

CONFIDENTIALITY, SECURITY, AND DOCUMENTATION



KIM C. STANGER

Idaho Health Care Ass'n

(4-22)

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

OVERVIEW

- Confidentiality obligations
 - Use and disclosure rules
 - Breach reporting
- Security obligations
 - Cybersecurity threats
 - Relevant laws
 - Resources
- Patient rights, especially right of access
- Documentation suggestions



ACTUAL CHART BLOOPERS

- *The patient had no history of suicides.*
- *The patient refused autopsy.*
- *[Patient] has no rigors or shaking chills, but her husband states she was very hot in bed last night."*
- *The patient has been depressed since she began seeing me in 1993.*
- *MD order: "Walk in hell."*
- *Fecal heart tones heard.*
- *Large brown BM up walking in halls.*
- *Occasional, constant infrequent headaches.*
- *Patient was in his usual state of good health until his airplane ran out of gas and crashed.*

ACTUAL CHART BLOOPERS

- *The patient is tearful and crying constantly. She also appears to be depressed.*
- *Patient had waffles for breakfast and anorexia for lunch.*
- *The skin was moist and dry.*
- *Skin: somewhat pale, but present.*
- *Patient was alert and unresponsive.*
- *Patient has two teenage children, but no other abnormalities.*
- *Patient lives at home with his mother, father, and pet turtle, who is presently enrolled in day care 3x a week.*

ACTUAL CHART BLOOPERS

- *Discharge status: Alive but without permission.*
- *Rectal exam revealed a normal size thyroid.*
- *[Patient] stated that she had been constipated for most of her life, until she got a divorce.*
- *I saw your patient today, who is still under our car for physical therapy.*
- *TheRapist in to see patient.*
- *The baby was delivered, the cord clamped and cut and handed to pediatrician, who breathed and cried immediately.*

ACTUAL CHART BLOOPERS

- *Both breasts are equal and reactive to light and accommodation.*
- *The lab test indicated abnormal lover function.*
- *The pelvic exam will be done later on the floor.*
- *While in the ER, [patient] was examined, x-rated, and sent home.*
- *Examination of genitalia was completely negative except for the right foot.*
- *Examination of genitalia reveals that he is circus sized.*

CONFIDENTIALITY LAWS AND REGULATIONS



CONFIDENTIALITY REQUIREMENTS

- Health Insurance Portability and Accountability Act ("HIPAA"), 45 CFR part 164
 - Privacy
 - Security
 - Breach reporting
- Facility regs, e.g.,
 - SNFs: 42 CFR 483.70(i)
 - ALFs: IDAPA 16.03.22.550
 - HHA: 42 CFR 484.110(d)
 - Hospice: 42 CFR 418.104(c)
- Provider laws and regs.
- Substance Use Disorder records, 42 CFR part 2
- Common law privacy torts, e.g.,
 - Public disclosure of private facts
 - Intrusion upon seclusion
- Negligence per se
 - Based on violation of statutory duty

SNF CONFIDENTIALITY

- “The facility must keep confidential all information contained in the resident’s records, regardless of the form or storage method of the records, except when release is—
 - (i) To the individual, or their resident representative where permitted by applicable law;
 - (ii) Required by Law;
 - (iii) For treatment, payment, or health care operations, as permitted by and in compliance with 45 CFR 164.506;
 - (iv) For public health activities, reporting of abuse, neglect, or domestic violence, health oversight activities, judicial and administrative proceedings, law enforcement purposes, organ donation purposes, research purposes, or to coroners, medical examiners, funeral directors, and to avert a serious threat to health or safety as permitted by and in compliance with 45 CFR 164.512.”

(42 CFR 483.70(i)(2); see also *id.* at 483.10(h)(3) and 483.20(f)(5); CMS SOM App. PP)

ALF CONFIDENTIALITY

- “Each resident must have the right to confidentiality of personal and clinical records.”

(IDAPA 16.03.22.550.09)

- “Each resident must have ... the right to confidentiality and privacy concerning their medical or dental condition and treatment.”

(IDAPA 16.03.22.550.12(c))

- “The facility must safeguard confidential information against loss, destruction, and unauthorized use.”

(IDAPA 16.03.22.330.03)

HHA CONFIDENTIALITY

- “The patient has the right to ... have a confidential clinical record. Access to or release of patient information and clinical records is permitted in accordance with [HIPAA,] 45 CFR parts 160 and 164.”

(42 CFR 484.50(c)(6); *see also* CMS SOM App.B)

- “The clinical record, its contents, and the information contained therein must be safeguarded against loss or unauthorized use. The HHA must be in compliance with the rules regarding personal health information set out at 45 CFR parts 160 and 164.”

(42 CFR 484.110(d))

HOSPICE CONFIDENTIALITY

- “The patient has the right to ... have a confidential clinical record. Access to or release of patient information and clinical records is permitted in accordance with [HIPAA,] 45 CFR parts 160 and 164.”

(42 CFR 418.52(c)(5); see also CMS SOM App. M)

- “The clinical record, its contents and the information contained therein must be safeguarded against loss or unauthorized use. The hospice must be in compliance with the Department’s rules regarding personal health information as set out [in HIPAA, 45 CFR parts 160 and 164.]”

(42 CFR 418.104(c))

COMPLY WITH MOST RESTRICTIVE LAW



**More
restrictive law**

HIPAA

**Less restrictive
law**

- HIPAA preempts less restrictive laws.
- Comply with more restrictive law, e.g.,
 - 42 CFR part 2
 - State licensing requirements
 - Federal regulations
 - Others?

HIPAA CRIMINAL PENALTIES

- Applies if employees or other individuals obtain or disclose protected health info from covered entity without authorization.

Conduct	Penalty
Knowingly obtain info in violation of the law	<ul style="list-style-type: none">• \$50,000 fine• 1 year in prison
Committed under false pretenses	<ul style="list-style-type: none">• 100,000 fine• 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	<ul style="list-style-type: none">• \$250,000 fine• 10 years in prison

HIPAA CIVIL PENALTIES

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none"> • \$127* to \$63,973* per violation • Up to \$25,630* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Violation due to reasonable cause	<ul style="list-style-type: none"> • \$1,280* to \$63,973* per violation • Up to \$102,522* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none"> • \$12,794* to \$63,973* per violation • Up to \$256,305* per type per year • Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none"> • At least \$63,973* per violation • Up to \$1,754,698* per type per year • Penalty is mandatory

(45 CFR 102.3, 160.404; 85 FR 2879)

HIPAA ENFORCEMENT

- State attorney general can bring lawsuit.
 - \$25,000 fine per violation + fees and costs
- 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.

HIPAA ENFORCEMENT

- 2009: HITECH Act requires HHS to establish a methodology for the distribution of a percentage of a civil monetary penalty or settlement collected for noncompliance with the HIPAA Rules to an individual harmed by the noncompliance.

(42 USC 17939(c)(2)-(3))



***Breaking
News***

- 4/6/22: OCR seeks comments on the regulation:
 - What “harm” will trigger damages
 - Method for allowing patients to recover percentage of fines or settlements.

(87 FR 19833)

HIPAA AVOIDING PENALTIES

You can likely avoid HIPAA 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.*

HIPAA PROTECTED HEALTH INFO



PROTECTED HEALTH INFO

- Protected health info (“PHI”) =
 - **Individually identifiable** health info, i.e., info that could be used to identify individual;
 - **Concerns physical or mental health, health care, or payment;**
 - Created or received by covered entity in its capacity as a healthcare provider; and
 - Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.
- Not “de-identified” info.

(45 CFR 160.103)



IS IT PROTECTED HEALTH INFO?

- Facility directory that includes patient's name but no medical info?
- Text to doctor that refers to resident by initials?
- Info that does not include patient's name but does include record number or other medical info?
- Photo of patient so long as there is no name?
- Patient's financial info but no medical info?
- Response to negative internet review so long as no medical info disclosed?
- Employee's health record?

HIPAA AND EMPLOYMENT RECORDS

Employer rendered healthcare to employee (e.g., vaccination, drug test, etc.)

- **HIPAA applies**
- To use/disclose PHI, need either:
 - Employee authorization, or
 - HIPAA exception.

