Breach Notification: Who, when, what, and how?

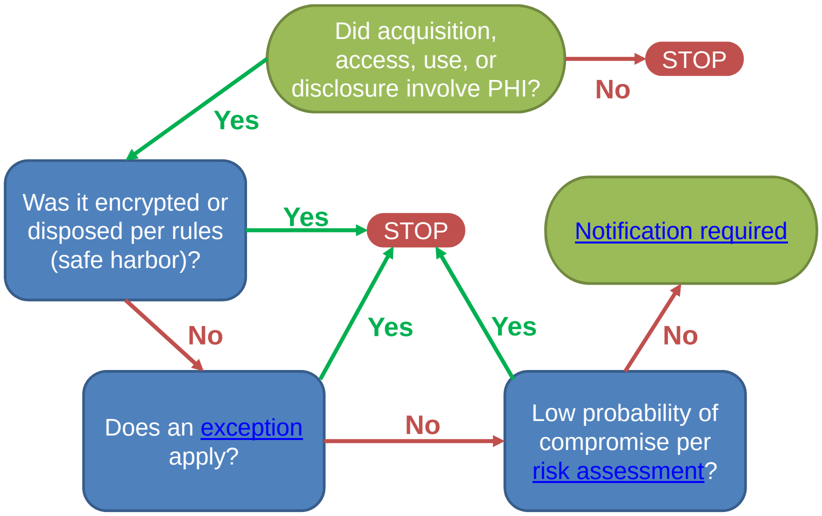
Jill Moore, UNC School of Government

September 2017

UNC SCHOOL OF GOVERNMENT www.sog.unc.edu

Review: What is a breach?

- Acquisition, access, use, or disclosure of protected health information (PHI) that:
  - Is not authorized by the HIPAA privacy rule, <u>and</u>
  - Compromises the privacy and security of the PHI.
- Breach is ***presumed*** unless:
  - A specific exception in the rule applies, or
  - A risk assessment shows a low probability that PHI was compromised.



Did acquisition, access, use, or disclosure involve PHI?

No

STOP

Yes

Was it encrypted or disposed per rules (safe harbor)?

Yes

STOP

Notification required

No

Yes

Yes

No

Does an exception apply?

No

Low probability of compromise per risk assessment?

Exceptions

- PHI could not reasonably be retained
- Access is unintentional and by a workforce member or business associate acting in good faith

- Inadvertent disclosure is made to another person within the CE or BA who is authorized to access PHI

Risk Assessment

What it is:

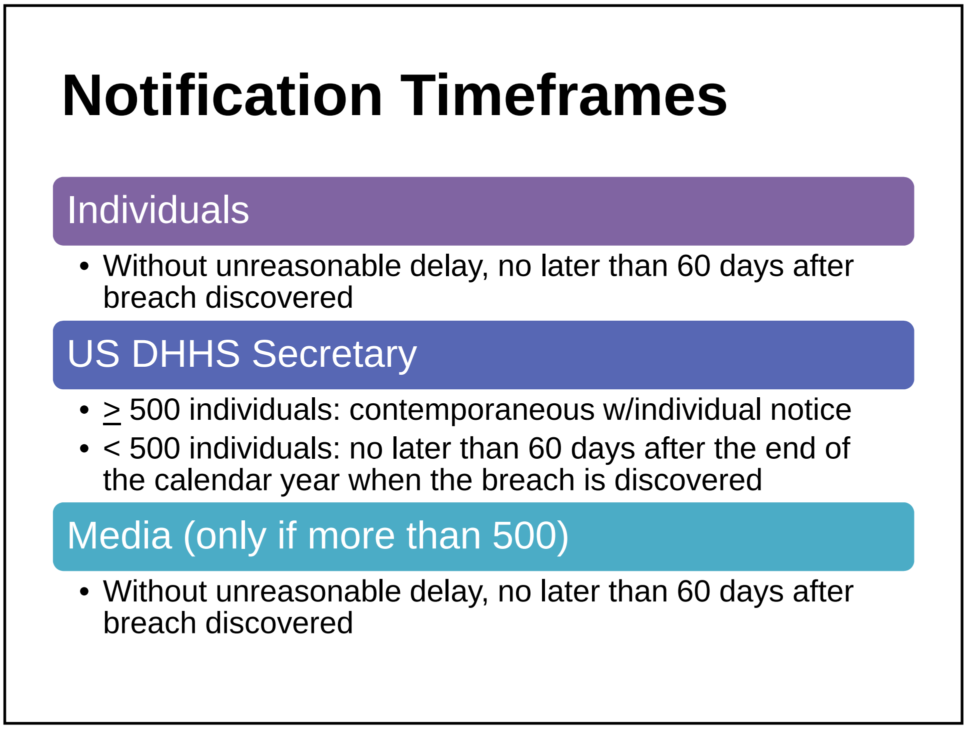
- Analysis you undertake to demonstrate low probability that PHI was compromised
- Demonstrated low probability of compromise defeats the presumption that unauthorized acquisition, access, use, or disclosure was a breach

