HIPAA PASS
Privacy and Security Solutions

How to Respond to a HIPAA Breach

Tuesday, Oct. 25, 2016

HealthInsight

This Webinar is Brought to You By….

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive, Helena MT 59602 | www.gotohts.org | 406.457.5897
transforming health care through innovative technology

HealthInsight

HIPAA
PASS
PRIVACY AND SECURITY SOLUTIONS

About HealthInsight and Mountain-Pacific Quality Health

- HealthInsight and Mountain-Pacific Quality Health are private, non-profit, community-based Quality Improvement Organizations (QIO) that have dedicated more than three decades to improving health and health care and are composed of locally governed organizations in: Alaska, Hawaii, Montana, Nevada, New Mexico, Oregon, Utah and Wyoming. As part of our efforts to assist hospitals and practices with HIPAA compliance, HealthInsight and Mountain-Pacific Quality Health teamed together to form **HIPAA Privacy and Security Solutions**, or ***HIPAA PASS***, to offer affordable, easy and comprehensive Risk Analysis and Risk Management services.

Susan Clarke, HCISPP

- (ISC)^2 certified Health Care Information Security and Privacy Practitioner.
- 15+ years of Health Care Experience.
- 10+ years design and development EHR software, BS with computer science major.
- Served on joint commission steering committee at Mayo Clinic affiliated Health Care System.
- National Incident Management Systems Certificate.
- Served on IT Security and Disaster Recovery councils with experience as communications unit lead during Health Care system's ready and complete alerts.
- Received national recognition as a peer reviewer for ONC and has served as a peer reviewer for CMS and HRSA for health information technology proposals.

Mark Norby, CHP

- 15 Years of IT experience
- Eight Years as the CIO of the Community Health Center of Central Wyoming and University of Wyoming Family Medicine Residency Program
- Six Years as a HIPAA Compliance Officer
- Four Years as a HIPAA Compliance Consultant
- Provided help to more than 150 hospitals and clinics

Disclaimers

- The presenters are not attorneys and do not give legal advice
- There are many different interpretations of HIPAA regulations
- Materials referenced are meant to serve as examples and may not be suitable for every organization

Agenda

- Definitions
- Breach Exclusions
- Policy Statement
- Reporting and Responding to an Incident
- Responding to an Incident or Complaint
- The Four Factor Risk Assessment
- Evaluating and Incident or Complaint
- Action Plan

Breach

Breach means the unauthorized acquisition, access, use, or disclosure of personal health information (PHI) in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information.

Discovered

Discovered means the first day on which the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity.