(67 FR 53191)

Employer obtained info solely in its capacity as the employer (e.g., from employee or other provider)

- HIPAA does not apply.
 - “Employment records” excluded from definition of PHI.
- Other laws may apply, e.g., ADA.

ADA AND EMPLOYEE HEALTH INFO

Under ADA:

- Employer may ask about employee vaccination status.
 - Employer must keep employee health info confidential, including vaccination status.
 - Store separately from personnel file.
 - May disclose to supervisors or managers to allow necessary accommodations.
 - May require those who are not vaccinated to wear a mask subject to reasonable accommodation.
- (29 CFR 1630.14; EEOC Guidance (5/21))
- Maybe allow employee to display something confirming that they may work without a mask but do not require notice of vaccination status.
 - Maybe allow voluntary vaccination stickers.

➤ *Check local laws.*

HIPAA PRIVACY RULE



**Don't access
if don't need
to know.**

**Don't disclose
unless fit
exception or have
authorization**

**Implement
reasonable
safeguards**

PROHIBITED ACTIONS

- Cannot use, access or disclose PHI unless:
 - Permitted by HIPAA, or
 - Have patient's or personal rep's authorization.
- Applies to
 - Unauthorized disclosure outside covered entity.
 - Unauthorized use within covered entity.
 - Unauthorized access from within or outside covered entity.

(45 CFR 164.502)

AUTHORIZATION

- Must obtain a valid written authorization to use or disclose protected PHI:
 - Psychotherapy notes.
 - Marketing
 - Sale of PHI
 - Research
 - For all other uses or disclosures unless a regulatory exception applies.
- Authorization may not be combined with other documents.
- Authorization must contain required elements and statements.
- Signed by patient or personal representative.

(45 CFR 164.508)

PERSONAL REPRESENTATIVES

- Under HIPAA, treat the personal rep as if they were the 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))

- In Idaho, personal reps =
 - Court appointed guardian
 - Agent in DPOA
 - Spouse
 - Adult child
 - Parent
 - Delegation of parental authority
 - Other appropriate relative
 - Any other person responsible for patient's care

(IC 39-4504)

PERSONAL REPRESENTATIVES

- Not required to treat personal rep as patient (i.e., do not disclose PHI to them) if:
 - Minor has authority to consent to care.
 - 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)

TREATMENT, PAYMENT OR 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)

TREATMENT, PAYMENT OR OPERATIONS

- If agree with patient to limit use or disclosure for treatment, payment, or healthcare operations, you must abide by that agreement except in an emergency.

(45 CFR 164.506 and 164.522)

- *Don't agree to limit disclosures for treatment, payment or operations.*
 - *Exception: disclosure to insurers; see discussion below.*
- *Beware asking patient for list of persons to whom disclosure may be made.*
 - *Creates inference that disclosures will not be made to others.*
 - *If list persons, ensure patient understands that we may disclose to others per HIPAA.*

BUSINESS ASSOCIATES

- May disclose PHI to business associates if have valid business associate agreement (“BAA”).

(45 CFR 164.502)

- Business associates =
 - Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity.
 - Covered entities acting as business associates.
 - Subcontractors of business associates.
 - Not members of workforce.

(45 CFR 160.103)

- Failure to execute BAA = HIPAA violation
 - May subject you to HIPAA fines.
 - Based on recent settlements, may expose you to liability for business associate’s misconduct.

[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

BUSINESS ASSOCIATES

See also CMS regulations:

- SNF: “The facility may release information that is resident-identifiable to an agent only in accordance with a contract under which the agent agrees not to use or disclose the information except to the extent the facility itself is permitted to do so.”

(42 CFR 483.20(f)(5))

- HHA: “The HHA and agent acting on behalf of the HHA in accordance with a written contract must ensure the confidentiality of all patient identifiable information contained in the clinical record...”

(42 CFR 484.40)

PERSONS INVOLVED IN CARE

- 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)

FACILITY DIRECTORY

- May disclose limited PHI for facility directory if:
 - Gave patient notice and patient does not object, and
 - Requestor asks for the person by name.
- If patient unable to agree or object, may use or disclose limited PHI for directory if:
 - Consistent with person's prior decisions, and
 - Determine that it is in patient's best interests
- Disclosure limited to:
 - Name
 - Location in facility
 - General condition
 - Religion, if disclosure to minister

(45 CFR 164.510)

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

VERIFICATION

- Before disclosing PHI:
 - Verify the identity and authority of person requesting info if he/she is not known.
 - E.g., ask for SSN or birthdate of patient, badge, credentials, etc.
 - Obtain any documents, representations, or statements required to make disclosure.
 - E.g., written satisfactory assurances accompanying a subpoena, or representations from police that they need info for immediate identification purposes.

(45 CFR 164.514(f))

- Portals should include appropriate access controls.

(OCR Guidance on Patient's Right to Access Their Information)

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.

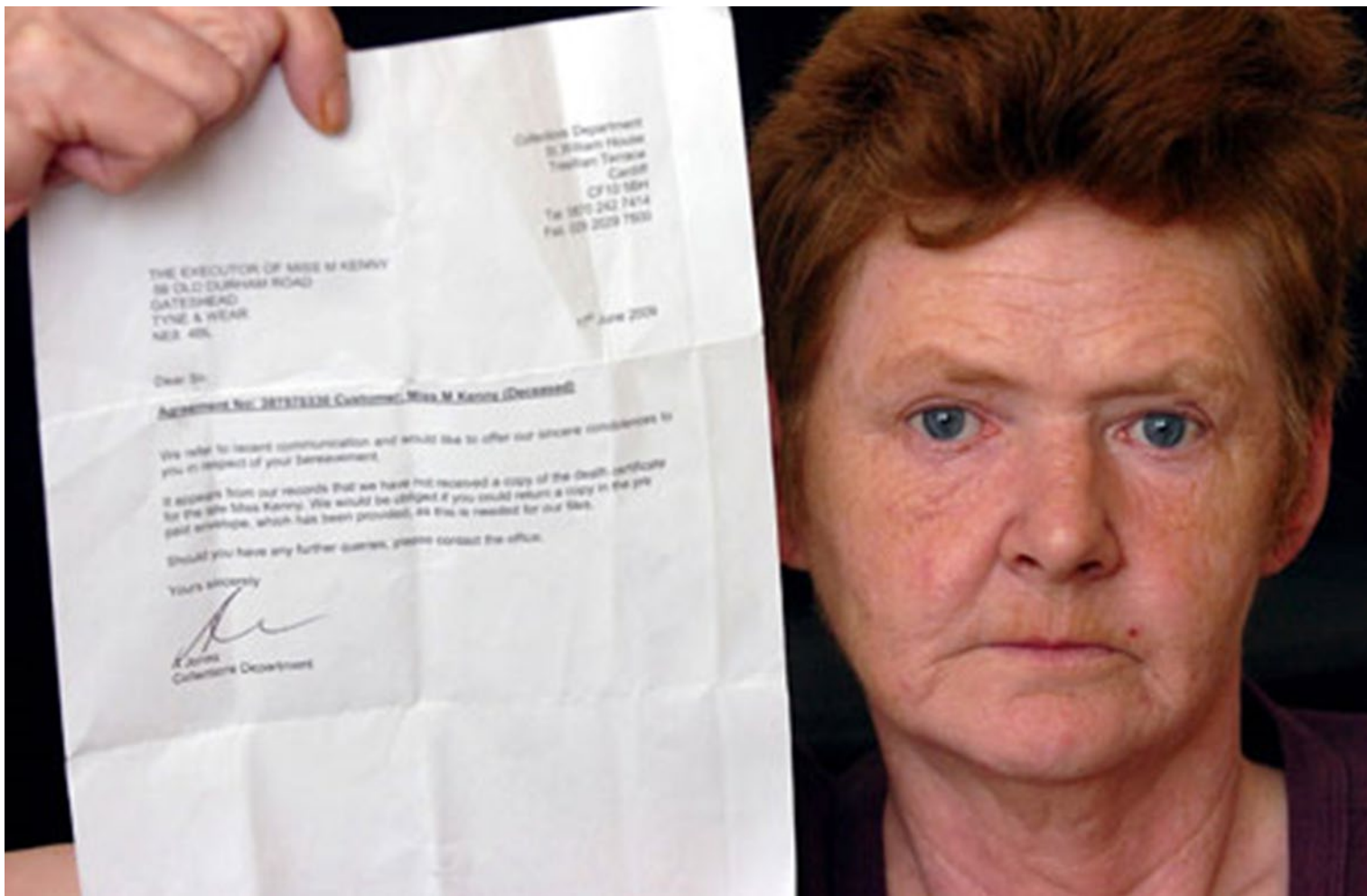
(45 CFR 164.502 and .514)

MINIMUM NECESSARY STANDARD

- Must adopt policies addressing—
 - Internal uses of PHI:
 - Identify persons who need access.
 - Draft policies to limit access accordingly.
 - External disclosures of PHI:
 - Routine disclosure: establish policies.
 - Non-routine disclosures: case-by-case review.
 - Requests for PHI:
 - Routine requests: establish policies.
 - Non-routine requests: case-by-case review.

