MOSSADAMS

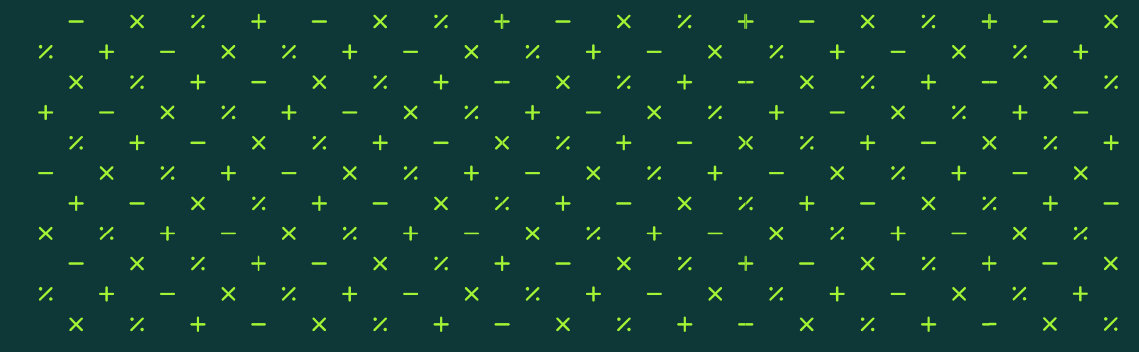
HIPAA Privacy Investigations and Standards

Melaney Scott, MBA, CIA, CHC,
Senior Manager

Agenda

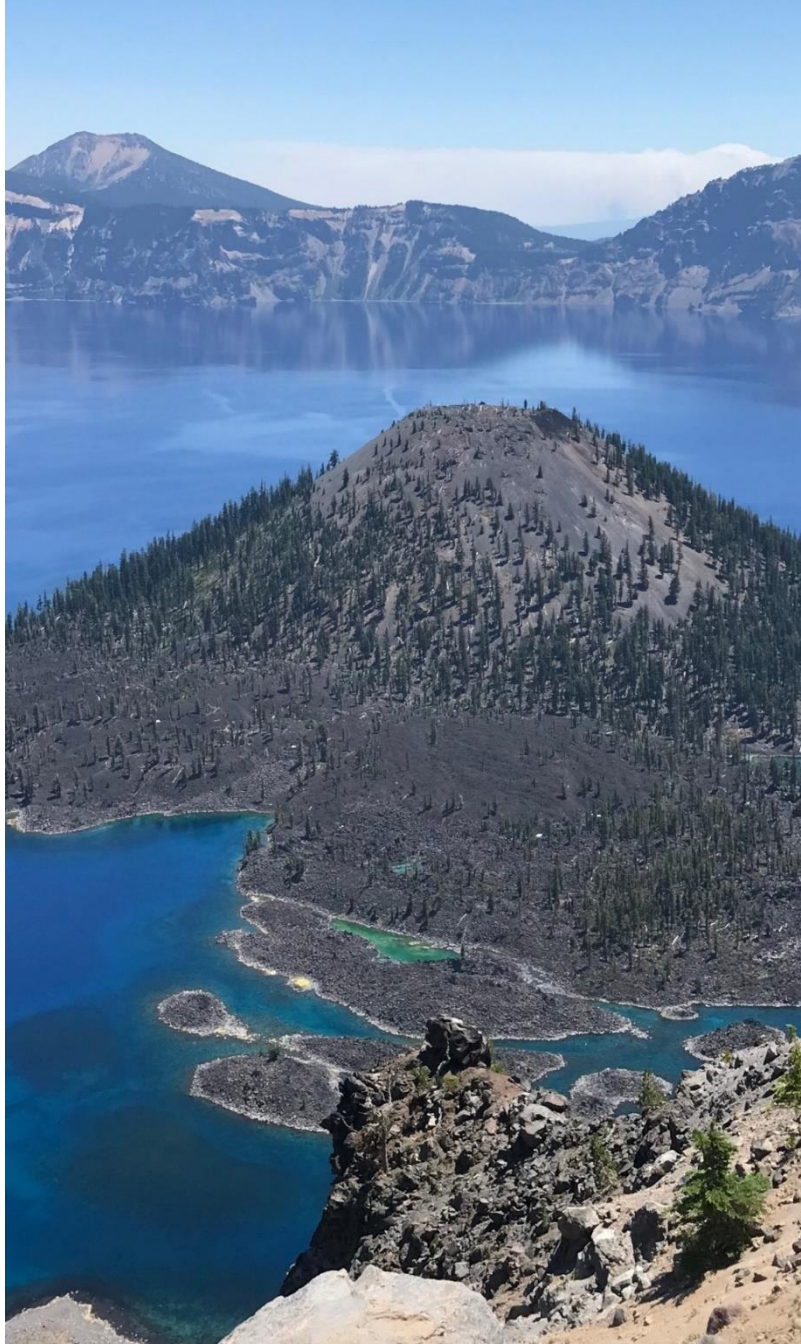
- HIPAA Privacy Overview
- Foundation for Conducting Privacy Investigations
- Considerations for Conducting and Documenting Investigations