Security Incident

Security incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

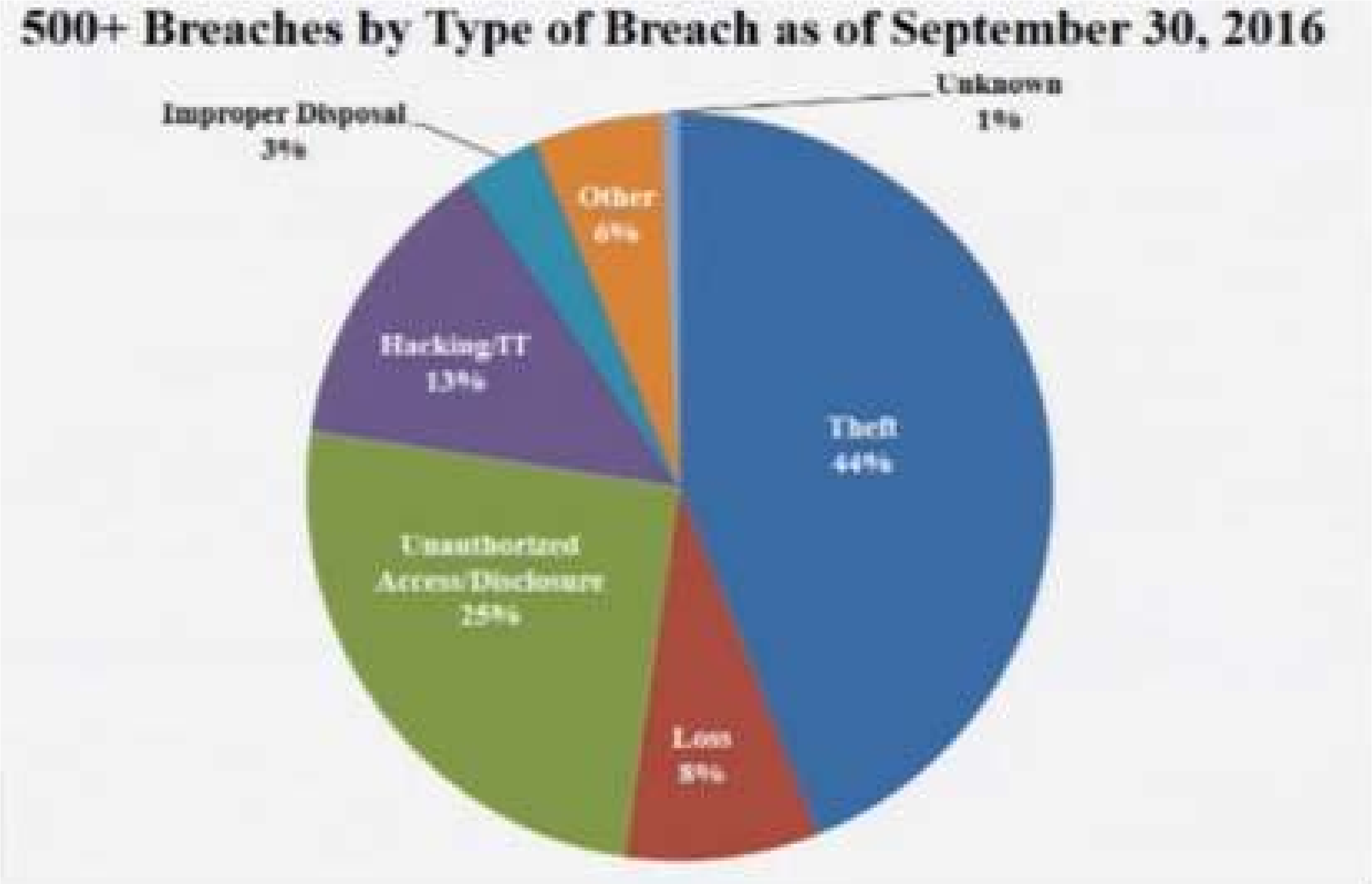
Protected Health Information (PHI)

Protected health information (PHI) generally means identifiable or potentially identifiable health information that is transmitted or maintained in electronic media or any other form or medium. (For the complete definition, please consult 45 CFR § 160.103).

Unsecured PHI

Unsecured PHI means PHI that is not secured through the use of a technology or methodology specified by the Secretary that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals. *E.G. has not be encrypted or properly destroyed.*

Where the Damage Comes From



Breach Exclusions

Any **unintentional** acquisition, access or use of protected health information **by a workforce member or person acting under the authority of a covered entity or a business associate**, if such acquisition, access, or use was **made in good faith and within the scope of authority** and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

Breach Exclusions Cont.

Any inadvertent disclosure **by a person who is authorized to access PHI at a covered entity or business associate to another person authorized** to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information **received as a result of such disclosure is not further used or disclosed** in a manner not permitted under the Privacy Rule.

Breach Exclusions Cont.

A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person **to whom the disclosure was made would not reasonably have been able to retain such information.**

Is It a Breach?

Other than the exclusions listed above, an acquisition, access, use, or disclosure of PHI in a manner **not permitted** under the Privacy Rule is **presumed to be a breach** unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a **risk assessment covering at least four factors…. to be covered shortly.**

Ransomware is a Breach

Ransomware is a type of malware (malicious software) that encrypts data with a key known only to the hacker and makes the data inaccessible to authorized users. After the data is encrypted, the hacker demands that authorized users pay a ransom in order to obtain a key to decrypt the data. Ransomware frequently infects devices and systems through **spam, phishing messages, websites, and email attachments and enters the computer when a user clicks on the malicious link or opens the attachment.**

Security Incident Policy Statement

The practice shall outline its process for evaluating and reporting known or suspected privacy violations or security incidents. This process shall include a **contact list** indicating to whom reports of such incidents should be made, who should be involved in determining if a breach of unsecured PHI has occurred and if affected individual(s) should be notified.

