Breach Notification Exercise: Real World Example

- Mat-Su Borough, Alaska (pop. 106,000)
- Zero Day, Advanced Persistent Threat Ransomware Attack
- Malware in a link clicked on by an employee May 3, 2018
- Laid dormant until July 24, 2018, and then a "crypto locker" was launched to lock/encrypt data files
- County was victim #210 of this virus
- Ransom: $400,000
- Infected all IT systems connected to the network (650 desktop computers and servers, networked phones, faxes, printers, copiers); Thousands of individuals
- County declared a disaster due to severity and magnitude of cyber attack
- County resorted to using typewriters, handwritten notes, using runners for messages- for months; disconnected from the internet
- County engaged 20 public and private agencies to assist
    - Law firms, IT consultants, FBI cybercrime unit
- All computers had to be cleaned and systems rebuilt
- Price tag: $2M (professional services, cleaning infected computers and servers, improving security systems with upgrades that had been deferred in the past)
    - State disaster money requested
    - FEMA money requested
    - Cyber insurance claims submitted (they had insurance to cover up to 52 bitcoin (valued at $400K))
- Some historical data was lost
- Ransom typically due in a short period of time, or the cost doubles every x days
    - The City of Valdez, AK was hit with a different ransomware attack the same month, and decided to pay the ransom in order to get the decryption key. Did not have critical data backed up (e.g., 15 years work of police and court data). Their attack infected 27 servers and 170 computers. They negotiated down to 4 bitcoin, which was valued around $26K. Before paying the ransom for the decryption key, they carried out tests to verify that the hacker group truly had the decryption key.
- Decided Not to Pay the Ransom
    - Untenable to use taxpayer dollars this way
    - Critical data had back-up
    - Could not confirm that paying the ransom would unlock the data
- IT analysts could not determine whether attackers accessed PHI (County EMS; County Behavioral Health; County Hospital)

GROUP 1 Questions:

Who do you include in your breach response team?

What are your primary resources (internal and external)? (think: laws, policies, agencies, people)

What is your timeline for the investigation? (Work backward from notification deadlines and other deadlines)

What agencies and third parties do you consider engaging/contacting, and why?

GROUP 2 Questions:

Is this a HIPAA Breach? (complete 4 part risk assessment, attached)

What are the main questions you have in order to answer this question?

GROUP 3 Questions:

Assuming this is a HIPAA breach, who is notified (see attached)?

How are they notified?

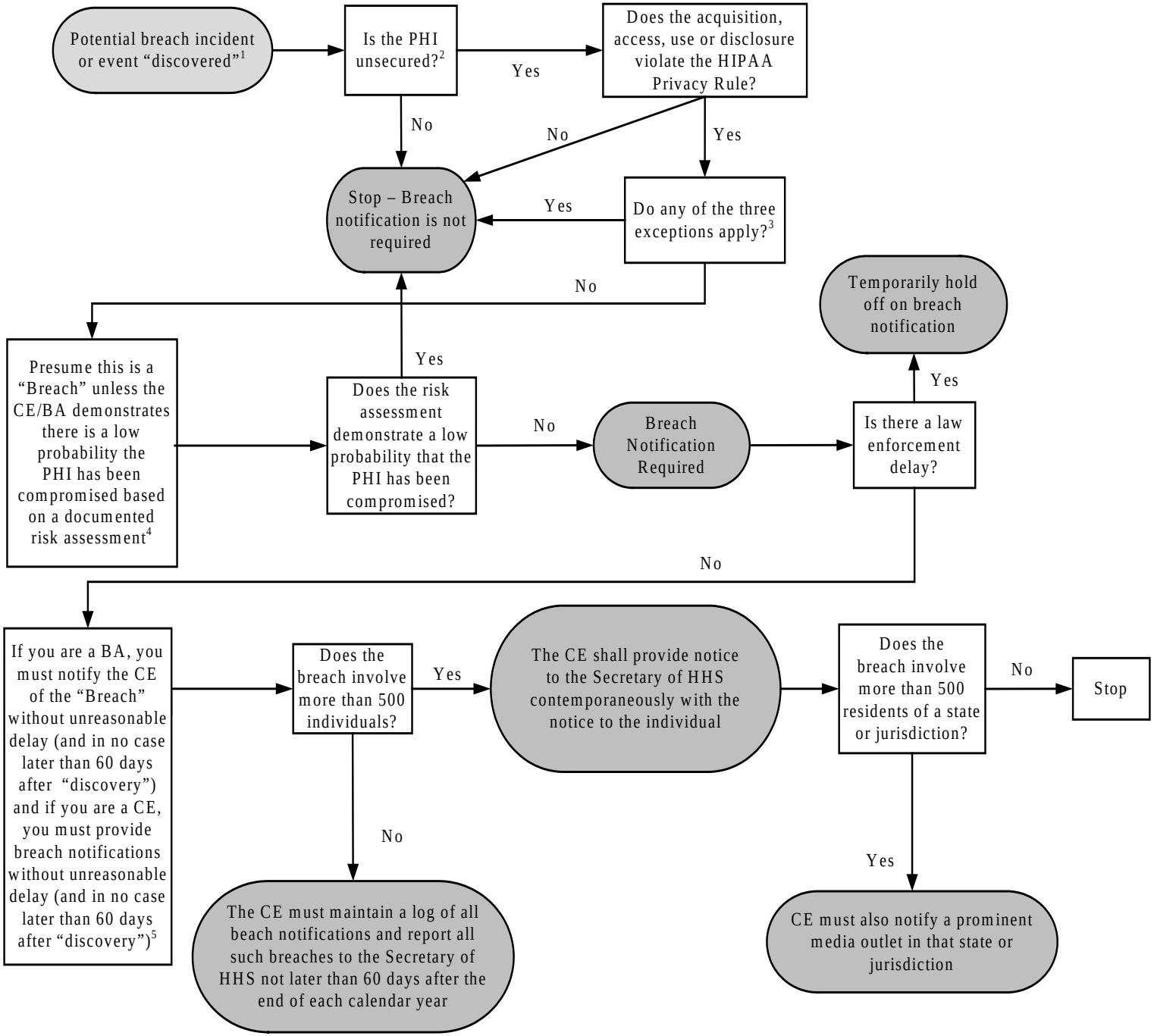
What is included in the notice?