Minimum factors:

- Nature and extent of PHI, including types of identifiers & likelihood of re-identification
- Unauthorized person who received disclosure or used PHI
- Whether PHI was actually acquired and viewed
- Extent to which any risk to PHI has been mitigated

Notification prep: date check

- If required to notify, must do so “without unreasonable delay” – no later than 60 days after breach discovered
- Breach deemed discovered even if no actual knowledge, if reasonable diligence would have revealed it



Notification Timeframes

Individuals

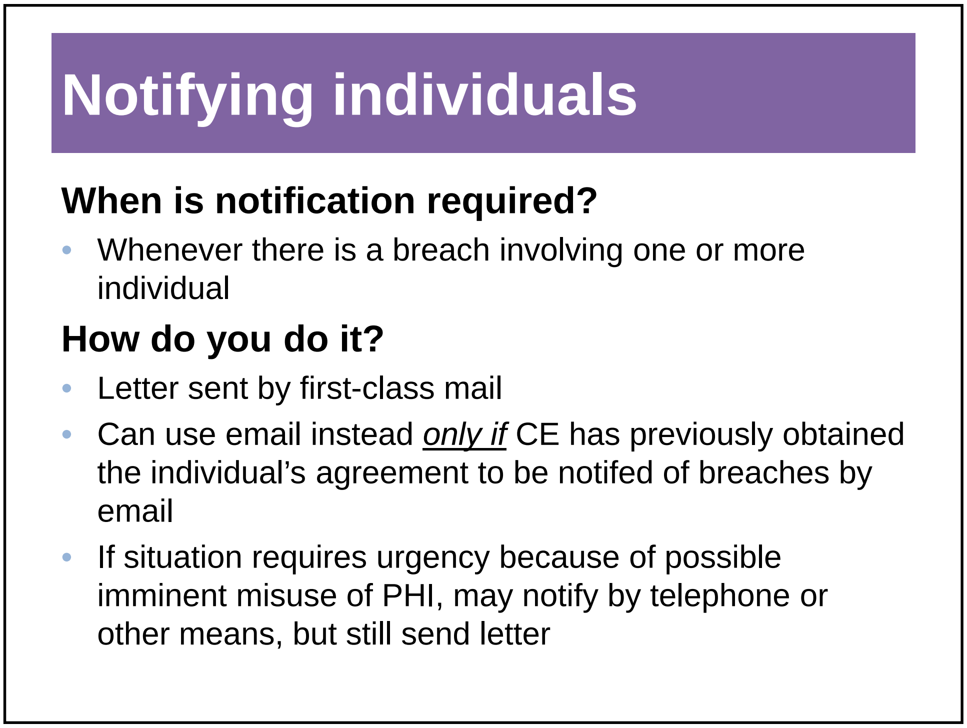
- Without unreasonable delay, no later than 60 days after breach discovered

US DHHS Secretary

- ≥ 500 individuals: contemporaneous w/individual notice
- < 500 individuals: no later than 60 days after the end of the calendar year when the breach is discovered

Media (only if more than 500)

