HIPAA PRIVACY, SECURITY AND BREACH NOTIFICATION RULES

Kristy M. Kimball

HOLLAND&HART LLP

DISCLAIMER

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.

HOLLAND&HART LLP

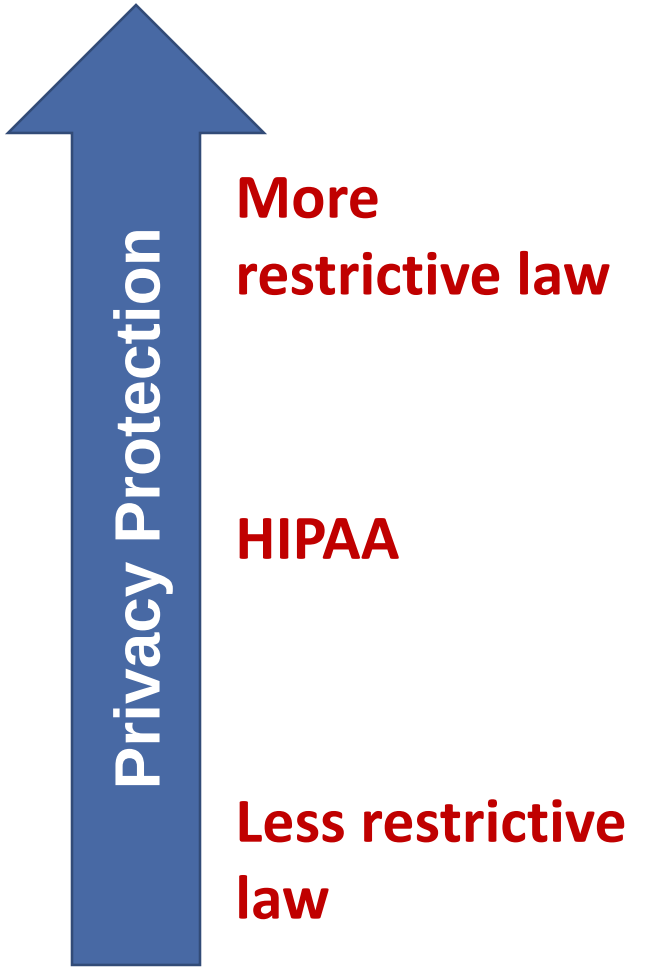
WRITTEN MATERIALS

- 42 CFR part 164
- OCR, *Patient's Right to Access Information*
- Checklists on www.hhhealthlawblog.com
  - HIPAA compliance
  - Required privacy policies and forms
  - Notice of privacy practices
  - Authorization
  - Business associate agreements
- Articles on www.hhhealthlawblog.com
  - Releases of Information v. Authorization
  - Responding to Subpoenas, Orders and Warrants
  - Responding to Law Enforcement
  - Records of Deceased Persons
  - Disclosures to Family Members
  - Disclosures to the Media
  - Communicating by E-mail or Text
  - Using and Employee's PHI
  - Others

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA")

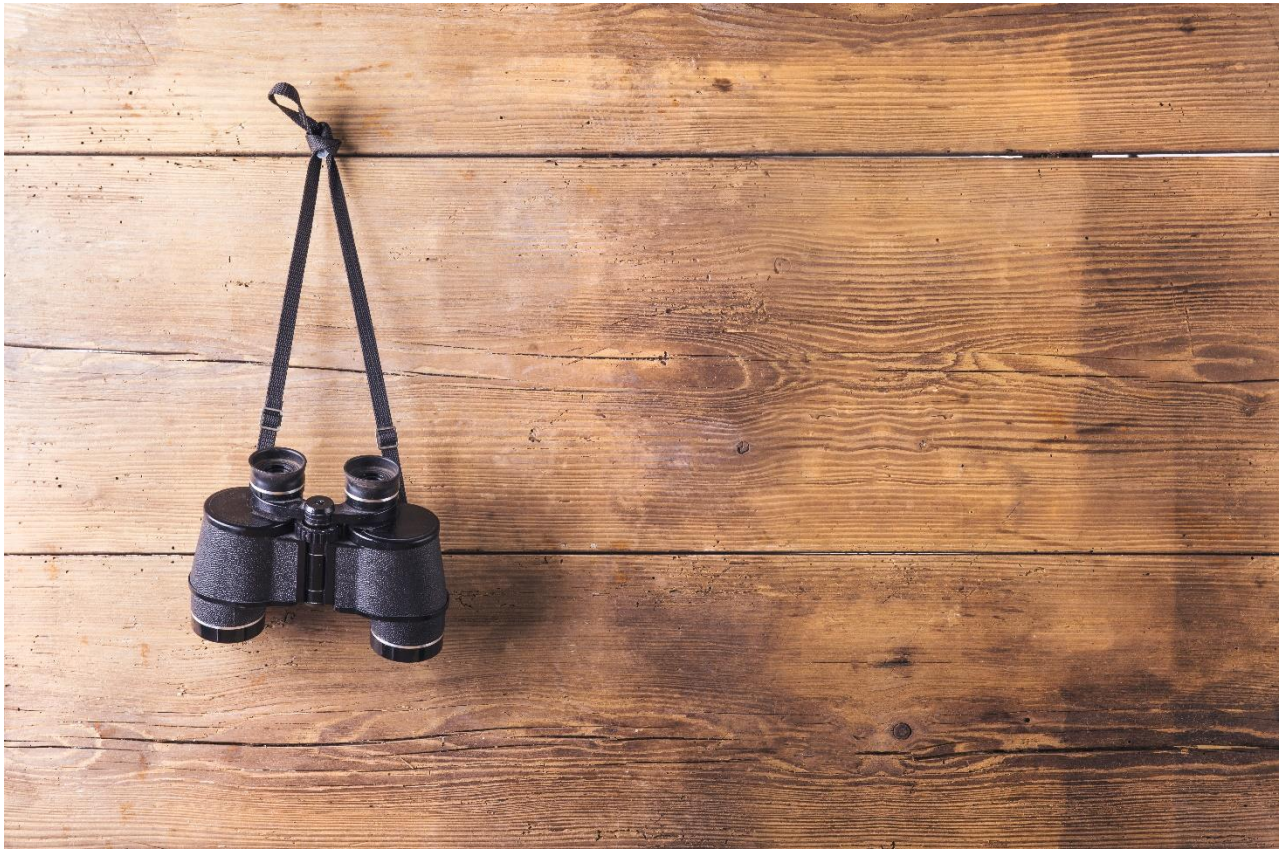
- 45 CFR 164
  - .500: Privacy Rule
  - .300: Security Rule
  - .400: Breach Notification Rule
- HITECH Act
  - Modified HIPAA
  - Implemented by HIPAA Omnibus Rule