When are they notified?

GROUP 4 Questions:

What are the physical (e.g., hardware, locks, doors), technical (e.g., anti-virus, data-backup) and administrative (e.g., policies, training, auditing) safeguards you would put in place going forward?

HIPAA BREACH NOTIFICATION DECISION TREE FOR COVERED ENTITY



HIPAA BREACH NOTIFICATION DECISION TREE FOR COVERED ENTITY

[1] A "Breach" is the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under HIPAA's Privacy Rule which compromises the security or privacy of the PHI. 45 CFR 164.402

A Breach is "discovered" on the first day on which the breach is known by the CE/BA, or, by exercising reasonable diligence, would have been known. There is a 60-day clock from date of discovery to provide notification. 45 CFR 164.404(a)(2) & (b)

[2] PHI is "unsecured" if it is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary. 45 CFR 164.402

[3] The three exceptions are:

(i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA, 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.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or OHCA in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in the manner not permitted under the Privacy Rule.

(iii) A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom disclosure was made would not reasonably have been able to retain such information. 45 CFR 164.402

[4] The risk assessment must include at least an assessment of the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of a reidentification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated. 45 CFR 164.402

[5] Each individual whose PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, used, or disclosed must be notified:

1. By 1st class mail (or electronic mail if the individual has agreed to electronic notice). If the contact information is out-of-date or insufficient to provide written notice, the CE must provide a substitute notice that is reasonably calculated to reach the individual (If the CE has insufficient contact information for less than 10 individuals, the substitute notice may be by mail, phone or other means. If the CE has insufficient contact information for more than 10 individuals, the substitute notice shall be either by a conspicuous posting on the CE website for at least 90 days, or in major print or broadcast media in the geographic areas where the individuals likely reside).

2. If notice must be sent urgently because of possible imminent misuse of unsecured PHI, the CE may provide information by telephone or other means, as appropriate, in addition to written notice.

3. If the affected individual is deceased, the CE must mail the notification by 1st class mail to the mailing address of the next of kin or personal representative (unless the contact information for the next of kin or personal representative is out-of-date or insufficient).

Breach Notification must be written in plain language and must include the following information:

(i) A brief description of what happened (including the date of the Breach and date of discovery, if known);

(ii) A description of the types of unsecured protected health information involved in the Breach;

(iii) Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

(iv) A brief description of the investigation, actions being taken to mitigate harm and protect against future breaches; and

(v) Contact procedure for more information.

Breach Risk Assessment Tool

Instructions:

This form must be completed thoroughly, in good faith, and the conclusion reached must be reasonable. For very simple incidents, this form may be completed by the Privacy Officer. If the incident is complicated, at least three individuals (e.g., Privacy Officer and other members of the Compliance Committee) should independently complete this form, and meet to discuss their findings. Legal counsel should be consulted regarding breach risk assessments.