(45 CFR 164.502 and .514)

HIPAA BREACH NOTIFICATION RULE



BREACH NOTIFICATION

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

(45 CFR 164.400 et seq.)

“BREACH” OF UNSECURED PHI

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

unless an exception applies.

(45 CFR 164.402)

“BREACH” OF UNSECURED PHI

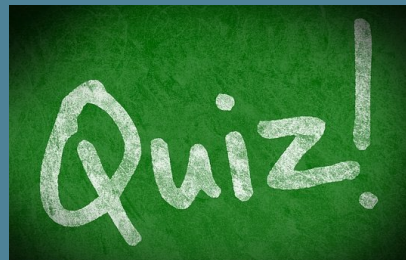
- “Breach” defined to exclude the following:
 - Unintentional acquisition, access or use by workforce member if made in good faith, within scope of authority, and PHI not further disclosed in violation of HIPAA privacy rule.
 - Inadvertent disclosure by authorized person to another authorized person at same covered entity, business associate, or organized health care arrangement, and PHI not further used or disclosed in violation of privacy rule.
 - Disclosure of PHI where covered entity or business associate have good faith belief that unauthorized person receiving info would not reasonably be able to retain info

(45 CFR 164.402)

INCIDENTAL DISCLOSURES

- “Incidental disclosures” do not trigger breach reporting so long as the provider had reasonable safeguards in place.
 - Incidental disclosures do not violate the privacy rule, so they are not reportable “breach.”
- Reasonable safeguards might include, e.g.,
 - Speaking quietly when discussing patient’s condition to avoid others overhearing.
 - Avoiding use of patient names in public areas.
 - Isolating or locking file cabinets or records rooms.

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html>



IS IT A REPORTABLE BREACH?

- In response to call, employee discloses that patient is receiving care, but no other info.
- Employee faxes patient medication info to wrong physician.
- Curious employee accesses PHI without a need to know.
- Employee responds to negative internet review about resident's care.
- Employee loses a smart phone that contains unencrypted PHI about a patient.
- Unencrypted laptop containing PHI is stolen from employee's home.
- Employee contacts family members to try to get them to pay for their mother's care.
- Visitor takes photos of his mother, but the photo includes other residents.
- Visitor overhears two CNAs talking about a patient.

NOTICE TO INDIVIDUAL

- Without unreasonable delay but no more than 60 days of discovery.
 - When known by anyone other than person who committed breach.
- Written notice to individual.
 - By mail.
 - Must contain elements, including:
 - Description of breach
 - Actions taken in response
 - Suggested action individual should take to protect themselves.

(45 CFR 164.404(d))

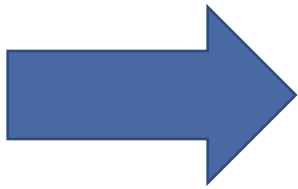
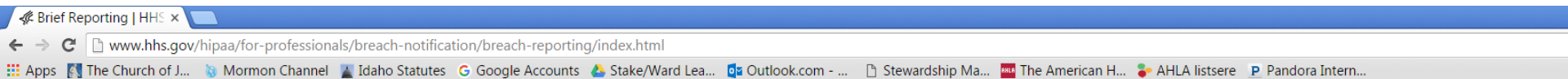
NOTICE TO HHS

- If breach involves fewer than 500 persons:
 - Submit to HHS annually within 60 days after end of calendar year in which breach was discovered (i.e., by March 1).
- If breach involves 500 or more persons:
 - Notify HHS contemporaneously with notice to individual or next of kin, i.e., without unreasonable delay but within 60 days.

(45 CFR 164.408)

- Submit report at <http://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](https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html)



- HIPAA for Professionals
- 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

Text Resize A A A Print Share f t +

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](#)

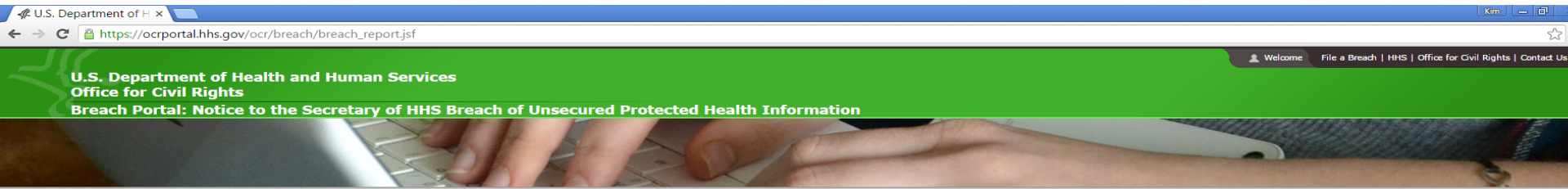
[View a list of Breaches Affecting 500 or More Individuals](#)

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



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	

NOTICE TO MEDIA

- If breach involves unsecured PHI of more than 500 residents in a state, covered entity must notify prominent media outlets serving that state (e.g., issue press release).
 - Without unreasonable delay but no more than 60 days from discovery of breach.
 - Include same content as notice to individual.

(45 CFR 164.406)

IDAHO IDENTITY THEFT STATUTE

- Generally, requires all commercial entities to immediately investigate and notify subject persons if there is a
 - Breach of computer system
 - Resulting in illegal acquisition
 - Of certain unencrypted computerized personal info
 - Name + certain other identifiers (e.g., SSN, driver's license, credit card number + PIN or password, etc.)
 - Actual or reasonably likely misuse of personal info
- \$25,000 fine if fail to notify persons.
- Compliance with HIPAA likely satisfies Idaho statute.

(IC 28-51-104)

CYBERSECURITY



HIPAA SECURITY RULE

Covered entities and business associates must:

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

(45 CFR 164.301 et seq.)

- Protect ePHI:
- Confidentiality
 - Integrity
 - Availability

FACILITY SECURITY REGULATIONS

- **SNF** must have “[a] system of medical documentation that preserves resident information, protects confidentiality of resident information, and secures and maintains the availability of records.” (42 CFR 483.73(b)(5))
- **ALF** “must safeguard confidential information against loss, destruction, and unauthorized use.” (IDAPA 16.03.22.330.03)
- **HHA** must have “[a] system of medical documentation that preserves patient information, protects confidentiality of patient information, and secures and maintains the availability of records.” (42 CFR 484.102(b)(4))
- **Hospice** must have “[a] system of medical documentation that preserves patient information, protects confidentiality of patient information, and secures and maintains the availability of records.” (42 CFR 484.102(b)(4))

CYBERSECURITY IN HEALTHCARE

- Ransomware encrypts your IT system so that you may not access it, including:
 - Patient records
 - Financial records
 - Employment records
- Hacker accesses data on your system
- Hacker manipulates or corrupts data on medical devices
- Employee error leads to access to thousands of patient records



What are the consequences to your organization?

CYBERSECURITY IN HEALTHCARE

- Ransomware encrypts your IT system so that you may not access it, including:
 - Patient records
 - Financial records
 - Employment records
- Hacker accesses data on your system
- Hacker manipulates or corrupts data on medical devices
- Employee error leads to access to thousands of patient records



- Harm to patients
- Inability to access data
- Corruption of data
- Forced to move patients
- Disruption of operations
- Lost revenue
- Cost of response
- Loss or damage to equipment
- Bad public relations
- Fines and penalties
- Lawsuits
- Others?