- Without unreasonable delay, no later than 60 days after breach discovered



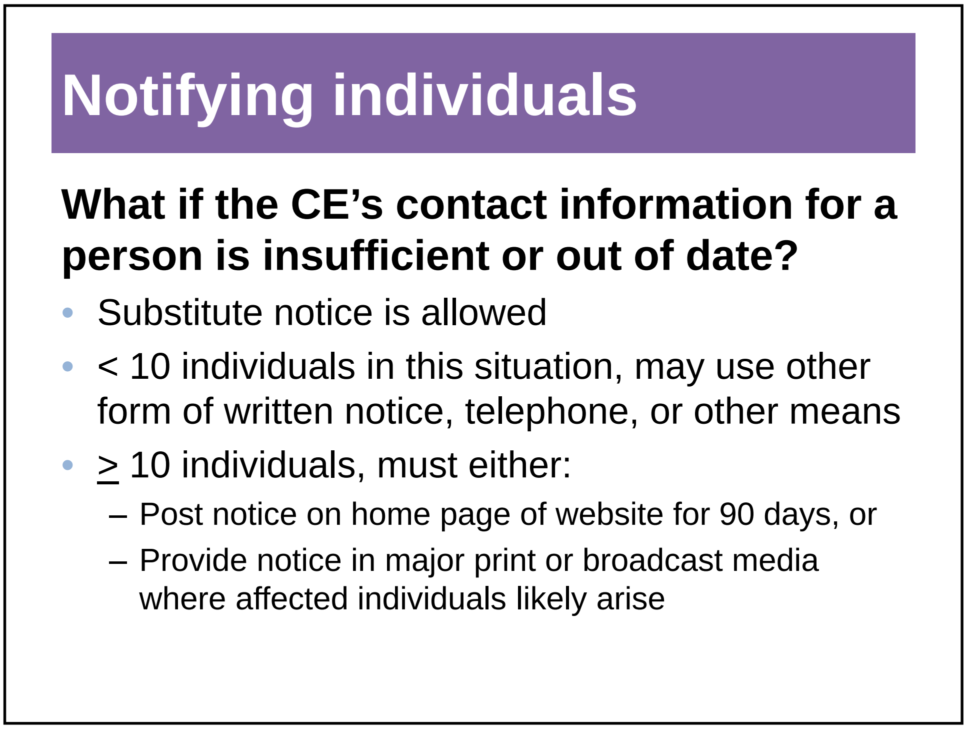
Notifying individuals

When is notification required?

- Whenever there is a breach involving one or more individual

How do you do it?

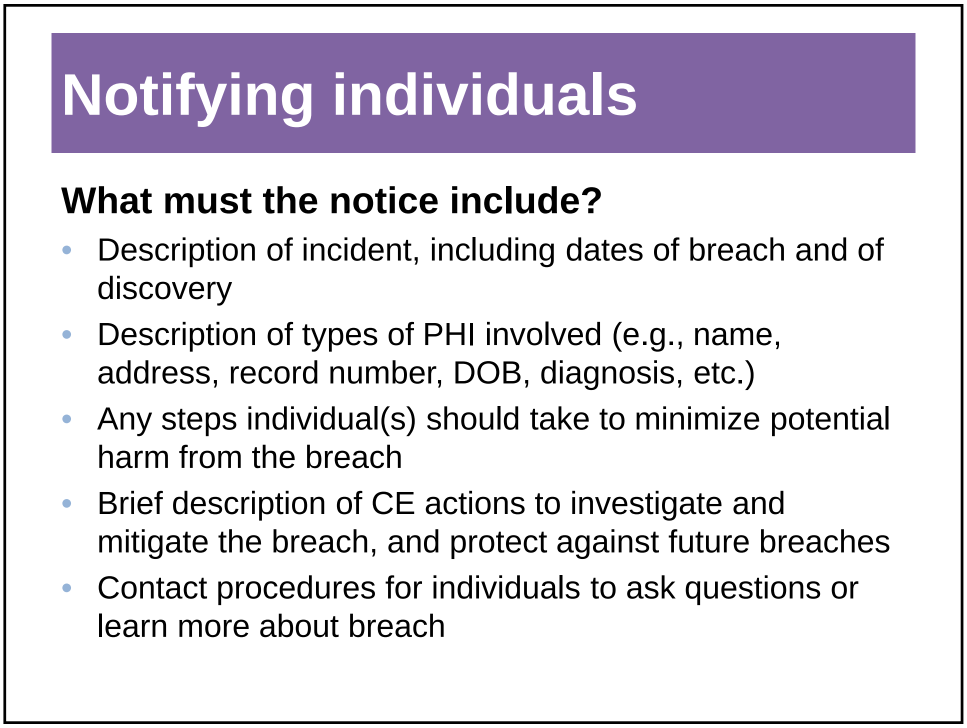
- Letter sent by first-class mail
- Can use email instead *only if* CE has previously obtained the individual’s agreement to be notifed of breaches by email
- If situation requires urgency because of possible imminent misuse of PHI, may notify by telephone or other means, but still send letter



Notifying individuals

What if the CE's contact information for a person is insufficient or out of date?

