do not violate HIPAA.
- Train workforce.
- Respond to complaints and violations.
- Mitigate improper disclosures.

(45 CFR 164.530)

No HIPAA penalties if:

- No “willful neglect”
- Correct action within 30 days

# 10. REPORT BREACH OF UNSECURED PHI

| Settlement  | Facts  |
|-------------|--|
| \$202,400   | Health dept failed to terminate ex-employee's access; 498 persons affected   |
| \$1,000,000 | Aetna had 3 breaches: (i) PHI disclosed through web searches; (ii) HIV info visible through envelopes; (iii) tx visible on envelope; 18,000+ persons |
| \$6,850,000 | Cyberattackers used phishing e-mail to access records of 10.4 million persons  |
| \$2,300,000 | Hacker accessed business associate's data of 6.12 million persons; FBI had warned  |
| \$1,500,000 | Hacker accessed records of 208,557 persons affected  |
| \$1,040,000 | Unencrypted laptop stolen from business associate; 20,431 persons affected   |
| \$25,000    | FQHC disclosed records of 1,263 to unknown e-mail account  |
| \$100,000   | GI practice dispute with business associate led to breach of 3,000 persons   |
| \$65,000    | Ambulance company loses unencrypted laptop; 500 persons affected   |
| \$2,175,000 | Hospital failed to do breach notice after sent info to wrong patients; 557 persons   |
| \$1,600,000 | Texas commission's info of 6,617 persons available on internet   |
| \$3,000,000 | Theft of unencrypted laptop and loss of unencrypted USB  |
| \$2,150,000 | Hospital system lost paper records of 2,000+, but failed to timely report  |
| \$10,000    | Dental practice disclosed PHI in responding to social media post   |

# OCR DIRECTOR SEVERINO

- “HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed.... When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR.”

(<https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html>)

# REPORT “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.

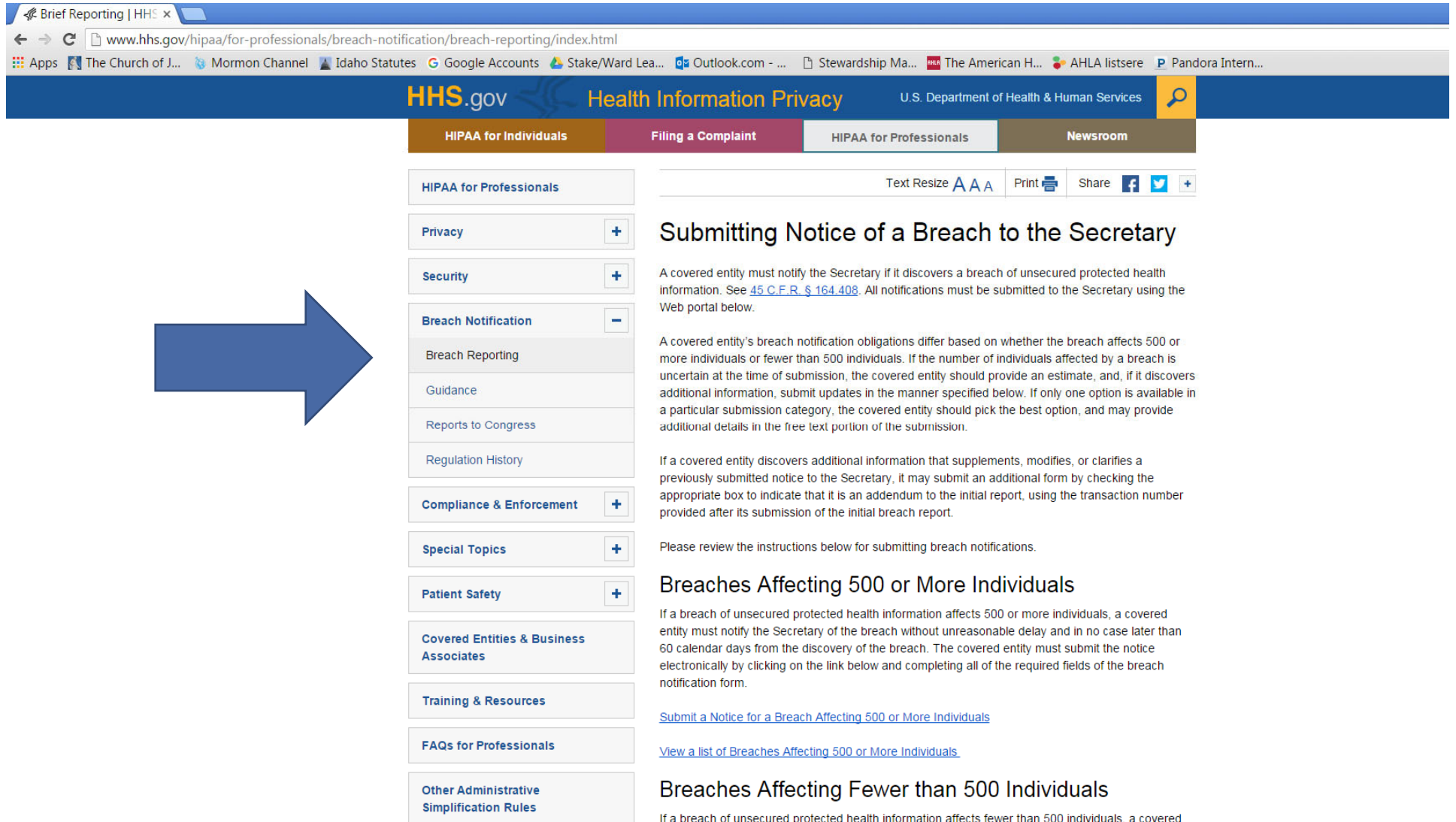
(45 CFR 164.402)