[HTTPS://WWW.HHS.GOV/SITES/DEFAULT/FILES/2021-RETROSPECTIVE-AND-2022-LOOK-AHEAD-TLPWHITE.PDF](https://www.hhs.gov/sites/default/files/2021-retrospective-and-2022-look-ahead-tlpwhite.pdf)



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



Health Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead

03/03/2022

HHS CYBERSECURITY REPORT (3/22)

Healthcare Cybersecurity Events of Interest: July 2021, Part 3



IBM Annual Data Breach Cost Report

- IBM released their 2021 [Cost of a Data Breach report](#)
- They assessed that the data breaches in 2021 cost a company \$4.24 million per incident on average, which is the highest figure in the 17-year history of this report.
 - In the United States, data breach costs averaged about \$9 million per incident.
 - The cost of breaches increased about 10% in a year, and IBM largely attributes that to the remote workforce which has increasingly been in place since the beginning of the pandemic.
 - On that note, IBM also found that the average cost of a breach increased about \$1 million when remote work was a factor in the breach.
- The average healthcare breach was \$9.23 million, which was a dramatic increase, about 30%, from \$7.13 million in 2019.

11

Consecutive years
healthcare had the highest
industry cost of a breach

Healthcare organizations experienced the
highest average cost of a data breach,
for the eleventh year in a row.

\$180

Per record cost of
personally identifiable
information

Customer personally identifiable
information (PII) was the most common
type of record lost, included in 44% of breaches.



HHS CYBERSECURITY REPORT (3/22)

Healthcare Cybersecurity Events of Interest: December 2021, Part 5



Coveware Quarterly Ransomware Report: 2021 Q4

Average Ransom Amount up Sharply in Q4 2021

Average Ransom Payment

\$322,168

+130% from Q3 2021

Median Ransom Payment

\$117,116

+63% from Q3 2021

The Most Common Ransomware Variants in Q4 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q3 2021
1	Conti V2	19.4%	-
2	LockBit 2.0	16.3%	+2
3	Hive	9.2%	+5
4	Mespinoza	4.1%	-2
5	Zeppelin	3.6%	+1
5	BlackMatter	3.6%	+4
6	Karakurt	3.1%	New in Top Variants
6	Suncrypt	3.1%	+2
6	AvosLocker	3.1%	New in Top Variants

Top 10: Market Share of the Ransomware attacks



[HTTPS://WWW.HHS.GOV/BLOG/2022/02/28/IMPROVING-CYBERSECURITY-POSTURE-HEALTHCARE-2022.HTML](https://www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html)



[A-Z Index](#)

- [About HHS](#)
- [Programs & Services](#)
- [Grants & Contracts](#)
- [Laws & Regulations](#)

[Home](#) > [Blog](#) > [Improving the Cybersecurity Posture of Healthcare in 2022](#)

Categories
Coronavirus (8)
Fraud (1)
Global Health (1)
Grants and Contracts (1)
Health Data (1)
Health IT (3)
HIPAA (1)
Holidays and Observances (2)
Prevention and Wellness (3)
Public Health and Safety (4)
Research (2)

61

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

Print

Share [f](#) [t](#) [e](#)

Improving the Cybersecurity Posture of Healthcare in 2022

February 28, 2022 | By: [Lisa Pino](#), Director for Office for Civil Rights (OCR)

Summary: Encourages HIPAA covered entities and business associates to strengthen their cyber posture in 2022.



OCR DIRECTOR PINO'S BLOG (2/28/22)

"I cannot underscore enough the importance of enterprise-wide risk analysis.... You should fully understand where all electronic protected health information (ePHI) exists across your organization - from software, to connected devices, legacy systems, and elsewhere across your network.... Some best practices include:

- "Maintaining offline, encrypted backups of data and regularly test your backups;
- "Conducting regular scans to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface;
- "Regular patches and updates of software and Operating Systems; and
- "Training your employees regarding phishing and other common IT attacks."

(Lisa Pino, Director of Office for Civil Rights (2/28/22))

[HTTPS://WWW.PHE.GOV/PREPAREDNESS/PLANNING/405D/PAGES/HIC-PRACTICES.ASPX](https://www.phe.gov/preparedness/planning/405d/Pages/hic-practices.aspx)

Top Healthcare Cybersecurity Threats

1. E-mail phishing attacks
2. Ransomware attacks
3. Loss or theft of equipment or devices
4. Insider data loss
5. Connected medical

The screenshot shows a web browser window displaying the PHE website. The browser's address bar shows the URL: <https://www.phe.gov/preparedness/planning/405d/Pages/hic-practices.aspx>. The website header includes the U.S. Department of Health & Human Services logo and the Office of the Assistant Secretary for Preparedness and Response. The main navigation bar has tabs for Preparedness, Emergency, and About ASPR. The page title is "Public Health Emergency" with the subtitle "Public Health and Medical Emergency Support for a Nation Prepared". The breadcrumb trail is: PHE Home > Preparedness > Planning > Aligning Health Care Industry Cybersecurity Approaches > Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. The main content area features the title "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" and a search bar. The text describes the HICP publication and lists three key resources: the HICP main document, Technical Volume 1 for small organizations, and Technical Volume 2 for medium and large organizations. A sidebar on the right contains a search box and a list of links under the heading "Cybersecurity Act of 2015, Section 405(d)", including "Health Industry Cybersecurity Practices", "About the CSA 405(d) Task Group", "Cybersecurity Reports and Tools", and "Get Involved". A large blue arrow points from the sidebar towards the main content area, labeled "Suggested Practices". The Windows taskbar is visible at the bottom of the browser window.

U.S. Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response

Preparedness Emergency About ASPR

Public Health Emergency
Public Health and Medical Emergency Support for a Nation Prepared

Search...

PHE Home > Preparedness > Planning > Aligning Health Care Industry Cybersecurity Approaches > Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, and resources and templates:

- ▶ **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP):** The HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.
- ▶ **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations:** Technical Volume 1 discusses the ten Cybersecurity Practices along with Sub-Practices for small health care organizations.
- ▶ **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations:** Technical Volume 2 discusses the ten Cybersecurity Practices along with Sub-Practices for medium and large health care organizations.

Cybersecurity Act of 2015, Section 405(d)

- ▶ Health Industry Cybersecurity Practices
- ▶ About the CSA 405(d) Task Group
- ▶ Cybersecurity Reports and Tools
- ▶ Get Involved

Suggested Practices

How To Spot A **PHISH**



What is Phishing? A technique used to fraudulently obtain usernames, passwords, credit card numbers, and other sensitive information.



Fraudulent emails typically ask you to:

- Open an attachment or,
- Click on a link, redirecting you to a malicious website.
- You may be prompted to enter personal information.

Types of Phishing Attacks



Spear Phishing: A highly targeted form of phishing that hones in on a specific group of individuals or organization.



Whaling: A form of phishing, targeted at executive level individuals.



Cloning: Whereby a legitimate email is duplicated but, the content is replaced with malicious links or attachments.

Anatomy of a Phishing Email

Contains links or attachments

Poor grammar and spelling

Requests personal or sensitive information

High sense of urgency and/or privacy

Discusses confidential subjects like salaries

Incentivizes through threat or reward



From: PayPal [service@paypal-australia.com.au]
To: [redacted]
Cc:
Subject: Your account has been limited

: 24 AM

1. Fake sender domain.
(not service@paypal-australia.com.au)

PayPal™

2. Suspicious Subject and content.

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

3. Bad grammar

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.

Click to follow link

[Log in your account now](#)

4. Hovering over link reveals suspicious URL.

PayPal Email ID PP32260008777636

From: Costco Shipping Agent <manager@cbcbuilding.com>
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>



Unfortunately the delivery of your order [COS-0077945599](#) was cancelled since the specified address of the recipient was not correct. You are recommended to complete [this form](#) and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.



From: LinkedIn Accounts

To: Amy B; Bryan; Dennis B; Gary; Jim C; Geff H; Louise K; Patty; Ihor M; Ted N; Chris P;

Subject: Account suspended!