- Substitute notice is allowed
- < 10 individuals in this situation, may use other form of written notice, telephone, or other means
- ≥ 10 individuals, must either:
  - Post notice on home page of website for 90 days, or
  - Provide notice in major print or broadcast media where affected individuals likely arise



Notifying individuals

What must the notice include?

- Description of incident, including dates of breach and of discovery
- Description of types of PHI involved (e.g., name, address, record number, DOB, diagnosis, etc.)
- Any steps individual(s) should take to minimize potential harm from the breach
- Brief description of CE actions to investigate and mitigate the breach, and protect against future breaches
- Contact procedures for individuals to ask questions or learn more about breach

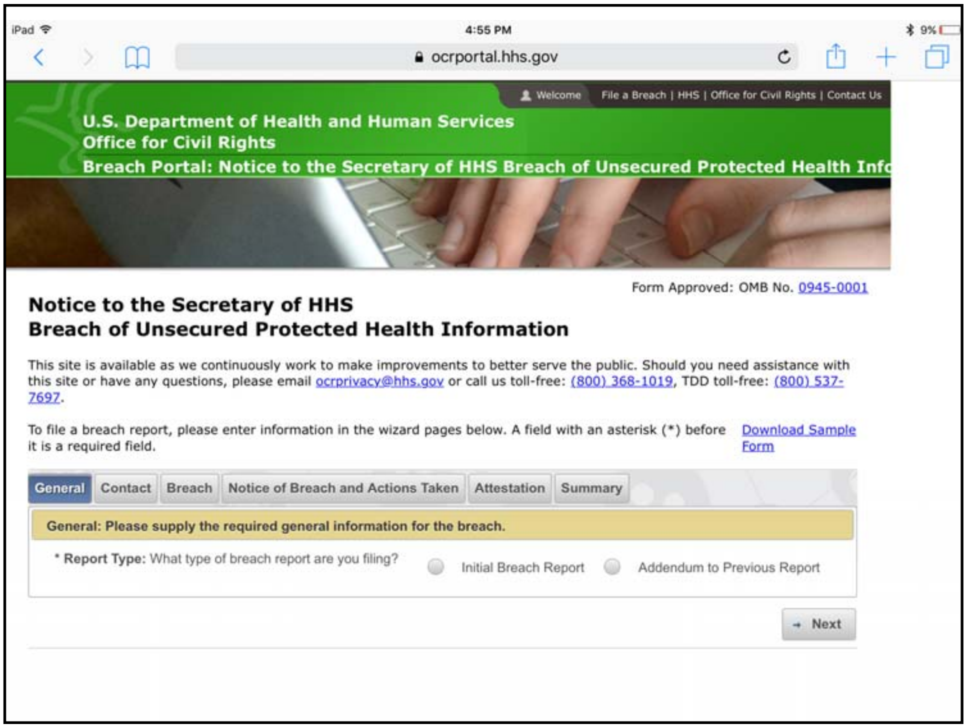
Notifying DHHS

When is notification required?

- Only when there’s a breach of unsecured PHI requiring notification.
- Number of individuals affected determines timing of notification:
  - 500 or more: same time as individual notification
  - Less than 500: within 60 days of end of calendar year

How do you do it?

- Online through HHS website
- One report per breach


iPad
4:55 PM
9%
ocrportal.hhs.gov
Welcome
File a Breach | HHS | Office for Civil Rights | Contact Us
U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Info
General
Contact
Breach
Notice of Breach and Actions Taken
Attestation
Summary
Next