HIPAA Privacy Overview



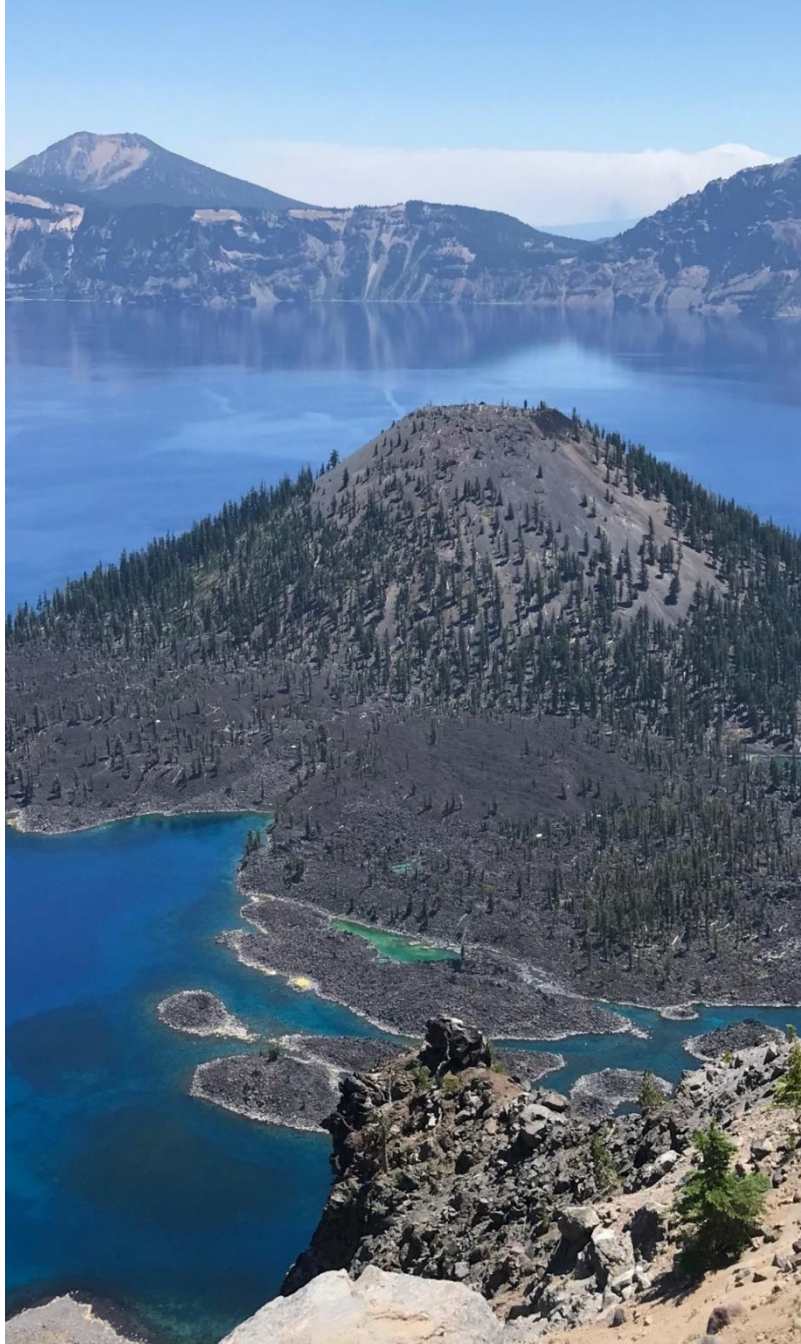
Overview

- HIPAA became law in 1996
- Over time created a system to recognize and enforce patient rights to protect medical record privacy
- Failure to comply can result in a violation, breach, and possible fines