Your LinkedIn account was suspended due to spam messages. To unlock your account open this link www.linkedin.com

Thank you for using LinkedIn!

The LinkedIn Team



Refund Notification

Due to a system error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE


You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

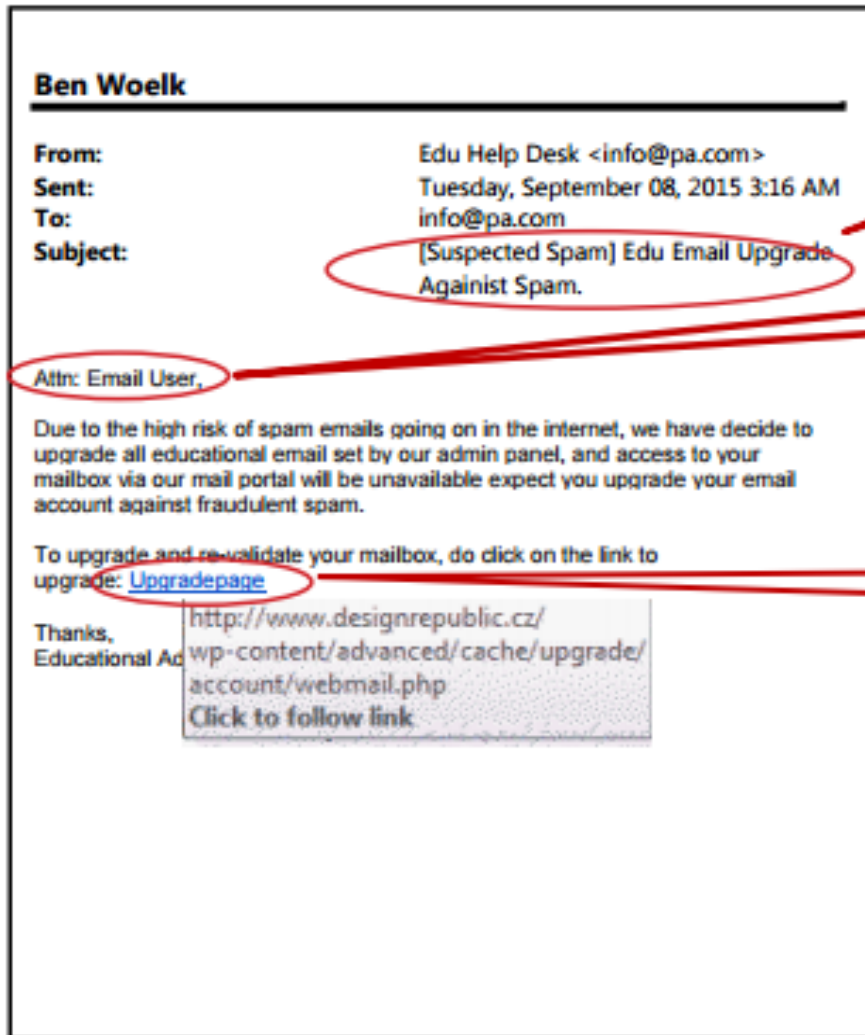
After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](https://www.amazon.com)

Email ID: 

MAY ALSO APPEAR TO BE INTERNAL E-MAILS



Spelling

Generic addressee

Link goes to external site

From: HelpDesk [mailto:xxxxx@connect.ust.hk]

Sent: Wednesday, April 12, 2017 2:23 PM

To: [redacted]

Subject: Validate Email Account

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

[Validate Email Account](#)

Sincerely

IT Help Desk

Office of Information Technology

The University

E-MAIL PHISHING ATTACKS

- Do you know the sender?
- Did you expect the e-mail?
- Is the subject generic, urgent, strange, or suspicious?
- Are there spelling, grammar, or other indicators that the tone or style is off?
- Does the e-mail require you to take some action, e.g.,
 - Disclose confidential info
 - Click on link
 - Open attachment
- Did you hover over link to see the URL destination?



Do NOT

- ***Open attachment***
- ***Click on link***
- ***Input info***

Regulatory Initiatives

- Key threats:
 - Phishing
 - Exploiting known vulnerabilities
 - Weak cyber practices
- Best practices to address threats
- Resources for covered entities

Other Administrative Simplification Rules

OCR Quarter 1 2022 Cybersecurity Newsletter

Defending Against Common Cyber-Attacks

Throughout 2020 and 2021, hackers have targeted the health care industry seeking unauthorized access to valuable electronic protected health information (ePHI). The number of breaches of unsecured ePHI reported to the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) affecting 500 or more individuals due to hacking or IT incidents increased 45% from 2019 to 2020.¹ Further, the number of breaches due to hacking or IT incidents accounted for 66% of all breaches affecting 500 or more individuals reported to OCR in 2020.²

Although some attacks may be sophisticated and exploit previously unknown vulnerabilities (*i.e.*, zero-day attack), most cyber-attacks could be prevented or substantially mitigated if HIPAA covered entities and business associates ("regulated entities") implemented HIPAA Security Rule requirements to address the most common types of attacks, such as phishing emails,³ exploitation of known vulnerabilities, and weak authentication protocols. If an attack is successful, the attacker often will encrypt a regulated entity's ePHI to hold it for ransom, or exfiltrate the data for future purposes including identity theft or blackmail. Cyber-attacks are especially critical in the health care sector as attacks on ePHI can disrupt the provision of health care services to patients. This newsletter explores preventative steps regulated entities can take to protect against some of the more common, and often successful, cyber-attack techniques.

Phishing

One of the most common attack vectors is phishing. Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information via electronic communication, such as email, by impersonating a trustworthy source.⁴ A recent report noted that 42% of ransomware attacks in Q2 2021 involved phishing.⁵ All regulated entities' workforce members should understand they have an important role in protecting the ePHI their organization holds from cyber-attacks. Part of that role involves being able to detect and take appropriate action if one encounters suspicious email. To ensure workforce members can take appropriate action, regulated entities should train their workforce members to recognize phishing attacks and implement a protocol on what to do when such attacks or suspected attacks occur (*e.g.*, report suspicious emails to appropriate IT personnel).

The Security Rule requires regulated entities to implement a security awareness and training program for all workforce members.⁶ A regulated entity's training program should be an ongoing, evolving process and be flexible enough to educate workforce members on new and current cybersecurity

OCR CYBERSECURITY NEWSLETTER (4/22)

Phishing

- Train workforce how to recognize, respond to, and report phishing attacks or suspicious e-mails.
- Educate staff about current and evolving cyberthreats.
- Send periodic security reminders, e.g., simulated phishing e-mails to gauge awareness.
- Implement anti-phishing technologies, e.g.,
 - Flags external e-mails
 - Verifies e-mails do not originate from known malicious sites
 - Scanning links and attachments and removing them.

OCR CYBERSECURITY NEWSLETTER (4/22)

Weak Cybersecurity Practices

- Weak authentication, e.g., weak passwords or single factor authentication.
- Beware remote access; use stronger authentication, e.g., 2-factor authentication.
- Beware privileged access management systems.
- Conduct periodic assessments.

OCR CYBERSECURITY NEWSLETTER (4/22)







Exploiting Known Vulnerabilities

- Be aware of known vulnerabilities, e.g., subscribe to alerts from:
 - Cybersecurity and Infrastructure Security Agency (“CISA”).
 - HHS Health Sector Cybersecurity Coordination Center (“HC3”)
- Apply vendor patches.
- Upgrade or replace vulnerable apps and devices.
- Conduct risk assessment and periodic penetration tests.

SECURITY RISK ASSESSMENT

ov/providers-professionals/security-risk-assessment-tool



Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates |      

in Partnership with the
National Learning Consortium 

Newsroom | FAQs | Multimedia | Implementation Resources

Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs


Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Security Risk Assessment > Security Risk Assessment Tool

 Print |  Share

Security Risk Assessment

Guide to Privacy and Security of Electronic Health Information

Health IT Privacy and Security Resources

Mobile Device Privacy and Security

Model Notices of Privacy Practices

Patient Consent for eHIE

Privacy & Security Training Games

Cybersecurity

Security Risk Assessment

Security Risk

Security Risk Assessment Tool

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

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a

downloadable [SRA Tool \[.exe - 69 MB\]](#) to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

We understand that users with Windows 8.1 Operating Systems may experience difficulties downloading the SRA Tool, we are working to resolve the issue and will post here when a resolution is identified and implemented.