See Breach Notification Sample Policy

Potential Members of Contact List

- Corporate Legal Officer
- **Practice Attorney**
- Insurance Agent
- Privacy Officer
- Security Officer
- CIO or Systems Manager
- Public Affairs/Corporate Communications
- **Local FBI Field Office (Cyber attacks should always be reported to the FBI)**
- **Local Law Enforcement**
- IT Vendor/Provider
- Key Vendor Contacts (software, infrastructure, data center)

Optional:

- Local Computer Forensics Contractor (funded, contracted)

Report Incidents and Complaints

Practice workforce members shall immediately report known or suspected privacy violations or security incidents to the Practice’s Compliance Officer.

Have the reporting employee or witness fill out a Security Incident Report (see samples)

Responding to the Incident or Complaint

Upon receipt of a Security Incident Report, an investigation into the incident shall be initiated.

The Security Incident Investigation Report should be completed as thoroughly as possible by the Incident Handler and Investigators.

Responding to the Incident or Complaint

As soon as possible, but not later than 45 calendar days following discovery of an incident, the Compliance Officer **shall complete a risk assessment** to determine the probability that PHI has been compromised and attach it to the report. The risk assessment shall **include, at minimum, the following four factors**:

Factor 1: Nature and Extent of PHI

The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification

A. Was PHI involved

B. Type of PHI

C. Does the incident meet the definition of breach

D. Likelihood of re-identification

Factor 2: To Whom the Disclosure was Made

A. Did the recipient have an obligation to protect the privacy and security of PHI?

B. Was the acquisition, access or use of PHI by a workforce member or person acting under the authority of the Practice?

C. Was such acquisition, access or use made in good faith?

D. Does the recipient have the ability to re-identify the PHI?

E. Was the acquisition, access or use within the recipient's scope of authority?

F. Did the acquisition, access, use or disclosure result in further use or disclosure in a manner **not** permitted by the Privacy Rule?

Factor 3: Was the PHI Accessed

A determination must be made of whether the PHI was actually acquired or viewed, or rather, the opportunity to acquire or view existed, but was not acted upon.

A. Was the PHI encrypted using at least 128 bit encryption or destroyed by an acceptable method of destruction?

B. Following a forensic examination, did evidence establish that the information was not accessed?

Factor 4: Risk Mitigation

The extent to which the risk to the PHI has been mitigated.

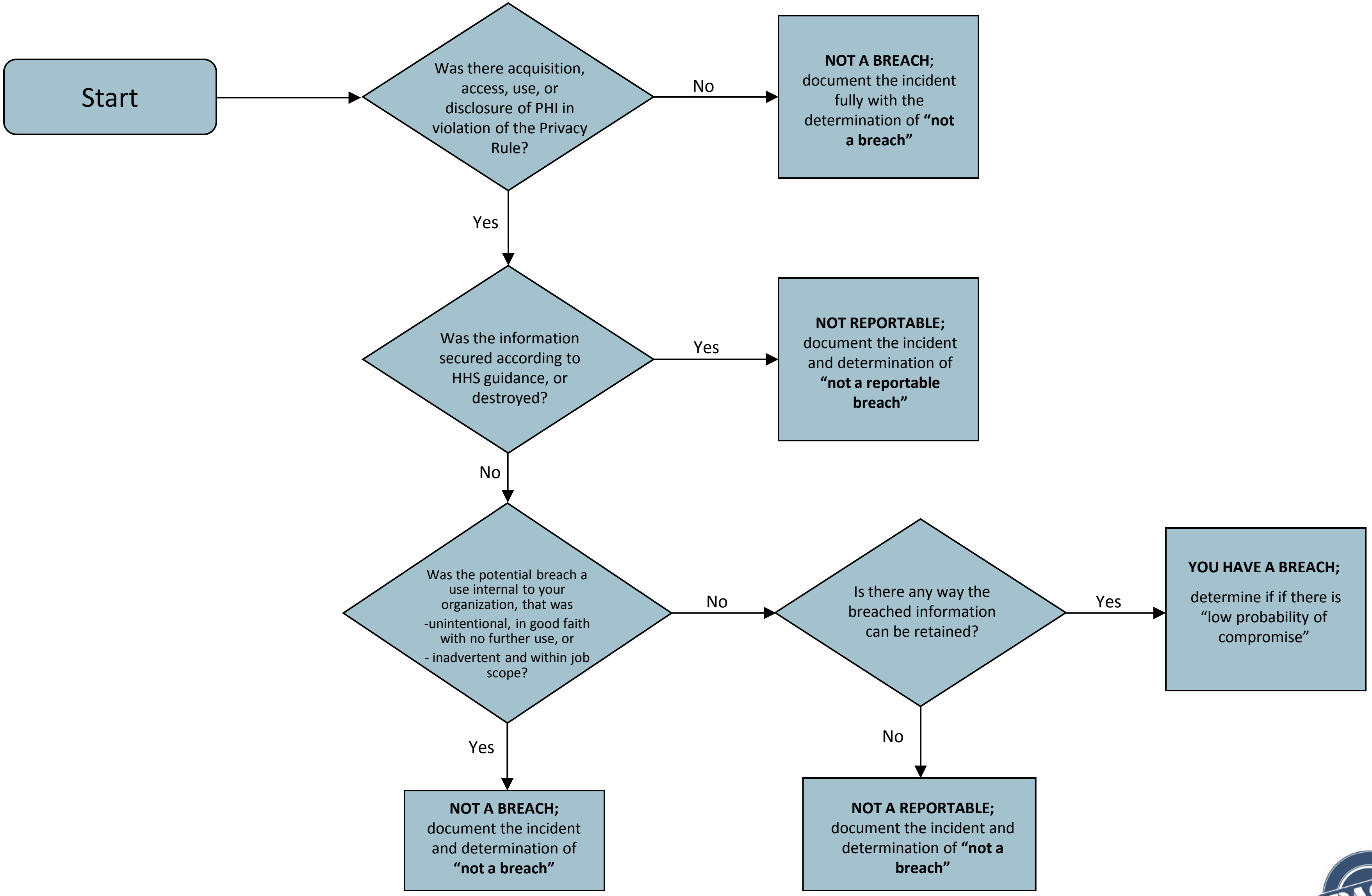
A. A satisfactory assurance has been received from the recipient stating that the PHI has or will not be further used or disclosed