REMEMBER OTHER LAWS



- HIPAA preempts less restrictive laws.
- Comply with more restrictive law, e.g.,
  - Federally assisted drug and alcohol treatment program (42 CFR part 2)
  - Others?

HIPAA ENFORCEMENT



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	• $50,000 fine • 1 year in prison
Committed under false pretenses	• 100,000 fine • 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	• $250,000 fine • 10 years in prison

(42 USC 1320d-6(a))

HIPAA CIVIL PENALTIES
(AS MODIFIED BY RECENT INFLATION ADJUSTMENT)

Conduct	Penalty
Did not know and should not have known of violation	• $114 to $57,051 per violation • Up to $1,71,533 per type per year • **No penalty if correct w/in 30 days** • OCR may waive or reduce penalty
Violation due to reasonable cause	• $1,141 to $57,051 per violation • Up to $1,711,533 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	• $11,182 to $57,051 per violation • Up to $1,71,533 per type per year • **Penalty is mandatory**
Willful neglect, but do not correct w/in 30 days	• At least $57,051 per violation • Up to $1,711,533 per type per year • **Penalty is mandatory**

(45 CFR 160.404; see also 83 FR 51378)

HOLLAND&HART LLP

HIPAA: AVOIDING 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.

HOLLAND&HART LLP

ENFORCEMENT

- 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.
- No private cause of action under HIPAA.

COVERED ENTITIES AND INFO

HOLLAND&HART LLP

ENTITIES SUBJECT TO HIPAA

- Covered entities
  - Health care providers who engage in certain electronic transactions.
    - Consider hybrid entities.
  - Health plans, including employee group health plans if:
    - 50 or more participants; or
    - Administered by third party (e.g., TPA or insurer).
  - Health care clearinghouses.
- Business associates of covered entities
  - Entities with whom you share PHI to perform services on your behalf.

PROTECTED HEALTH INFORMATION

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.
- Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.

NOT COVERED BY HIPAA

- Info after person has been dead for 50 years.
- Info maintained in capacity other than as provider.
  - e.g., as employer
  - Beware using patient info for employment purposes.
- "De-identified" info, i.e., remove certain identifiable info
  - Names
  - Dates (birth, admission, discharge, death)
  - Telephone, fax, and e-mail
  - Social Security Number
  - Medical Record Number
  - Account numbers
  - Biometric identifiers
  - Full face photos and comparable images
  - Other unique identifying number, characteristic, or code

PHI protected by HIPAA

PROHIBITED ACTIONS

- Unauthorized disclosure outside covered entity.
- Unauthorized use within covered entity.
- Unauthorized access from within or outside covered entity.

USE AND DISCLOSURE RULES
(45 CFR 164.502-.514)

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

Don't disclose unless exception applies or have authorization

Implement reasonable safeguards

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)

HOLLAND&HART LLP

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 discuss 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.*

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.

PATIENT AUTHORIZES DISCLOSURE

- Written requests
- Authorizations

PATIENT REQUEST TO PROVIDE INFORMATION

- Must provide PHI in designated record set to third party if:
  - Written request by patient;
  - Clearly identifies the designated recipient and where to send the PHI; and
  - Signed by patient.

(45 CFR 164.524(c)(3)(ii))

- Part of individual's right of access.
  - Must respond within 30 days.
  - May only charge reasonable cost-based fee.

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

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.

(45 CFR 164.508)

EMPLOYMENT PHYSICALS, DRUG TESTS, OR IMES

- HIPAA generally applies to employment physicals, drug tests, school or physicals, independent medical exams ("IME"), 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 OSHA, MSHA, etc.
  - Workers compensation

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))

SALE OF PHI

- Cannot sell PHI unless obtain patient's prior written authorization and the authorization discloses whether covered entity will receive remuneration in exchange for PHI.
- "Sale of PHI" = disclosure of PHI by covered entity or business associate if they receive (directly or indirectly) any remuneration (financial or otherwise) from or on behalf of the recipient of the PHI in exchange for the PHI.