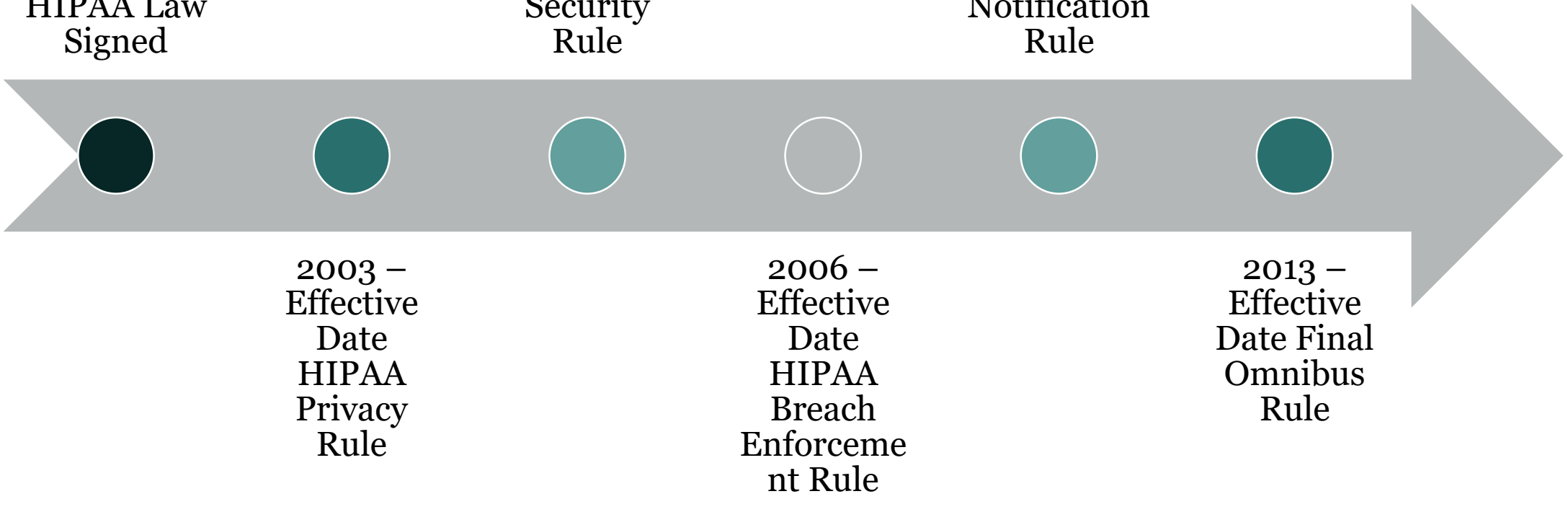


Overview

- Enforced by the Office of Civil Rights (OCR)
- Ongoing initiative around Right of Access
- OCR settlements highlight that not just large entities are at risk