B. The efficiency of the mitigation effectively limited availability to the PHI

C. Does an exception to the notification requirement exist?

D. Do the affected individuals need to be notified?

Breach Notification Decision Tree



Start

Was there acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule?

No

NOT A BREACH; document the incident fully with the determination of **“not a breach”**

Yes

Was the information secured according to HHS guidance, or destroyed?

Yes

NOT REPORTABLE; document the incident and determination of **“not a reportable breach”**

No

Was the potential breach a use internal to your organization, that was
-unintentional, in good faith with no further use, or
- inadvertent and within job scope?

Yes

NOT A BREACH; document the incident and determination of **“not a breach”**

No

Is there any way the breached information can be retained?

Yes

YOU HAVE A BREACH;

determine if if there is “low probability of compromise”

No

NOT A REPORTABLE; document the incident and determination of **“not a breach”**

Evaluating an Incident or Complaint

The reporting obligation for the practice is triggered when a breach of **unsecured** PHI occurs. In order to have a breach of unsecured PHI, there must be **PHI + a violation of the HIPAA Privacy Rule + compromise of the privacy and security of the PHI + unsecured PHI and no breach exclusions**.

Evaluating an Incident or Complaint

A. **PHI involved:** If no PHI is involved, there is no breach of unsecured PHI and no obligation to notify.

B. **Violation of the Privacy Rule:** If the Compliance Officer determines that the violation compromises the privacy and the security of PHI, **then the violation is a "breach."**

C. **Ability of Practice to mitigate the risk of harm:** The risk of harm may depend upon the ability of the Practice to mitigate the effects of the breach.

The Risk Assessment Analysis tool can be used to help clarify whether you have a breach or not.

Action Plan

- Inquire about your incident response plan and review it
- Call a stakeholder meeting to plan improvements to breach readiness
- Update incident response plan
- Initiate review of state and federal breach notification requirements
- Draft/customize all templates
- Finalize roles and responsibilities
- Test your incident response plans

Links

http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Join our Next Webinar

Breach Notification Requirements

Date TBD!

- Timing of Notice
- Content of Notice
- Substitute Notice
- Notice to the Secretary of Health and Human Services
- Notice to the Media
- Necessary Templates
- Notice to Business Associates
- Retention of Documentation

Questions?

Mark Norby, Certified HIPAA Professional

(307) 258-5322

mnorby@healthinsight.org

Visit our website:

www.healthinsight.org/hipaapass

for more information about our Privacy and Security Solutions!

Thank you and have a wonderful day!!