(45 CFR 164.508(a)(4))

- May apply to charging excessive fees to copy or produce records

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

PARENTS AND PERSONAL REPRESENTATIVES

HOLLAND&HART LLP

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))

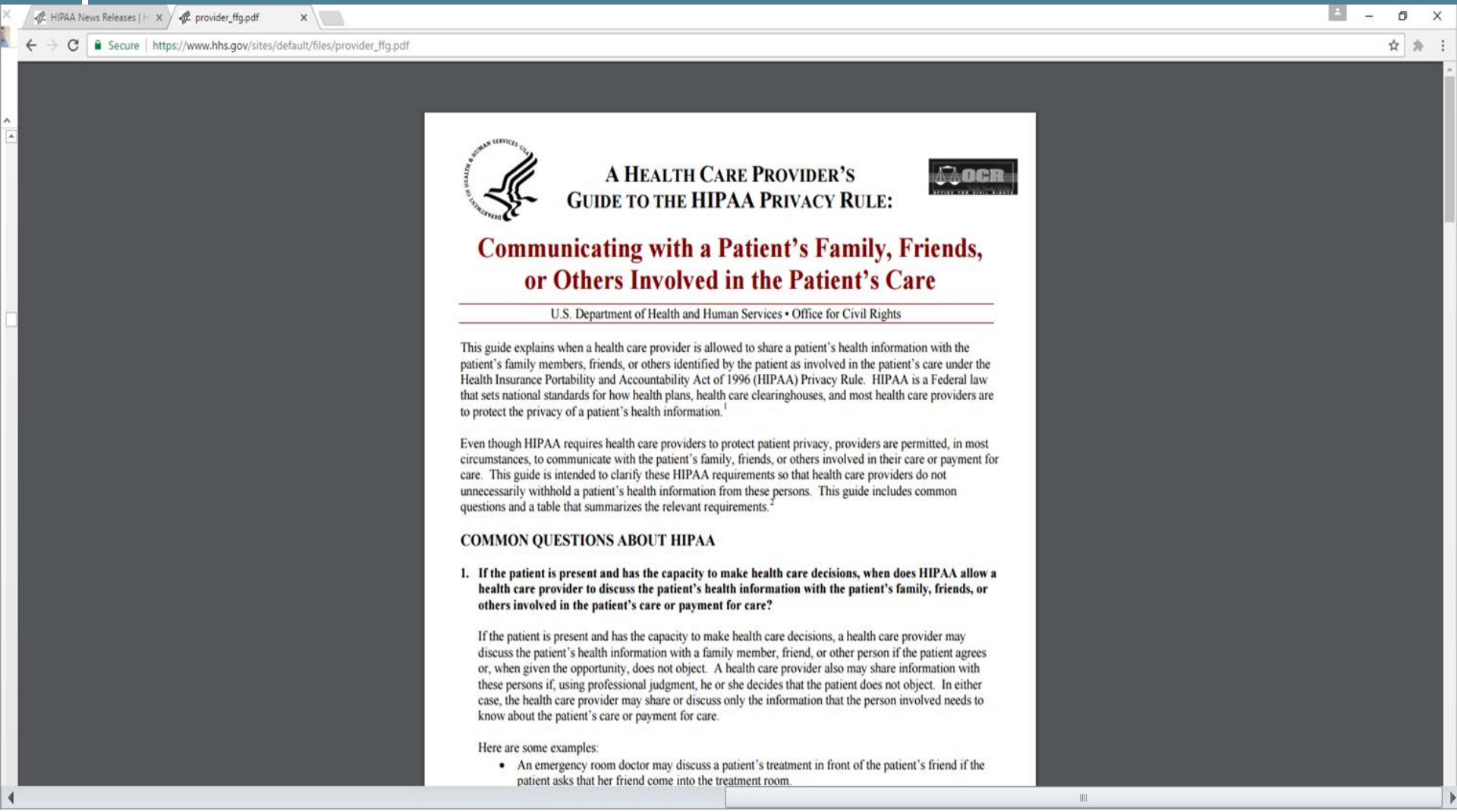
* Legal custody of minor (even if parent doesn't have physical custody); generally, unless parent has had their parental rights terminated, they still have legal custody and can act as personal representative. (Note that can always elect not to treat parent as personal rep, if feel it is not in minor's best interest.)

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 representative as the patient is not in the best interest of patient, e.g., abuse.

(45 CFR 164.502(g))

HTTPS://WWW.HHS.GOV/SITES/DEFAULT/FILES/PROVIDER_FFG.PDF



HOLLAND&HART LLP

BUSINESS ASSOCIATES

HOLLAND&HART LLP

BUSINESS ASSOCIATES

- May disclose PHI to business associates if have valid business associate agreement ("BAA").
- Failure to execute BAA = HIPAA violation
  - May subject you to HIPAA fines.
    - Recent settlement: gave records to storage company without BAA: $31,000 penalty.
  - Based on recent settlements, may expose you to liability for business associate's misconduct.
    - Turned over x-rays to vendor ; no BAA: $750,000.
    - Theft of business associate's laptop; no BAA: $1,550,000.