# BREACH NOTIFICATION

- If there is “breach” of “unsecured PHI”,
  - Individuals w/in 60 days
  - HHS
    - >500 persons: w/in 60 days
      - Name added to “wall of shame”
    - < 500 persons: w/in 60 days after end of calendar year
  - Local media, if breach involves > 500 persons in a state.

(45 CFR 164.400 et seq.)

# [HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/BREACH-NOTIFICATION/BREACH-REPORTING/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html)



Brief Reporting | HHS x

www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

Apps The Church of J... Mormon Channel Idaho Statutes Google Accounts Stake/Ward Lea... Outlook.com - ... Stewardship Ma... The American H... AHLA listserve Pandora Intern...

HHS.gov Health Information Privacy U.S. Department of Health & Human Services

HIPAA for Individuals Filing a Complaint HIPAA for Professionals Newsroom

HIPAA for Professionals

Text Resize A A A Print Share f t +

Privacy +

Security +

Breach Notification -

Breach Reporting

Guidance

Reports to Congress

Regulation History

Compliance & Enforcement +

Special Topics +

Patient Safety +

Covered Entities & Business Associates

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules

## Submitting Notice of a Breach to the Secretary

A covered entity must notify the Secretary if it discovers a breach of unsecured protected health information. See [45 C.F.R. § 164.408](#). All notifications must be submitted to the Secretary using the Web portal below.

A covered entity's breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate, and, if it discovers additional information, submit updates in the manner specified below. If only one option is available in a particular submission category, the covered entity should pick the best option, and may provide additional details in the free text portion of the submission.

If a covered entity discovers additional information that supplements, modifies, or clarifies a previously submitted notice to the Secretary, it may submit an additional form by checking the appropriate box to indicate that it is an addendum to the initial report, using the transaction number provided after its submission of the initial breach report.

Please review the instructions below for submitting breach notifications.

### Breaches Affecting 500 or More Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

[Submit a Notice for a Breach Affecting 500 or More Individuals](#)

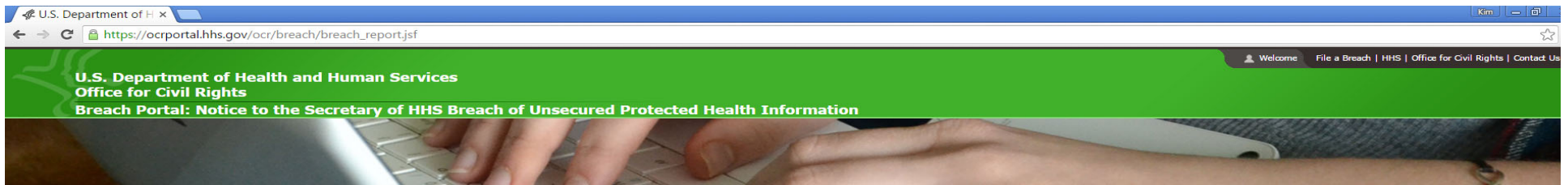
[View a list of Breaches Affecting 500 or More Individuals](#)

### Breaches Affecting Fewer than 500 Individuals

If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which

# NOTICE TO HHS

- HHS posts list of those with breaches involving more than 500 at [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsfpersons](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsfpersons)