Top 10 Myths of Security Risk Analysis

As with any new program or regulation, there may be misinformation making the rounds.

[Read the top 10 list distinguishing fact from fiction.](#)

SRA Tool (Windows version)



[Download Tool](#)

HTTPS://WWW.CISA.GOV/STOP RANSOMWARE

Stop Ransomware | CISA

https://www.cisa.gov/stopransomware

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



Search



**WHAT IS
RANSOMWARE?**

LEARN MORE

**HAVE YOU
BEEN HIT BY
RANSOMWARE?**

LEARN MORE

Known Exploited
Vulnerabilities
Catalog

cisa.gov

UPdated



https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Locum Tenens Billi...pdf

Show all



Raining now 10:28 PM 3/16/2022

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

How to Protect Your Networks from

<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 government and private industry best practices

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

Recommended Practices

1. E-mail protection system
 2. Endpoint protection system
 3. Access management
 4. Data protection and loss prevention
 5. Network management
 6. Vulnerability management
 7. Incident response
 8. Medical device security
 9. Cybersecurity policies
- Sample Forms
 - Resources

/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)

agencies/asa/ocio/hc3/index.html



Search...



Tools ?

[About HHS](#) [Programs & Services](#) [Grants & Contracts](#) [Laws & Regulations](#)

[Home](#) > [About](#) > [Agencies](#) > [ASA](#) > [Office of the Chief Information Officer \(OCIO\)](#) > Health Sector Cybersecurity Coordination Center (HC3)

Assistant Secretary for Administration (ASA)

About ASA

EEO, Diversity & Inclusion



Office of Business Management & Transformation (OBMT)



Office of Human Resources (OHR)



Office of the Chief Information Officer (OCIO)



About OCIO

What We Do

Our Mission

Text Resize **A A A**

Print

Share



Health Sector Cybersecurity Coordination Center (HC3)

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

Threat Briefs

Highlights relevant cybersecurity topics and raise the HPH sector's situational

Sector Alerts

Provides high-level, situational background information and context for technical and

Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs

Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

HealthIT.gov > For Providers & Professionals > Privacy and Security

Print | Share

Privacy and Security

Health Information Privacy, Security, and Your EHR

Ensuring privacy and security of health information, including information in electronic health records (EHR), is a key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.

Your practice, not your EHR vendor, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR and comply with The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules and CMS' Meaningful Use requirements.

Ensuring the Security of Electronic Health Records

0:00 / 2:34



Cybersecure:

Your Medical Practice

[Play the Game](#)

Integrating Privacy & Security Into Your Medical Practice

The HIPAA Privacy and Security Rules protect the privacy and security of your health information.

Privacy & Security 10 Step Plan

Ensuring privacy and security of health information in an EHR is a vital part of Meaningful Use. Security risk analysis and management are foundational to...

Privacy & Security and Meaningful Use

HIPAA privacy and security requirements are embedded in the Medicare and Medicaid EHR Incentive Programs through the following...

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

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

Print

Share



Privacy

Security

[Summary of the Security Rule](#)

[Guidance](#)

[Combined Text of All Rules](#)

Breach Notification

Compliance & Enforcement

Special Topics

Patient Safety

Covered Entities & Business Associates

Training & Resources

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](#)

82
[Administrative Safeguards](#)

[Physical Safeguards](#)

[HTTPS://WWW.HEALTHIT.GOV/SITES/DEFAULT/FILES/PDF/PRIVACY/PRIVACY-AND-SECURITY-GUIDE.PDF](https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf)

1. Importance of Privacy and Security Matters
2. HIPAA Rules
3. Patient's Rights
4. EHR, HIPAA Security, and Cybersecurity
5. Meaningful Use Rules
6. 7-Step Approach for Security Management
7. Breach Notification Rules

The Office of the National Coordinator for
Health Information Technology



Guide to Privacy and Security of Electronic Health Information

Version 2.0
April 2015

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

Putting the I in HealthIT
HealthIT.gov

ENCRYPTION

- Encryption is an addressable standard per 45 CFR 164.312:
 - (e)(1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.
 - (2)(ii) *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
- ePHI that is properly encrypted is “secured”.
 - Not subject to breach reporting.
- OCR presumes that loss of unencrypted laptop, USB, mobile device is breach.

BEWARE MOBILE DEVICES



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



Newsroom

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [HIPAA Compliance and Enforcement](#) > [Resolution Agreements](#) > Business Associate's Failure to Safeguard PHI Leads to Settlement

HIPAA for Professionals

Regulatory Initiatives

Privacy



Security



Breach Notification



Compliance & Enforcement



Enforcement Rule

Enforcement Process

Enforcement Data

Text Resize **A A A**

Print

Share



Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to \$650,000 HIPAA Settlement

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of \$650,000 and a corrective action plan.

"Business associates must implement the protections of the HIPAA Security Rule for the electronic protected health information they create, receive, maintain, or transmit from covered entities," said U.S. Department of Health and Human Services Office for Civil Rights (OCR) Director Jocelyn Samuels. "This includes an enterprise-wide risk analysis and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule." OCR initiated its investigation on April 17, 2014, after



BEWARE MOBILE DEVICES

providers-professionals/your-mobile-device-and-health-information-privacy-and-security



Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates



in Partnership with the
National Learning Consortium

Newsroom | FAQs | Multimedia | Implementation Resources



Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs

Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Your Mobile Device and Health Information Privacy and Security

Print | Share

Privacy & Security

Your Mobile Device and Health Information Privacy and Security



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



Read and Learn

- How Can You Protect and Secure Health Information When Using a Mobile Device?
- You, Your Organization and Your Mobile Device
- Five Steps Organizations Can Take To Manage Mobile Devices



Watch and Learn

- Worried About Using a Mobile Device for Work? Here's What To Do!
- Securing Your Mobile Device is Important!
- Dr. Anderson's Office Identifies a Risk



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)

PATIENT RIGHTS, INCLUDING RIGHT TO ACCESS INFO



HIPAA PATIENT RIGHTS

- Notice of Privacy Practices
- Request restrictions on use or disclosure.
- Receive communications by alternative means.
- **Access to info**
- Amendment of info
- Accounting of disclosures of info

(45 CFR 164.520 et. seq.)

HIPAA RIGHT OF ACCESS

- Resident 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.
 - * Proposed rule would shorten to 15 days.
 - May need to respond sooner under other laws.
- Must provide records in requested form if readily producible, including electronic form.
- May charge reasonable cost-based fee, i.e., cost of actual labor and materials in making copies, not administrative or retrieval fee.
- Limited exceptions to right to access.

(45 CFR 164.524)

HIPAA

DISCLOSURE DIRECTED BY PATIENT


- Individual or personal representative has right to direct that a copy of the record be transmitted to a third party.
- Written request signed by individual or personal representative and clearly identifies recipient and recipient's address.
 - Limits on charges apply.
 - Must transmit in manner, form and format requested if readily producible.
- Compare authorization:
 - Individual requests transmittal: individual request rules in 45 CFR 164.524 apply.
 - Third party requests transmittal: authorization rules in 45 CFR 164.508 apply.