BUSINESS ASSOCIATES

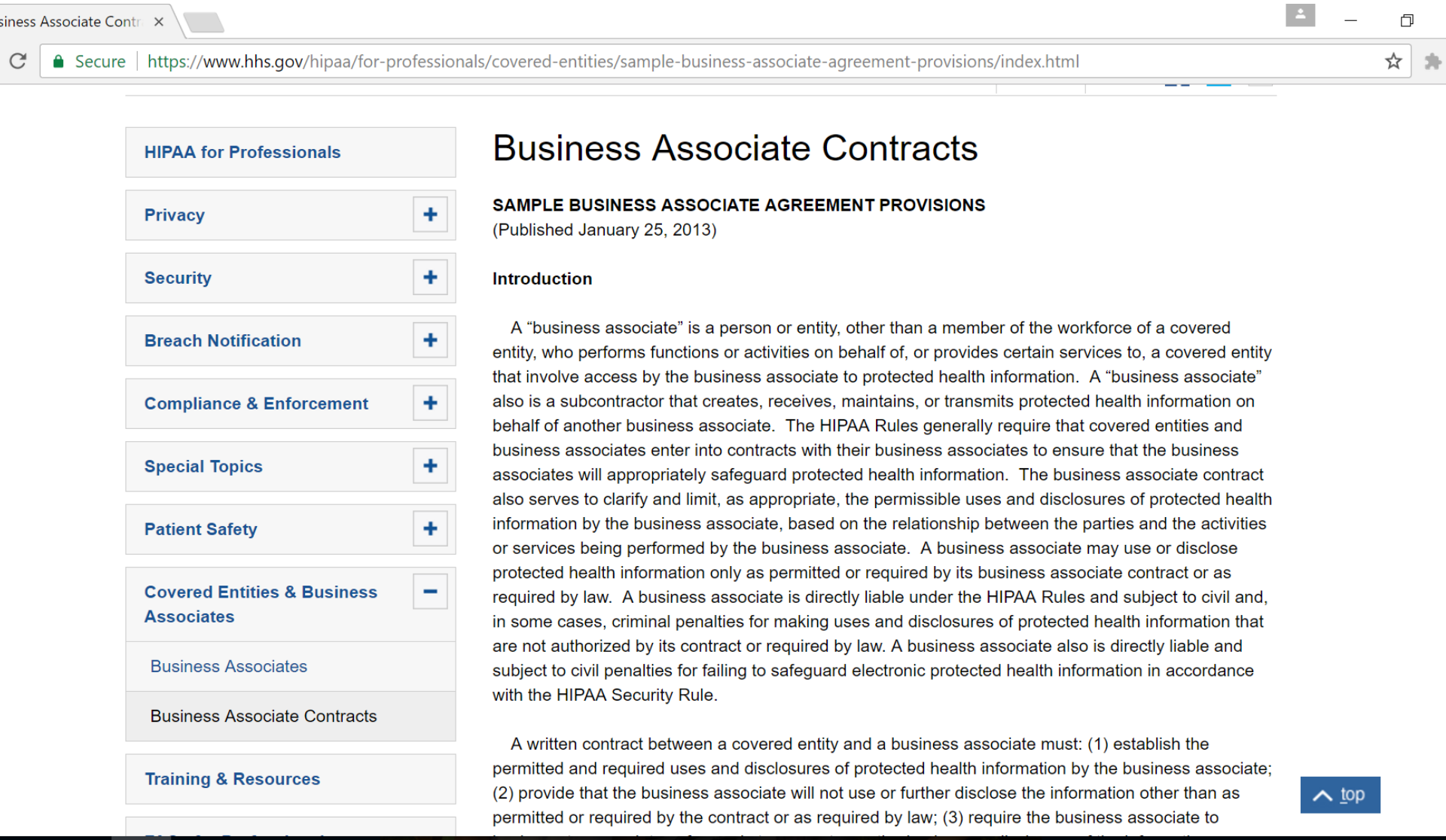
- Business associates =
  - Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity.
  - Covered entities acting as business associates.
  - Subcontractors of business associates.

(45 CFR 160.103)

- BAAs
  - Cannot be combined with other documents.
  - Must contain required terms and statements.

(45 CFR 164.314, 164.504(e))

HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/COVERED-ENTITIES/SAMPLE-BUSINESS-ASSOCIATE-AGREEMENT-PROVISIONS/INDEX.HTML



LIABILITY FOR ACTS OF BUSINESS ASSOCIATE OR SUBS

- Covered entity or business associate:
  - Knows that business associate or subcontractor is violating HIPAA, and
  - Fails to take action to end the violation or terminate the BAA.

(45 CFR 164.504(e)(1))

- Business associate or subcontractor is acting as agent of the covered entity within the scope of the agency.
  - Test: right of control
  - *Maintain independent contractor status!*

(45 CFR 160.402(c))

MAKING THE DISCLOSURE

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. Only release what is specified.

(45 CFR 164.514(f))

- Portals should include appropriate access controls.