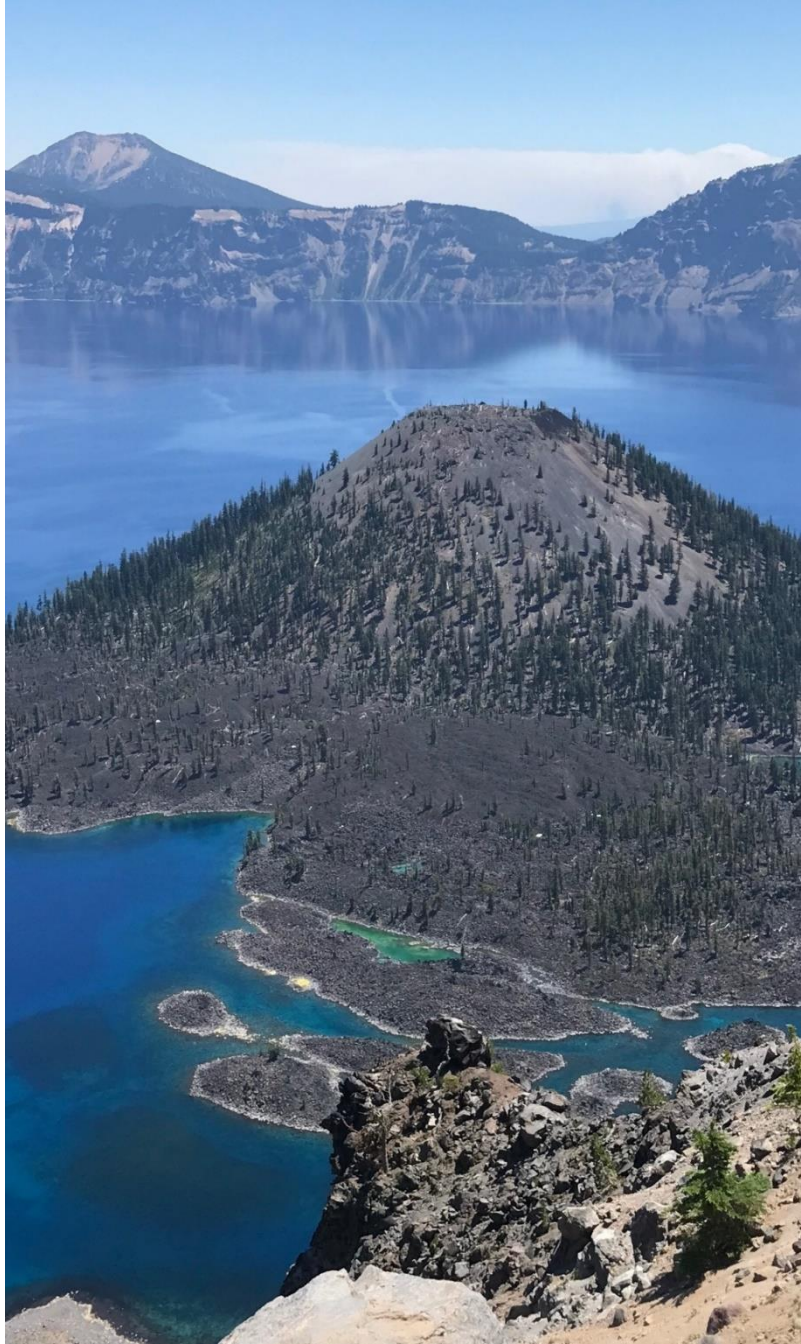
HIPAA Timeline



10 Most Common HIPAA Violations

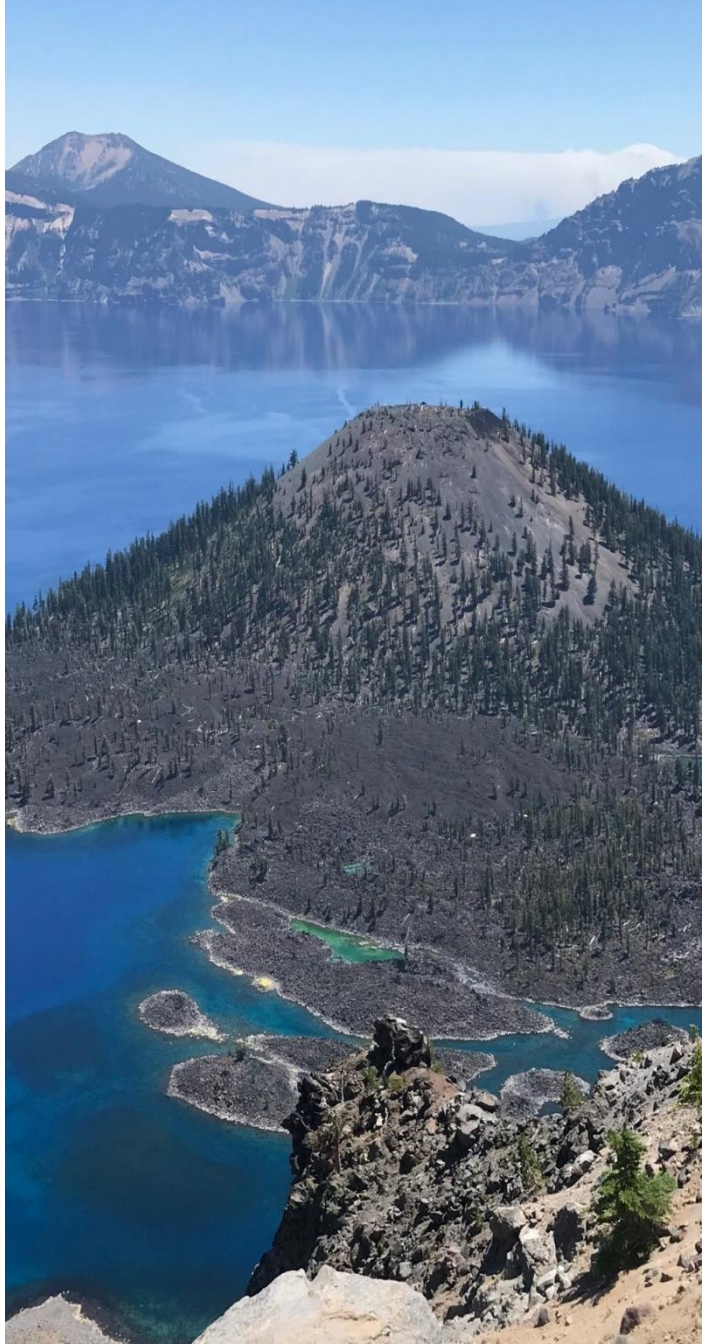
Healthcare record snooping	Insufficient ePHI access controls
Not performing organization-wide risk analysis	Improper disposal of PHI
Failure to manage security risks / lack of a risk management process	Failure to use encryption or an equivalent measure to safeguard ePHI on portable devices