(45 CFR 164.524; OCR Guidance on Access)


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

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

OCR RIGHT OF ACCESS INITIATIVE



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



Newsroom

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [HIPAA Compliance and Enforcement](#) > [Resolution Agreements](#) > Five enforcement actions hold healthcare providers accountable for HIPAA Right of Access

HIPAA for Professionals

Regulatory Initiatives

Privacy



Security



Breach Notification



Compliance & Enforcement



Enforcement Rule

Enforcement Process

Enforcement Data

93

Resolution Agreements

Text Resize **A A A**

Print

Share



Five enforcement actions hold healthcare providers accountable for HIPAA Right of Access

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) announced the resolution of five investigations in its HIPAA Right of Access Initiative, bringing the total number of these enforcement actions to twenty-five since the initiative began. The Health Insurance Portability and Accountability Act, or HIPAA, for short, gives people the right to see and get copies of their health information from their healthcare providers and health plans. After receiving a request, a HIPAA covered entity has 30 days (or 60 days if an extension is applicable) to provide an individual or their representative with their records in a timely manner. OCR has taken the following enforcement actions that underscore the importance and necessity of compliance with the HIPAA Right of Access:

- [Read the HHS Press Release](#)
- Read the [Advanced Spine & Pain Management \(ASPM\)](#) Resolution Agreement and Correction Action Plan
- Read the [Denver Retina Center](#) Resolution Agreement and Correction Action Plan

SNF RIGHT OF ACCESS

- SNF

- “The facility must provide the resident with access to personal and medical records pertaining to him or herself, upon an oral or written request, in the form and format requested by the individual, if it is readily producible ... (including in an electronic form or format when such records are maintained electronically); or, if not, in a readable hard copy form or such other form and format as agreed to by the facility and the individual, within 24 hours (excluding weekends and holidays); and
- “The facility must allow the resident to obtain a copy of the records or any portions thereof (including in an electronic form or format when such records are maintained electronically) upon request and 2 working days advance notice to the facility.”

(42 CFR 483.10(g)(2))

SNF RIGHT OF ACCESS

- SNF: “The facility may impose a reasonable, cost-based fee on the provision of copies, provided that the fee includes only the cost of:
 - (A) Labor for copying the records requested by the individual, whether in paper or electronic form;
 - (B) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; and
 - (C) Postage, when the individual has requested the copy be mailed.”

(42 CFR 483.10(g)(2))

ALF RIGHT OF ACCESS

- ALF: “Upon request, a resident or others authorized by law, must be provided immediate access to information in their record, and copies of information within two (2) business days.”

(IDAPA 16.03.22.550.01)

HOME HEALTH AND HOSPICE RIGHT OF ACCESS

- HHA: “The patient has the right to ... have a confidential clinical record. Access to or release of patient information and clinical records is permitted in accordance with [HIPAA,] 45 CFR parts 160 and 164.”

(42 CFR 484.50(c)(6); see also CMS SOM App.B)

- Hospice: “The patient has the right to ... have a confidential clinical record. Access to or release of patient information and clinical records is permitted in accordance with [HIPAA,] 45 CFR parts 160 and 164.”

(42 CFR 418.52(c)(5); see also CMS SOM App. M)

INFO BLOCKING RULE

- Applies to “actors”
 - Healthcare providers.
 - Developers or offerors of certified health IT.
 - Not providers who develop their own IT.
 - Health info network/exchange.

(45 CFR 171.101)

- Prohibits info blocking, i.e., practice that is likely to interfere with access, exchange, or use of electronic health info, and
 - Provider: knows practice is unreasonable and likely to interfere.
 - Developer/HIN/HIE: knows or should know practice is likely to interfere.

(45 CFR 171.103)

INFO BLOCKING RULE: PENALTIES

Developers, HIN, HIE

- Complaints to ONC
 - <https://www.healthit.gov/topic/information-blocking>.
- ONC investigations
- Proposed rule:
 - Civil monetary penalties of up to \$1,000,000 per violation

(85 FR 22979 (4/24/2020);
proposed 42 CFR 1003.1420)

Healthcare Providers

- “Appropriate disincentives to be established by HHS.”
- Waiting for rule.



INFO BLOCKING: EXAMPLES

- Refusing to timely respond to requests.
- Charging excessive fees.
- Imposing unreasonable administrative hurdles.
- Imposing unreasonable contract terms, e.g., EHR agreements, BAAs, etc.
- Implementing health IT in nonstandard ways that increase the burden.
- Others?

INFO BLOCKING EXCEPTIONS



**PREVENTING
HARM
EXCEPTION**



**PRIVACY
EXCEPTION**



**SECURITY
EXCEPTION**

**EXCEPTIONS THAT INVOLVE
not fulfilling requests to access,
exchange, or use EHI**



**INFEASIBILITY
EXCEPTION**



**HEALTH IT
PERFORMANCE
EXCEPTION**

8

**EXCEPTIONS TO THE
INFORMATION
BLOCKING
PROVISION**



**LICENSING
EXCEPTION**



**FEES
EXCEPTION**



**CONTENT AND
MANNER
EXCEPTION**

**EXCEPTIONS THAT INVOLVE
procedures for fulfilling requests
to access, exchange, or use EHI**

TIME FOR RESPONDING TO PATIENT REQUESTS

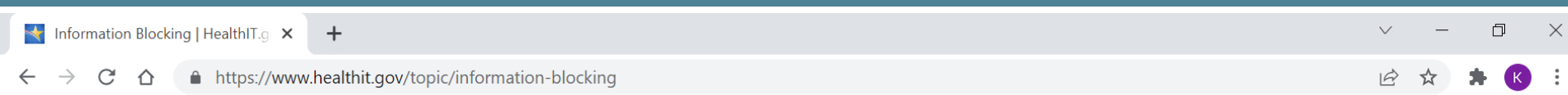
“Q: When would a delay in fulfilling a request for access [to] EHI be considered an interference under the [IBR]?”

“A determination as to whether a delay would be an interference ... would require a fact-based, case-by-case assessment of the circumstances....”

“Unlikely to be an Interference: If the delay is necessary to enable the access, exchange, or use of EHI, it is unlikely to be considered an interference For example, if the release of EHI is delayed ... to ensure that the release complies with state law, it is unlikely to be considered an interference so long as the delay is no longer than necessary. Longer delays might also be possible ... if no longer than necessary, in scenarios where EHI must be manually retrieved and moved from one system to another system ...”

“Likely to be an Interference: It would likely be considered an interference ... if a health care provider established an organizational policy that, for example, imposed delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results.... [I]t also would likely be considered an interference where a delay in providing access ... occurs after a patient logs in to a patient portal to access EHI that a health care provider has (including, for example, lab results) and such EHI is not available—for any period of time—through the portal.”

[HTTPS://WWW.HEALTHIT.GOV/TOPIC/INFORMATION-BLOCKING](https://www.healthit.gov/topic/information-blocking)



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

NEW: Health IT Feedback Portal

CONTACT EMAIL UPDATES

Connect with us: [in](#) [twitter](#) [youtube](#) [rss](#)

TOPICS | BLOG | NEWS | DATA | ABOUT ONC

Search

HealthIT.gov > Topics > Information Blocking

Information Blocking

Report Information Blocking

Information Blocking

What is information blocking?

In general, information blocking is a practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider that, except as required by law or specified by the Secretary of Health and Human Services (HHS) as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information (EHI).



Have questions about information blocking? [View our Information Blocking Frequently Asked Questions \(FAQs\)](#)

What are examples of practices that could constitute information blocking?

Section 4004 of the Cures Act specifies certain practices that could constitute information blocking:

- Practices that restrict authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law

Additional Resources

- [Fact Sheets](#)
- [Webinars](#)
- [FAQs](#)
- [Report Information Blocking](#)

Locum Tenens Billi....pdf

Show all



PATIENT CHARTING



GOOD MEDICAL RECORDS ARE IMPORTANT!

- Proper medical records are essential to—
 - Proper patient care
 - Proof of proper conduct
 - Regulatory compliance
 - Payment and reimbursement
- Even more important given patients' right to access info.



BAD MEDICAL RECORDS

- Criminal fines and penalties
 - Criminal negligence, fraud, false claims, etc.
- Civil lawsuits, fines, and penalties
 - Malpractice, fraud and abuse, lack of consent, privacy violation, etc.
- Administrative penalties
 - Licensing board actions, civil monetary penalties, program exclusion, etc.
- Adverse business consequences
 - Poor care, denied payment, patient relation problems, loss of privileges, loss of employment, etc.

PRACTICAL STANDARDS

- Practical standards defined by purpose for medical records.
 - Document patient's health and treatment.
 - Communicate patient's status and care to other practitioners.
 - Provide basis for evaluating adequacy and appropriateness of care.
 - Support claims for payment or reimbursement.
 - Protect legal interests of patient and provider.
 - Provide data for planning, research, education.
- Make sure chart is sufficient to accomplish these purposes.