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

MINIMUM NECESSARY STANDARD

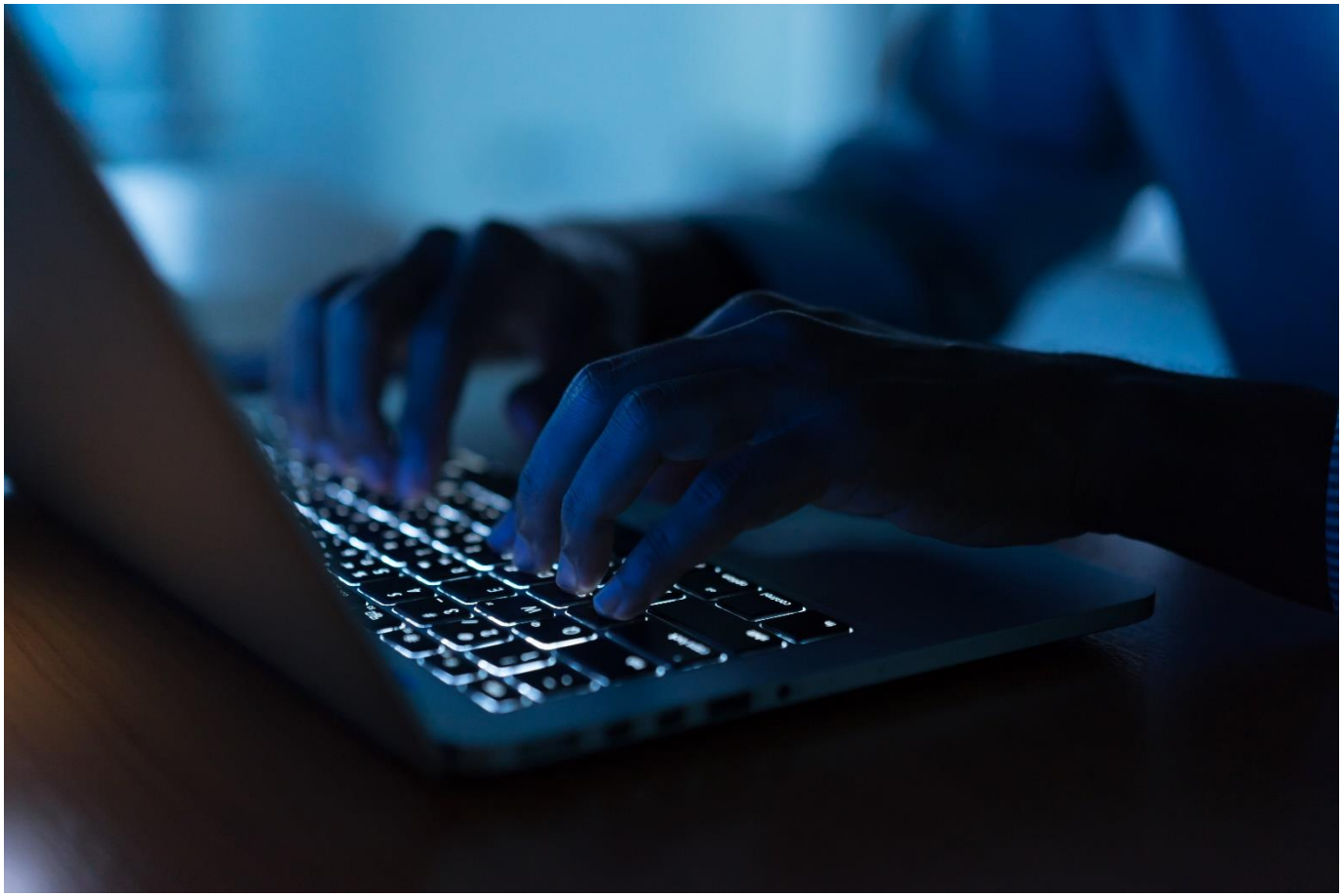
- Cannot use or disclose more PHI than is reasonably necessary for intended purpose.
- Minimum necessary standard does not apply to disclosures to:
  - Patient.
  - Provider for treatment.
  - Per individual's authorization.
  - As required by law.
- May rely on judgment of:
  - Another covered entity.
  - 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.

HIPAA SECURITY RULE (45 CFR 164.300 ET SEQ.)



HOLLAND&HART LLP

OCR Settlements in 2017

12/17	Cancer center failed to implement safeguards to protect ePHI despite prior warnings that its information had been hacked.	$2,300,000
5/17	Hospital issued press release containing patient's name after patient used fraudulent identification card.	$2,400,000
5/17	Health center faxed HIV information to wrong entity.	$387,000
4/17	Monitoring company's laptop containing 1,390 patients' info stolen from car; insufficient risk analysis and no finalized security policies.	$2,500,000
4/17	No business associate agreement ("BAA") with record storage company.	$31,000
4/17	FQHC's info hacked; no risk analysis and insufficient security rule safeguards.	$400,000
2/17	Hospital allowed unauthorized employees to access and disclose records of 80,000 patients; failed to terminate users' right of access.	$5,500,000
2/17	Hospital lost unencrypted PDAs containing info of 6,200 persons; failure to take timely action to address known risks.	$3,200,000
1/17	Insurance company's unencrypted USB containing info of 2,209 persons stolen; no risk analysis, implementation, or encryption.	$2,200,000
1/17	Failure to timely report breach.	$475,000

FOR IMMEDIATE RELEASE
February 1, 2018

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules

Fresenius Medical Care North America (FMCNA) has agreed to pay $3.5 million to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and to adopt a comprehensive corrective action plan, in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. FMCNA is a provider of products and services for people with chronic kidney failure with over 60,000 employees that serves over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.

On January 21, 2013, FMCNA filed five separate breach reports for separate incidents occurring between February 23, 2012 and July 18, 2012 implicating the electronic protected health information (ePHI) of five separate FMCNA owned covered entities (FMCNA covered entities).