****

Date/Description of Incident:

_____

_____

_____

Factors to Consider[1]**:**

1) What is the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification?

   (HHS gave the following examples in the Final Rule:: If you impermissibly disclosed a list of patient names, addresses, and hospital identification numbers, the PHI is obviously identifiable, and a risk assessment would likely show more than a low probability the information was compromised. Alternatively, if you disclosed a list of patient discharge dates and diagnoses, consider whether any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served, or whether the unauthorized recipient may have the ability to combine the information with other available information to re-identify the individuals.)

_____

_____

_____

_____

2) Who is the unauthorized person who impermissibly used the protected health information or to whom the impermissible disclosure was made?

   (HHS gave the following examples in the Final Rule:: If you disclose PHI to another HIPAA-regulated entity, or a federal entity obligated to comply with the Privacy Act of 1974 or Federal Information Security Management Act of 2002, there may be a lower probability of compromise. However, if you disclose dates of health care service and diagnoses of certain employees with their employer, the employer may be able to determine that the information pertains to specific employees based on other information, such as dates of absence from work, creating a greater risk of compromise.)

_____

_____

_____

_____

3) Have you investigated the impermissible use or disclosure to determine if the protected health information was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed? Please explain.

   (HHS gave the following examples in the Final Rule:: If a laptop computer is stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or

[1] For more information on the factors to consider, and a description of each of the examples, please see Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Federal Register 5565 (Jan. 25, 2013).

otherwise compromised, you can determine the PHI was not actually acquired, though the opportunity existed. However, if you mailed information to the wrong individual who opened the envelope and called you to say she received the information in error, then she viewed and acquired the information because she opened and read it.)

_____
_____
_____
_____

4) What is the extent to which the risk to the protected health information has been mitigated?

(HHS gave the following examples in the Final Rule: If you misdirect a fax containing PHI to the wrong physician practice, and upon receipt, the receiving physician calls you to say he has received the fax in error and has destroyed it. HHS has said that though this scenario does not fit into any of the statutory or regulatory exception, HHS believes notification should not be required if you can demonstrate there is a low probability the data has been compromised. The extent of mitigation may depend on the assurances of those who received information in error. For example, you may be able to rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the entity or person destroyed the information it received in error, while such assurances from other third parties may not be sufficient.)

_____
_____
_____
_____

5) Are there any other factors relevant to your analysis of this incident? Please list such factors below:

_____
_____
_____
_____

Based on consideration of the above factors, can we conclude there is a very low probability of compromise? (Please check yes or no).

☐ Yes: Explain why:

_____
_____

☐ No: Breach notification required.

****

Completed by: _____
Title: _____
Date: _____

SAMPLE BREACH NOTIFICATION LETTER (TYPICALLY, BREACH NOTIFICATION SENT BY THE COVERED ENTITY AS REQUIRED BY LAW, SO THIS TEMPLATE LETTER IS INCLUDED FOR YOUR INFORMATION)

[LETTERHEAD]

VIA First Class Mail

[Date]

[Address]

Re: Breach Notification

Dear **[Individual/Next-of-Kin/Personal Representative]**:

[Provide brief description of what happened, including the date of the breach and the date it was discovered] This letter is to notify you that on _____ **[insert date of discovery]** we discovered that your PHI was improperly used or disclosed on or about _____ **[insert date of improper use/disclosure]**. Specifically, we discovered that [describe what happened].

[Provide a description of the types of unsecured PHI that were involved, such as full name, SSN, DOB, home address, account number, diagnosis, or other types of information] The following PHI was involved in the breach: _____.

[Provide a brief description of what you are doing to investigate the breach, to mitigate harm to the Individual, and to protect against further breaches. For example, who was notified and interviewed? What other steps are you taking to investigate the breach? Have you flagged the Individual's account or taken other measures to protect the Individual from further harm, such as offering free credit monitoring for the Individual for a period of time? Were applicable staff members or business associates notified/retrained? Were policies and procedures amended to reflect new safeguards related to preventing other similar breaches? etc.]

[Describe any steps the Individual should take to protect him or herself from potential harm resulting from the breach. For example, consider recommending that the Individual take steps to monitor the Individual's credit for a period of time.]

[Insert the contact procedures for Individuals to use if they have questions. This must include at least one of the following methods of contact: a toll-free telephone number, an email address, a web site, or a postal address.] If you have any questions or would like to talk to someone at _____ about this breach, please contact _____ at _____.

Sincerely,