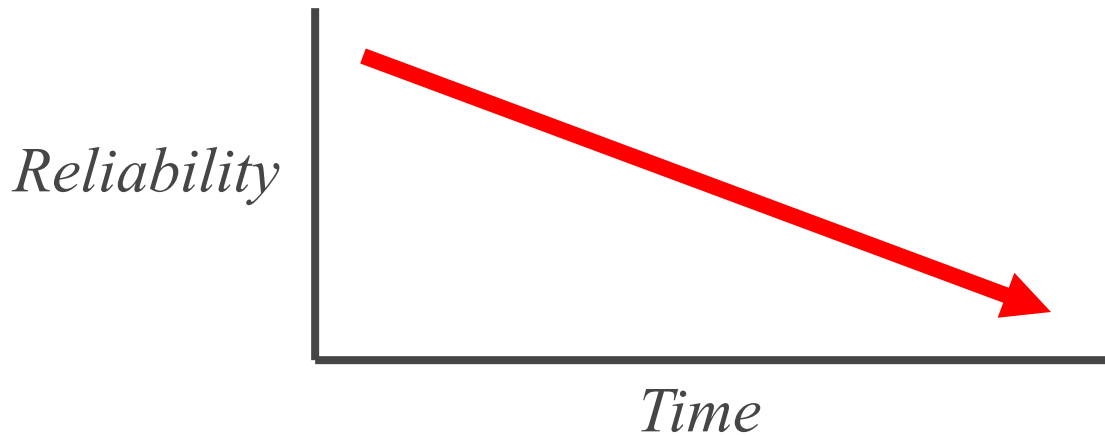
REMEMBER THE PRESUMPTIONS...

- *If it's not in the chart, it didn't happen.*
- *If the chart has been altered, you must be guilty.*
- *If the chart can't be found, it must have contained bad stuff.*



PROMPT CHARTING

- Document as soon as possible.



- Easy to forget details with time.
 - Exact time of entry may be very important.
 - Evidentiary exception for “business record” requires that record is made at or near the time.
- Others may rely on record in meantime.

LATE ENTRIES

- Late entries are okay.
 - May be unavoidable.
 - Better than no, incomplete, or incorrect entry.
 - Subject to scrutiny.
- To make late entry—
 - Add entry at first available line.
 - Reference “*late entry*”
 - Identify the date, time, and name of person making entry.

MISTAKEN ENTRIES AND CORRECTIONS



- Corrections and amendments are okay.
 - Truthfully document patient care and status.
 - Better than incorrect entry.
 - Still subject to scrutiny.
- Corrections should preserve original entry.
 - For mistaken entry, draw single line through entry, designate it as “*mistaken entry*”, and initial with date, time, and reason for change if reason not obvious.
 - Avoid using “*error*”
 - Do not write over original entry.
 - For additions, initial the addition and state the date, time, title, and reason for change if not obvious.

MISTAKEN ENTRIES AND CORRECTIONS

- Be careful about making entries after notice of potential claim or complication.
 - May create inference of “padding” the record.
 - Opposing counsel may already have copy of original claim.
 - Consult with risk manager or attorney.
- Correction may still be appropriate if necessary to provide effective patient care.

CHART FACTS

- Remain objective and document facts.
 - What you see, hear, smell, feel, measure and count.
 - Not what you opine, infer, or assume, or speculate.
- * *“Just the facts, ma’am”*



BE SPECIFIC

- Document observations in specific, quantifiable terms if possible.
- Avoid vague terms, e.g., *light, moderate, heavy, occasional, frequent*.
 - Subject to broad interpretation.
- Compare:
 - *"Output adequate" → "Output 1,200 ml"*
 - *"Pt. appears to be in pain" → "Pt. requested pain medication after complaining of severe lower back pain radiating to right leg."*

DOCUMENT EXACT QUOTES

- Document quotes, especially when they contain significant information, e.g., *Patient states, "I slipped as I was trying to get out of bed."*
 - Exact quotes are more credible.
 - Exact quotes avoid inference of bias.

BE PROFESSIONAL



BE PROFESSIONAL

- Always be professional in comments.
 - Describe patient behavior objectively;
 - Do not label the patient negatively,
 - e.g., *complainer, malingerer, frequent flyer, alcoholic, abusive, bizarre, obnoxious, problem patient, rude, uncooperative, disagreeable, drunk, etc.*
 - Creates impression of anti-patient bias.
 - Suggests that patient received substandard care because the nurse disliked the patient.
 - Avoid flippant remarks, e.g., “PBBB”
- * *Assume that patient or jury may read your notes at some future time.*

DON'T BLAME

- In chart, do not—
 - Blame or accuse others
 - Admit fault
- * *You may not know all the facts.*
- There may be other times or places where such discussions may occur, but the chart is not the place for such comments.

FROM PATIENT CHARTS...

- *Primary nursing could not be given because nurse patient ratio 1:20*
- *Patient in extreme pain because night shift refused to give prescribed medication*
- *If [the doctor] doesn't start returning calls, he's going to kill a patient.*
- *Patient going into shock. Could not get Dr. [X] to come. We never can!!!*
- *If nurses around here would read medication orders, we'd have fewer emergencies.*
- *Patient fell out of bed because nurse left the side rail down.*

REPORTING INCIDENTS

- Document incidents in separate incident report.
 - Subject to peer review privilege.
- Document incidents immediately.
 - Time
 - What happened
 - Name and time physician notified
 - Follow-up care
 - Patient's response
- Remember: do not
 - Opine
 - Speculate
 - Blame
 - Admit

DOCUMENT NON-TREATMENT

- Phone calls
 - Missed medications
 - Missed appointments
 - Missed treatment
 - Failure to follow advice
 - Failure to take medication
 - Non-compliance with treatment
 - Misconduct by patient
- * *Include warnings or notice of risks, e.g.,*
- *“Patient refused fetal monitor; limitation on our ability to identify fetal distress emphasized.”*
- * *Remember: be objective and professional.*

TAMPERING WITH MEDICAL RECORDS

- Tampering includes—
 - Rewriting/altering record without notation.
 - Addition to chart at later time without notation.
 - Placing inaccurate info in the record.
 - Intentionally omitting significant facts.
 - Dating entry to appear as if written at earlier time.
 - Destroying records.
 - Adding to someone else's entry.
- Relatively easy to detect tampering.



TAMPERING WITH MEDICAL RECORDS



- Tampering may be worse than the actions it is designed to hide.
 - Creates inference of improper conduct.
 - May constitute spoliation of evidence.
 - May justify punitive damages.
 - May subject you to criminal penalties.

TAMPERING WITH MEDICAL RECORDS

- People are very forgiving of those who acknowledge and accept responsibility for mistakes.
- People do not easily forgive dishonesty.
- Once lost, credibility is nearly impossible to restore.



ADDITIONAL RESOURCES



<https://www.hollandhart.com/healthcare#overview>

Healthcare | Holland & H x

Secure | <https://www.hollandhart.com/healthcare#overview>

EXCELLENCE IN LEGAL SERVICE

MENU HOLLAND & HART 70 YEARS EST. 1947

OVERVIEW ▶

PRACTICES/INDUSTRIES

NEWS & INSIGHTS

CONTACTS



Kim Stanger
Partner
Boise



Blaine Benard
Partner
Salt Lake City



HEALTH LAW BLOG

Access to previous webinar recordings, publications, and more.

The Healthcare Industry is now ready to stand ready to help

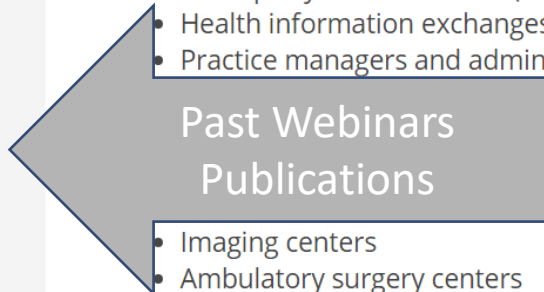
Issues such as rising health care costs, innovations in health care, and the minds of many of our clients are opportunities that arise.

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
- Health care facilities

Past Webinars
Publications

- Imaging centers
- Ambulatory surgery centers



QUESTIONS?

Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com