HIPAA SECURITY RULE

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

(45 CFR 164.301 et seq)

Protect ePHI:

- Confidentiality
- Integrity
- Availability

RISK ASSESSMENT

Security Risk Assessm ×

https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

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

HealthIT.gov

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

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.

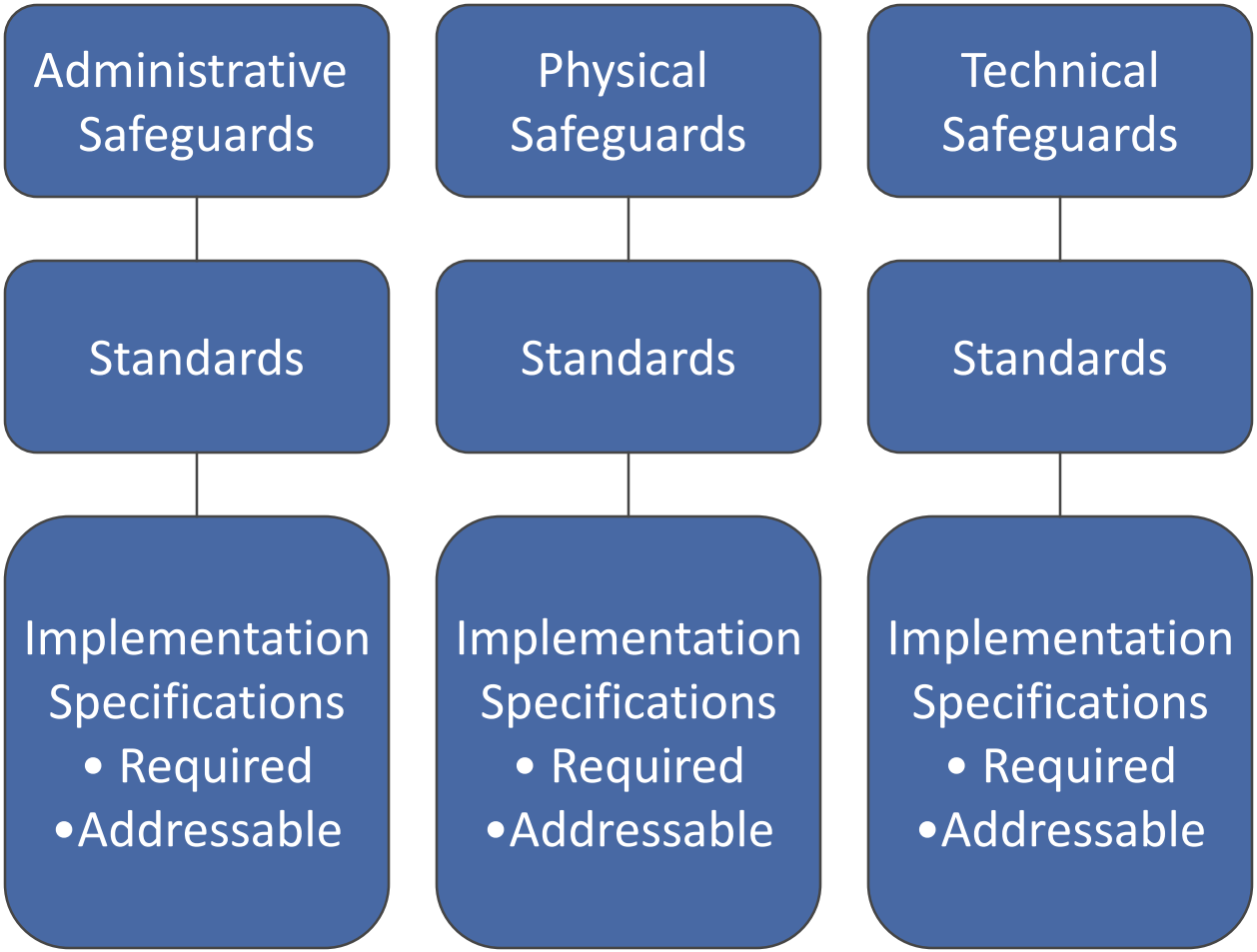
Top 10 Myths of Security Risk Analysis

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

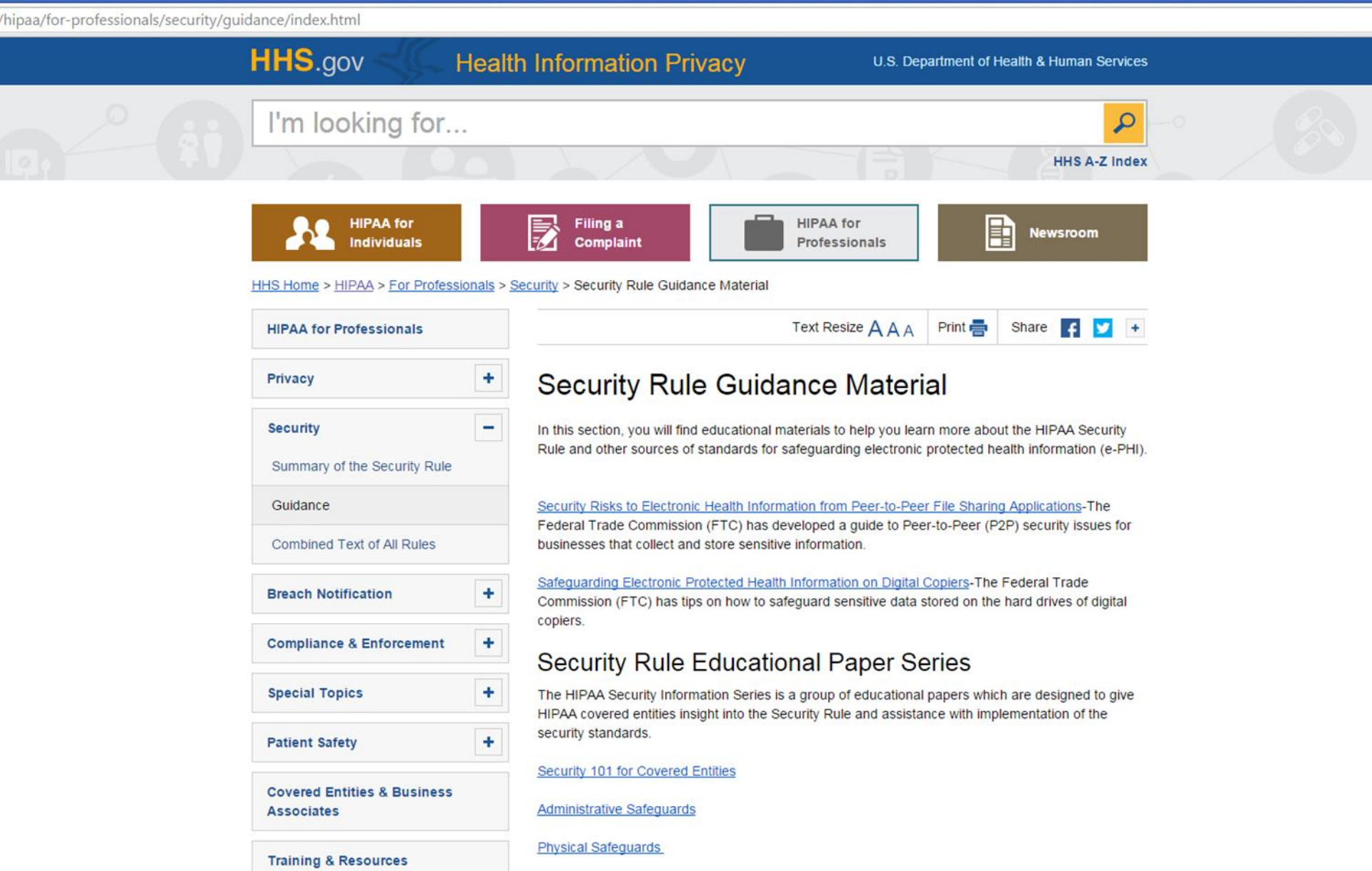
Read the top 10 list distinguishing fact from fiction.

SRA Tool (Windows version)

SAFEGUARDS


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

WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SECURITY/GUIDANCE/INDEX.H



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.

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 e health

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

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

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

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

HealthIT.gov

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?

Watch and Learn

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

COMMUNICATING BY E-MAIL OR TEXT

- General rule: must be secure, i.e., encrypted.

EMAIL: May communicate via unsecure e-mail if warned patient and they choose to receive unsecure.

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

TEXTING:

- Between provider and patient: If warn patient and they choose to receive, but limit to minimum necessary.
- Between healthcare team members: Can text if within a secure platform—SMS texting IS NOT a secure platform.

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

  - But, CANNOT use secure texting for Orders: Medicare Conditions of Participation and Conditions for Coverage generally prohibit texting orders, even if on a secure platform.

(CMS letter dated 12/28/17)

PATIENT RIGHTS

HOLLAND&HART LLP

PATIENT RIGHTS

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

(45 CFR 164.520 et. seq.)

WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/PRIVACY/GUIDANCE/ACCESS/INDEX.HTML

ADMINISTRATIVE REQUIREMENTS

ADMINISTRATIVE REQUIREMENTS

- Designate HIPAA privacy and security officers
- Implement policies and safeguards
- Train workforce
- Respond to complaints
- Mitigate violations
- Maintain documents for 6 years

(45 CFR 164.530)

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 rules 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.

"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)

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))