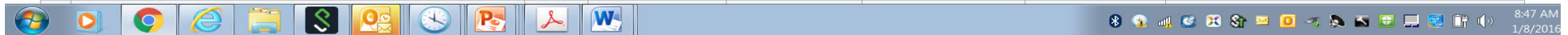


## Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

| Breach Report Results                                 |       |                     |                      |                        |                |   |  |
|---|-------|---------------------|----------------------|------------------------|----------------|---|--|
| Name of Covered Entity                                | State | Covered Entity Type | Individuals Affected | Breach Submission Date | Type of Breach | Location of Breached Information                            |  |
| Brooke Army Medical Center                            | TX    | Healthcare Provider | 1000                 | 10/21/2009             | Theft          | Paper/Films   |  |
| Mid America Kidney Stone Association, LLC             | MO    | Healthcare Provider | 1000                 | 10/28/2009             | Theft          | Network Server  |  |
| Alaska Department of Health and Social Services       | AK    | Healthcare Provider | 501                  | 10/30/2009             | Theft          | Other, Other Portable Electronic Device                     |  |
| Health Services for Children with Special Needs, Inc. | DC    | Health Plan         | 3800                 | 11/17/2009             | Loss           | Laptop  |  |
| Mark D. Lurie, MD                                     | CA    | Healthcare Provider | 5166                 | 11/20/2009             | Theft          | Desktop Computer  |  |
| L. Douglas Carlson, M.D.                              | CA    | Healthcare Provider | 5257                 | 11/20/2009             | Theft          | Desktop Computer  |  |
| David I. Cohen, MD                                    | CA    | Healthcare Provider | 857                  | 11/20/2009             | Theft          | Desktop Computer  |  |
| Michele Del Vicario, MD                               | CA    | Healthcare Provider | 6145                 | 11/20/2009             | Theft          | Desktop Computer  |  |
| Joseph F. Lopez, MD                                   | CA    | Healthcare Provider | 952                  | 11/20/2009             | Theft          | Desktop Computer  |  |
| City of Hope National Medical Center                  | CA    | Healthcare Provider | 5900                 | 11/23/2009             | Theft          | Laptop  |  |
| The Children's Hospital of Philadelphia               | PA    | Healthcare Provider | 943                  | 11/24/2009             | Theft          | Laptop  |  |
| Cogent Healthcare, Inc.                               | TN    | Business Associate  | 6400                 | 11/25/2009             | Theft          | Laptop  |  |
| Democracy Data & Communications, LLC (                | VA    | Business Associate  | 83000                | 12/08/2009             | Other          | Paper/Films   |  |
| Kern Medical Center                                   | CA    | Healthcare Provider | 596                  | 12/10/2009             | Theft          | Other   |  |
| Rick Lawson, Professional Computer Services           | NC    | Business Associate  | 2000                 | 12/11/2009             | Theft          | Desktop Computer, Electronic Medical Record, Network Server |  |
| Detroit Department of Health and Wellness Promotion   | MI    | Healthcare Provider | 646                  | 12/15/2009             | Theft          | Desktop Computer, Laptop                                    |  |
| Detroit Department of Health and Wellness Promotion   | MI    | Healthcare Provider | 10000                | 12/15/2009             | Theft          | Other Portable Electronic Device                            |  |



# FAILURE TO REPORT

- “A covered entity’s employee lost an unencrypted laptop that contained unsecured protected health information. HHS’s investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 *et seq.*”

- ✓ **Willful neglect**

(75 FR 40879)

- Loss or theft of unencrypted device with e-PHI is presumptively a reportable breach.
- When in doubt, you’re usually better off reporting.



# ADDITIONAL RESOURCES




# http://www.hhs.gov/hipaa/

HIPAA for Profession x

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

HHS.gov Health Information Privacy U.S. Department of Health & Human Services

I'm looking for...  HHS A-Z Index

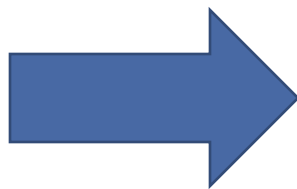
 HIPAA for Individuals

 Filing a Complaint

 HIPAA for Professionals

 Newsroom

[HHS Home](#) > [HIPAA](#) > HIPAA for Professionals



HIPAA for Professionals

- Privacy +
- Security +
- Breach Notification +
- Compliance & Enforcement +
- Special Topics +
- Patient Safety +
- Covered Entities & Business Associates
- Training & Resources
- FAQs for Professionals
- Other Administrative Simplification Rules

Text Resize [A](#) [A](#) [A](#) Print  Share   

## 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).
- The [Enforcement Rule](#) provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a [final Omnibus rule](#) that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the [Breach Notification Rule](#).
- [View the Combined Regulation Text](#) (as of March 2013). This is an unofficial version that presents all the HIPAA regulatory standards in one document. The official version of all federal regulations

# [HTTPS://WWW.HOLLANDHART.COM/HEALTHCARE-SERVICES](https://www.hollandhart.com/healthcare-services)

Healthcare Law | Hospital Law | H x +

hollandhart.com/healthcare-services

OVERVIEW

MENU INTRODUCTION PEOPLE

HOLLAND & HART


CLICK HERE FOR COVID-19 RESOURCES FOR HEALTHCARE PROFESSIONALS


Search by Keyword


PRACTICES/INDUSTRIES


NEWS AND INSIGHTS

CONTACTS

  
**Blaine Benard**  
Partner  
Salt Lake City

  
**Kim Stanger**  
Partner  
Boise

 **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.

**In recent years, healthcare has experienced dramatic change, extraordinary competition, and increasingly complex regulation.**

Our experienced attorneys help clients navigate through and respond to these challenges. By remaining on the forefront of healthcare law, we are able to provide coordinated services to meet our clients' business, transactional, litigation, compliance and regulatory needs.

**Clients We Serve**

- Hospitals
- Individual medical providers
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)
- Health information exchanges (HIEs)
- Practice managers and administrators
- Insurance providers
- Associations (IPAs)
- Health plans
- Health care providers
- Health care companies
- Rehabilitation centers
- Extended and eldercare facilities

Free articles and webinars

8:26 PM 11/4/2020

# QUESTIONS?



Kim C. Stanger  
office 208-383-3913  
cell 208-409-7907  
[kcstanger@hollandhart.com](mailto:kcstanger@hollandhart.com)