Denying patients' access to health records/exceeding timescale for providing access	Exceeding the 60-day deadline for issuing breach notifications
Failure to enter into a HIPAA-compliant business associate agreement	Impermissible disclosures of protected health information

- https://www.hipaajournal.com/common-hipaa-violations/



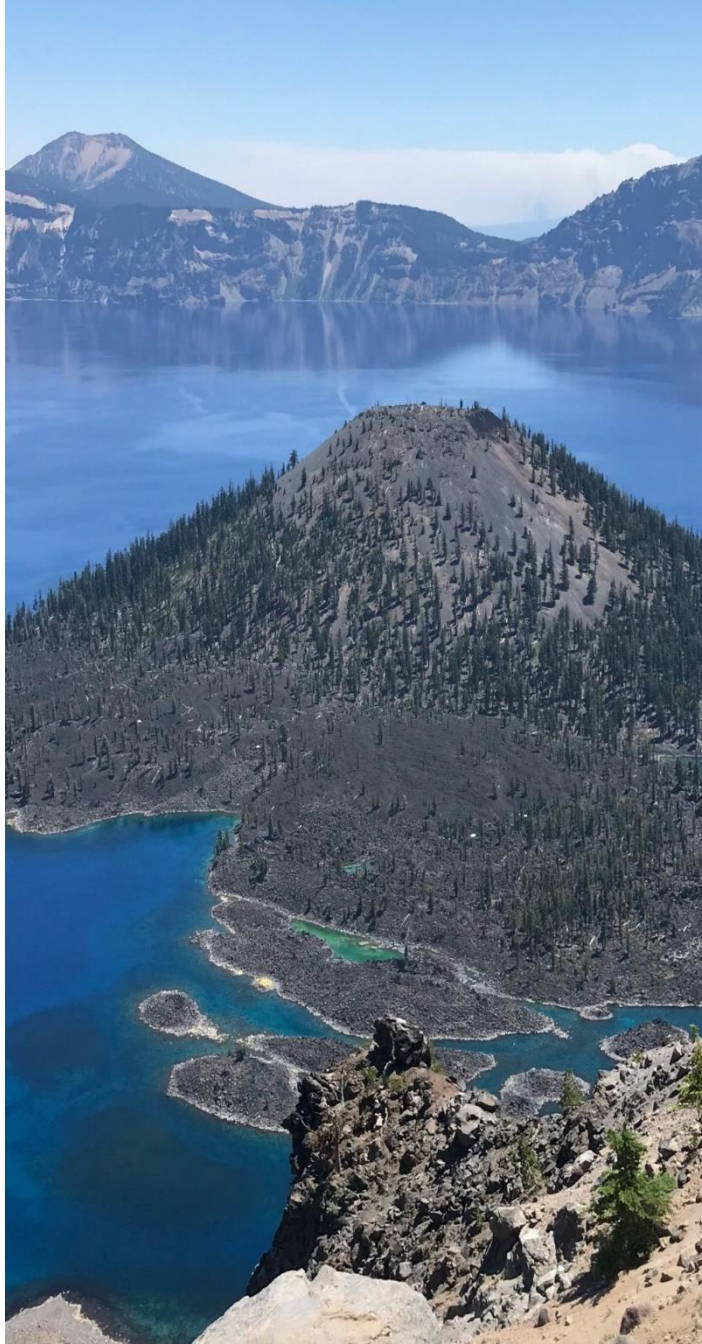
Most Common Types of HIPAA Violations by Workforce Members

