

Common Misconceptions in Privacy and Security

JEFFREY DUNIFON & MEGHAN O'CONNOR
HIPAA COW FALL CONFERENCE, NOVEMBER 3, 2022



1

What Laws Apply?

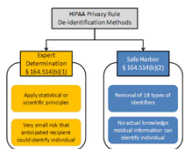
COMMON MISCONCEPTIONS IN PRIVACY AND SECURITY




2

Q: What is PHI? What are the 18 identifiers for de-identification?

- See Dr. Malin's presentation for more on the expert determination opinion
- Safe Harbor 18 elements relate to individual, relatives, employers or household members of individual



<https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard>



3

De-Identification Safe Harbor 18 elements

- Names
- Geographic subdivisions smaller than a state
- All elements of date (except year) directly related to individual
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URLs
- IP addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- **Any other unique identifying number, characteristic, or code**

** Must have no actual knowledge that information could be used alone or in combination with other information to identify subject individual



4

Q: Are bank account numbers held by a TPA covered under HIPAA and GLB?

- HIPAA vs. GLB
 - HIPAA applies to CEs and BAs
 - GLB applies to companies that offer consumers financial products or services
- If the data element is processed by the TPA, HIPAA
- If the data element is processed by a bank, GLB



5

Q: When does HIPAA apply vs. FERPA?

	Who Must Comply?	What Information?	What Information is Excluded?
FERPA	Public and private institutions (elementary, secondary, and post-secondary) receiving Dept of Education funding and agencies	Student education records containing information (1) directly related to a student and (2) maintained by an educational institution / agency or a party acting for it	Treatment records, i.e., records on a student 18+ made or maintained by physician/paraprofessional acting in profession capacity which are made, maintained, or used only in connection with provision of treatment to student
HIPAA	CEs and BAs	PHI	De-identified data Education records under FERPA
HIPAA	No one – not a real law	No data	All data



6

When do HIPAA and FERPA intersect?

- Health care services provided at an elementary or secondary school, e.g., Medicaid waiver services
 - Is there a covered entity? Who creates and maintains the records? How are services billed?
- Student health records
 - Is the provider a school employee (treatment records) or third-party CE?
- Postsecondary institutions
 - Campus health clinic (treatment records) vs. university hospital (PHI)
- Also consider state law, as it does not follow the HIPAA CE concept



7

Access Questions

COMMON MISCONCEPTIONS IN PRIVACY AND SECURITY



8

Q: Please discuss access requirements under HIPAA and information blocking

- HIPAA
 - OCR right access initiative
- Information blocking
- Must balance privacy obligations with individual rights
 - Erring on the side of protection is not always the correct route
 - HIPAA: Unreasonable measures
 - Information blocking: Action or action that does (or is likely to) interfere with access, exchange or use of electronic health information



9

Q: How do you confirm a subpoena for PHI is valid in WI?

- Who is issuing party (judge, attorney, other)?
- What information is requested (PHI, sensitive information, business information)?
- What is the location of court (WI or other state)? Needs to be properly served in WI.
- Is subpoena signed by judge or court commissioner?
- If subpoena is signed by attorney, pro se litigant, or court clerk, does a valid authorization or qualified protective order accompany subpoena?
- Is the subpoena requesting record release or appearance? Does the authorization contemplate the required action?



10

Q: How do CEs implement communications to family members/others involved in care?

- CE may disclose to family member, other relative, or close personal friend of the individual, or any other person identified by the individual, PHI directly relevant to such person's involvement with individual's health care or payment related to individual's care
- OCR is deliberately open and vague
- Plenty of room for CE judgment
 - Documentation
 - Securing evidence that disclosure was appropriate



11

Q: How should a CE respond to verbal ROI requests?

- CE may require individual to request access in writing, provided CE informs individual of requirement
- Questions to consider
 - What does your NPP say?
 - What does your access policy say?
 - Are you able to understand and process the request as submitted?
 - Do you have identity verification concerns?
 - Is data requested subject to additional restrictions for disclosure (e.g., sensitive information?)
 - What is in the best interest of the patient and organization?



12

Q: Facility directories – can you opt in for certain immediate family members?

- Facility directory is permissive
- Data elements:
 - Name
 - Location in facility
 - General condition
 - Religious affiliation (clergy only)
- Use / disclosure to:
 - Members of clergy
 - People who ask for individual by name
- Individual may object to some or all uses / disclosures permitted under HIPAA



13

Operational Questions

COMMON MISCONCEPTIONS IN PRIVACY AND SECURITY



14

Q: Does provider have to disclose that PHI may be shared with offshore entities?

- Not a HIPAA requirement
- See upstream contractual requirements
- See applicable regulatory requirements
 - Medicare Advantage offshoring attestation to CMS
 - Developing state laws
- Being a good steward of data / ick factor
 - But be careful about precedent



15

Q: What do you do when an essential vendor refuses to agree to an offshoring limitation?

- Is offshoring a requirement or a practical risk concern / preference?
 - Contractual requirement
 - Regulatory requirement (e.g., Medicaid, Medicare Advantage)
 - Whitelist / blacklist countries
 - Country with localization requirements
- Will any other options mitigate concerns?
 - View-only access
 - Other compensating technical controls



16

Q: Please discuss business operation disclosures in the context of non-compete enforcement (e.g., cease and desist process)

- Fact specific
- Disclosure may be authorized under litigation discovery process under HIPAA
- Minimum necessary
- Request a protective order
- Be sensitive to public perception vis-a-vis non-compete enforcement



17

Q: Working from a mobile phone – how do you reconcile app access requirements / terms and security?

- Importance of mobile device / BYOD policy
- Vet each app you allow people to use for company business.
 - Use case specific. Why do you want to use app and for what purpose?
 - Loop in privacy / security teams to review privacy policy and terms of use at the outset.
 - Many consumer-facing apps will not meet your security criteria. Consider apps built for industry.
- Regulator’s response: assess risks in conjunction with the use case. No good carte blanche method.



18

Incident Response


COMMON MISCONCEPTIONS IN PRIVACY AND SECURITY



19

Q: Are incidental disclosures reportable?


- Secondary use/disclosure incident to a use/disclosure otherwise permitted or required by HIPAA
- CE must have in place administrative, physical, and technical safeguards that limit incidental uses/disclosures
 - Safeguards not expected to *guarantee* privacy of PHI from any and all potential risks
- Should not be reportable breach, but fact-specific



20

Q: When can you rely on an attestation that PHI was destroyed? Does it mitigate the compromise?

- Risk assessment low probability of compromise factors:
 - Nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification
 - Unauthorized person who used PHI or to whom the disclosure was made
 - Whether PHI was actually acquired or viewed
 - Extent to which the risk to the protected health information has been mitigated
- Who is third party providing attestation? How reliable?
- Is the attestation the only factor demonstrating low probability of compromise?
- Mitigation ≠ reporting exception



21

Q: When a snooper is identified, should they ever be given a second chance?

- Not addressed in HIPAA
- What does your policy say?
 - Shift away from “one strike you’re out” policies
 - Reporting to licensing boards
- Risks in inconsistent enforcement
 - Wrongful termination
 - Regulatory interest



22

Thank you. Questions?



23