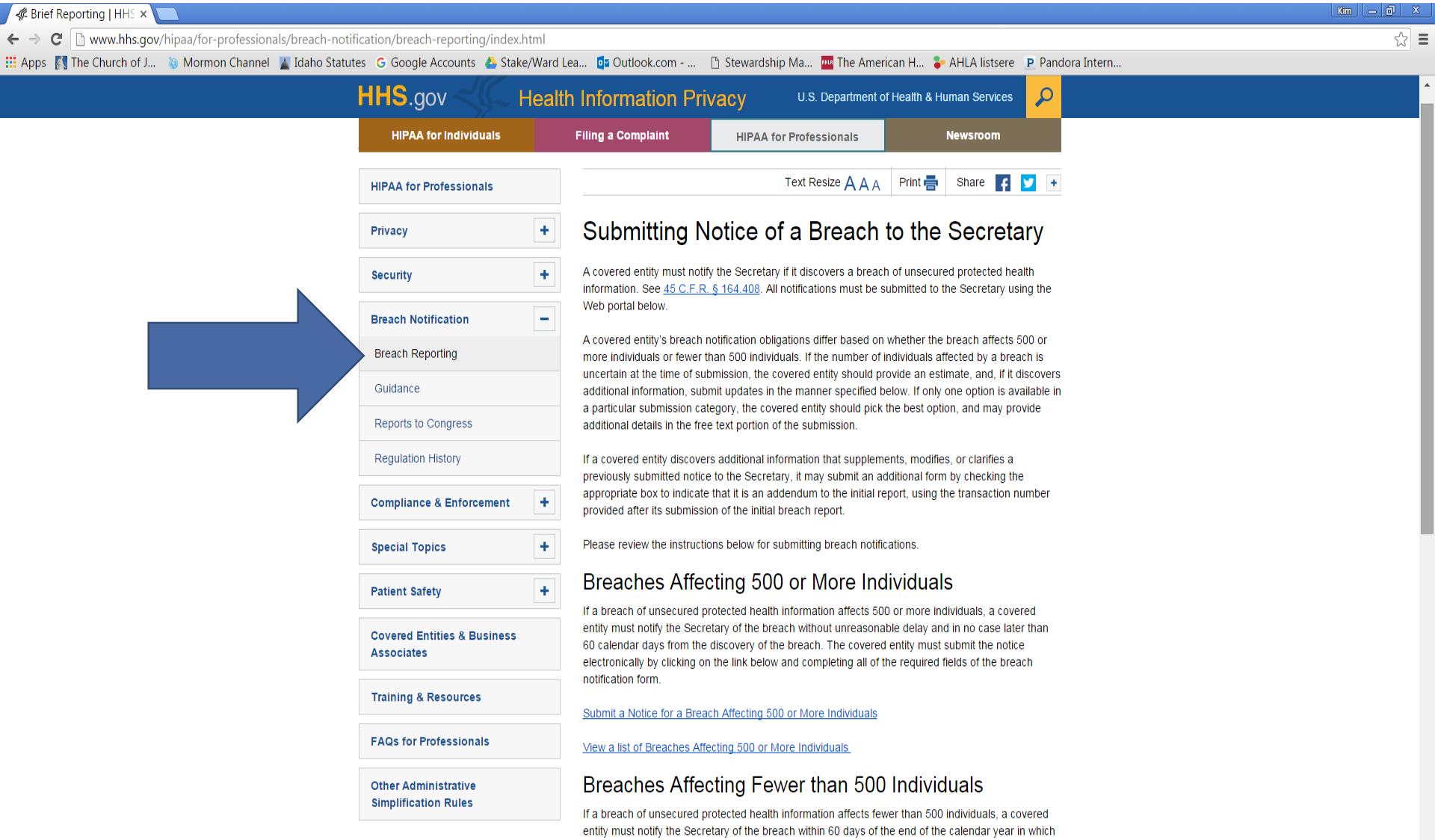
NOTICE TO HHS

- 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)

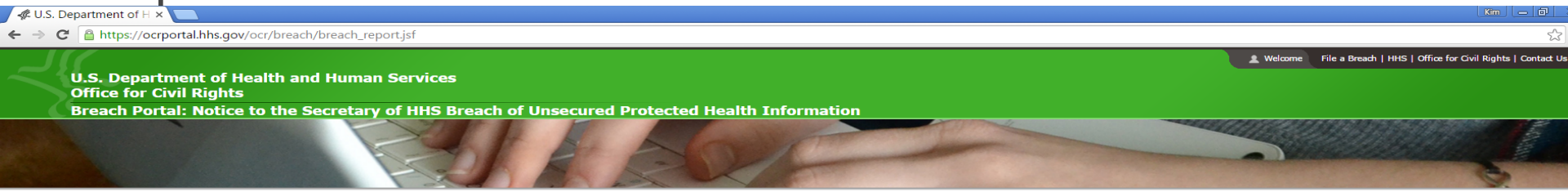
- Submit report at http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/BREACH-NOTIFICATION/BREACH-REPORTING/INDEX.HTML



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

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)

NOTICE BY BUSINESS ASSOCIATE

- Business associate must notify covered entity of breach of unsecured PHI:
  - Without unreasonable delay but no more than 60 days from discovery.
  - Notice shall include to extent possible:
    - Identification of individuals affected, and
    - Other info to enable covered entity to provide required notice to individual.

(45 CFR 164.410)

- Business associate agreements may impose different deadlines.

WYOMING BREACH REPORTING STATUTE (WSA 40-12-501)

HOLLAND&HART LLP

WYOMING BREACH REPORTING STATUTE

- Generally requires commercial entities to immediately investigate and notify subject persons if:
  - Unauthorized acquisition of computerized data that materially compromises security, confidentiality, or integrity of data;
  - "personal identifying info", i.e.,
    - Name + certain other identifiers (e.g., SSN; driver's license; account #, credit card #, debit card # + code; tribal ID; username or e-mail + password; birth/marriage certificate; health info; individual tax ID);
  - Misuse could cause injury to Wyoming resident; and
  - Misuse is likely to occur.
- AG may bring suit to enforce statute or recover damages.
- Compliance with HIPAA satisfies Wyoming statute.

(WSA 40-12-502)

HOLLAND&HART LLP

ADDITIONAL RESOURCES

HOLLAND&HART LLP

HTTP://WWW.HHS.GOV/HIPAA/

HTTPS://WWW.HOLLANDHART.COM/HEALTHCARE#OVERVIEW

HOLLAND&HART LLP

QUESTIONS?

KRISTY M. KIMBALL

OFFICE: (801) 799-5792

kmkimball@hollandhart.com

HOLLAND&HART LLP