- Snooping on healthcare records
- Emailing PHI to personal email accounts / Removing PHI from facility
- Leaving portable electronic devices / paper unattended
- Releasing PHI to unauthorized individual or without authorization

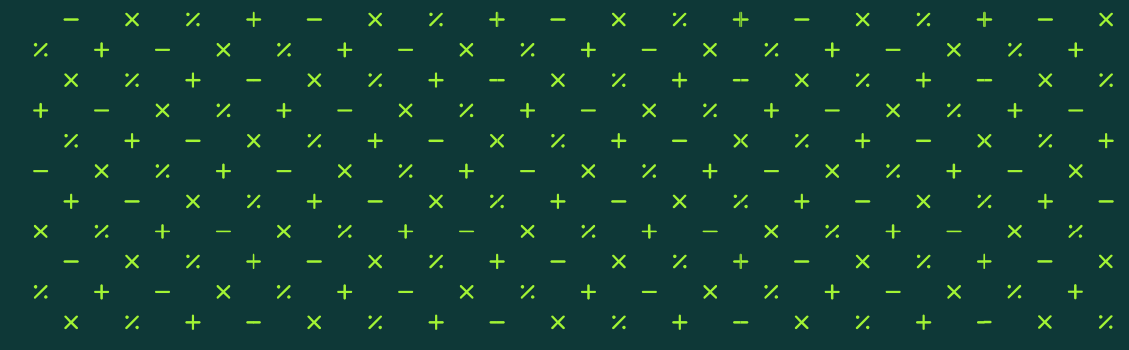


Most Common Types of HIPAA Violations by Workforce Members

- Disclosure after authorization expires
- Downloading PHI to unauthorized devices
- Providing unauthorized access to medical records



Foundation for Conducting Privacy Investigations



HIPAA Privacy Program Foundation

Creating a Culture of HIPAA Privacy Compliance

HIPAA Privacy Program Foundation - Investigations

Can use components of the seven elements of an effective compliance program principles, which include

- Designated individual or department for complaints
- Standards of conduct, policies, and procedures
- Effective training and education
- Enforcement standards

- https://oig.hhs.gov/documents/provider-compliance-training/945/Compliance101tips508.pdf

Policies and Procedures

45 CFR §164.530(i)

- Implement P&Ps designed to comply with the standards, implementation specifications, or other requirements of the Breach Notification Rule
- Reasonably designed based on individual entity to ensure compliance
- Process to change P&Ps as necessary / appropriate to comply with law changes

Training

45 CFR §164.530(b)

Train all workforce members of P&Ps as necessary and appropriate for workforce members to carry out functions

Designation for Receiving Complaints

45 CFR §164.530(a)

- Privacy official responsible for developing and implementing P&Ps
- Contact person or office to receive complaints
- Documenting these items and retaining for six years

Complaint Process

45 CFR §164.530(d)

- Process for individuals to make complaints
- Document all complaints received and disposition, if any

Sanctions

45 CFR §164.530(e)

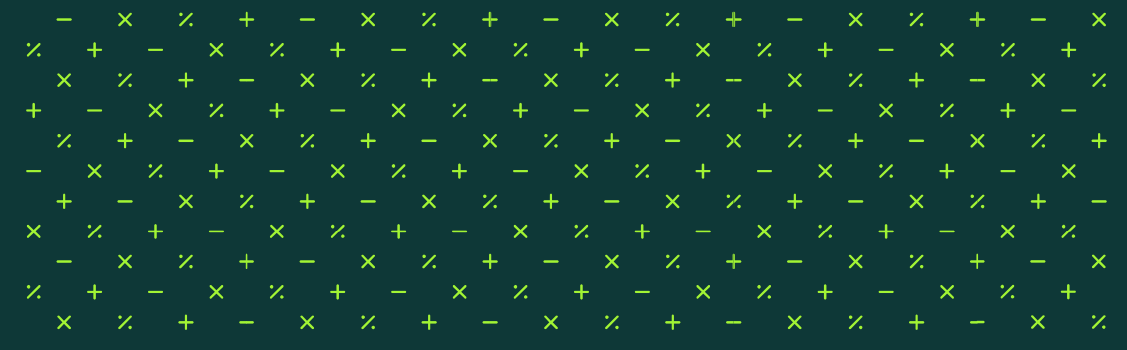
- Have and apply appropriate sanctions
- Document any applied sanctions

Refraining from Intimidating or Retaliatory Acts

45 CFR §164.530(g)

CE may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising a right or participating in any process provided for in the HIPAA or Breach Notification Rules

Considerations for Conducting and Documenting Privacy Investigations



Complaint Process

- Ensure statement in Notice of Privacy Practices referencing Secretary and to the CE and non-retaliation statement
- Methods available for an individual to complain?
- How ensure all complaints received are documented?

Logging a Complaint

Minimum elements to include

Incident number	If referred to another department, which department and why
Date of incident	Investigation substantiated or unsubstantiated
Date complaint received	Has workforce member been involved in prior complaints
Specifics of complaint (who, what, where, when, how, etc.)	Final disposition
Who assigned to for investigation	If determined breach – document risk assessment, if performed
Investigation notes	Date of notification

Completing an Investigation

- Develop and maintain a system for retaining all related documentation surrounding an investigation
- Document all stages of complaint and investigation
- Actions will depend on nature of complaint

Investigation Best Practice Considerations

- Take prompt action
- Objective is to identify if an impermissible use or disclosure of an individual's PHI occurred (Breach)
- Identify date incident occurred and document date complaint received

Investigation Best Practice Considerations

- Review internal policies and procedures related to complaint
- Identify all who potentially involved
- Interview individuals who involved
- Consider nature and extent of PHI involved
- Document, document, document

What to Include in Documentation

- Policies and procedures reviewed (keep copy)
- Individuals identified as involved
- Interviews conducted
- Identification of nature and extent of PHI involved
- Determination of whether Breach occurred

What to Include in Documentation

- What caused the Breach
- What steps were taken to stop further inappropriate use / disclosure PHI
- Who Breach needs reported to
- Risk assessment and outcome, if conducted
- Involve HR if disciplinary measures needed in accordance with progressive discipline policy

Risk Assessment if breach identified

45 CFR §164.402

Factors to include in a risk assessment:

- Nature and extent of PHI involved
- The unauthorized person who used PHI or PHI was disclosed to
- If PHI was acquired or viewed
- Extent risk to PHI has been mitigated

Best Practices and Wrapping Up

- Have foundational components in place to provide guidance on making complaints, investigating complaints, and disciplinary actior in accordance with documented P&Ps
- Train staff on duty to report violations of P&Ps and what constitutes impermissible use and disclosure of PHI
- Maintain documentation for all actions taken while conducting the investigation and the disposition of each complaint

Questions? Now or later…

Melaney Scott
Melaney.Scott@mossadams.com
253-284-5228

Melaney Scott, MBA, CIA, CHC, Senior Manager, Moss Adams Health Care Consulting

Melaney has over 20 years of combined experience in all facets of GAAP accounting, finance, and auditing. She has experience auditing based on COSO, GASB, GAAS, GAGAS, and IIA standards. Specific experience includes: managing the planning, preparation, and execution of risk based compliance audit programs, covering contracting, operational, and financial related audits; leading day-to-day activities of audit teams on complex and multiple audits to ensure audit objectives and deadlines are met, which includes planning, preparation, and execution of risk based financial, federal compliance (Uniform Guidance - Single Audits), and operational audits as well as special projects. Prior auditing experience includes the Medicaid program, which included eligibility, claims, and drug rebates.

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.