Form Approved: OMB No. 0945-0001

Notice to the Secretary of HHS
Breach of Unsecured Protected Health Information

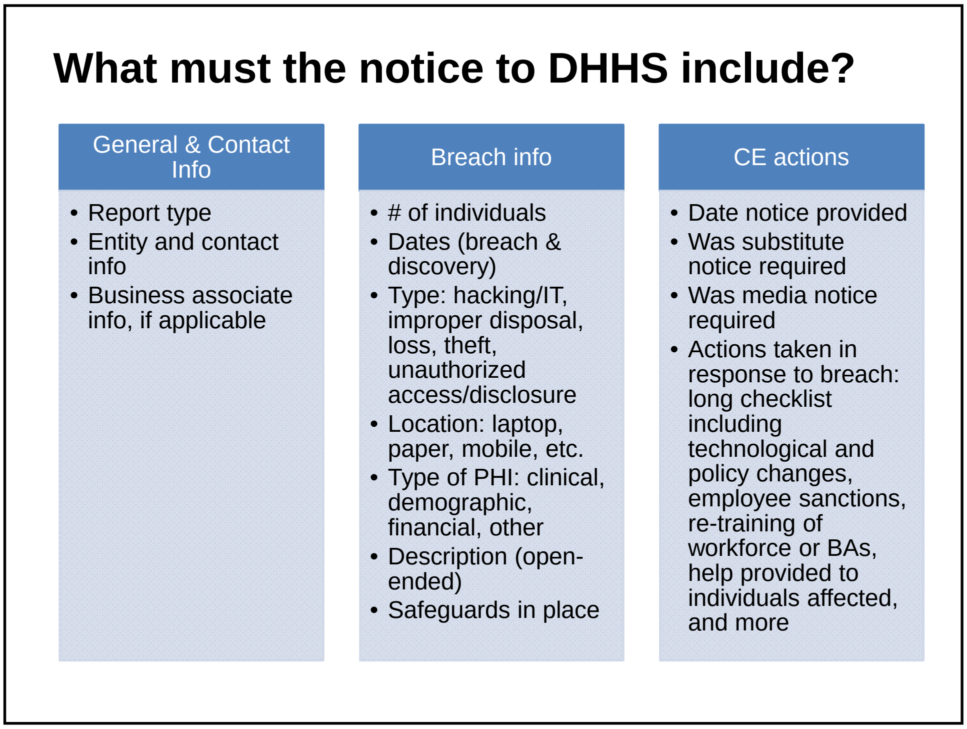
This site is available as we continuously work to make improvements to better serve the public. Should you need assistance with this site or have any questions, please email ocrprivacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697.

To file a breach report, please enter information in the wizard pages below. A field with an asterisk (*) before it is a required field.

Download Sample Form

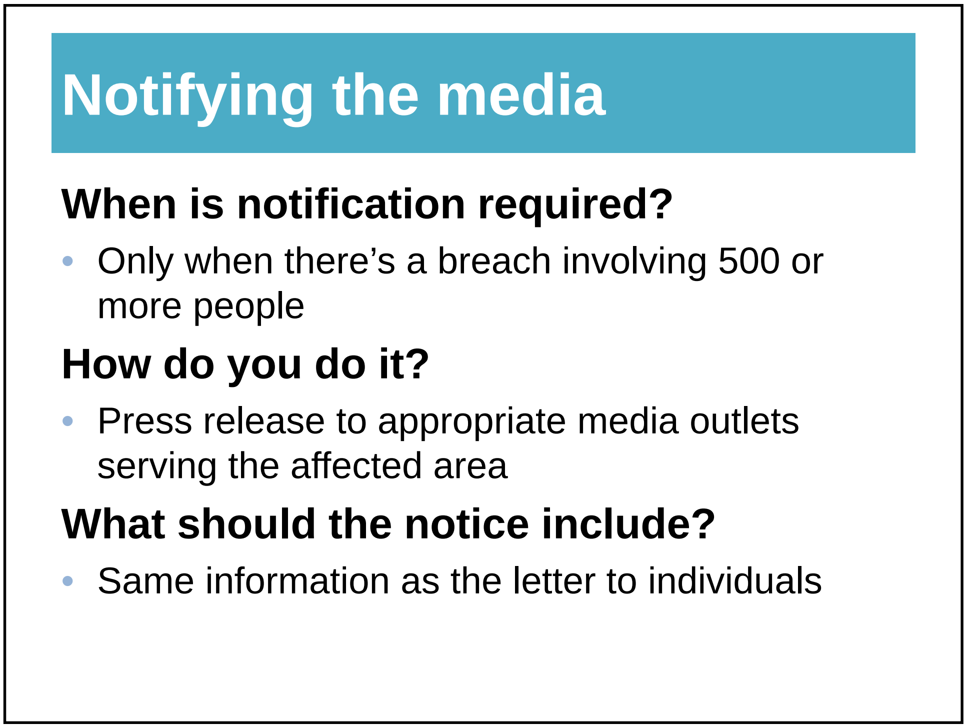
General: Please supply the required general information for the breach.

* **Report Type:** What type of breach report are you filing? ○ Initial Breach Report ○ Addendum to Previous Report



What must the notice to DHHS include?

General & Contact Info	Breach info	CE actions
• Report type • Entity and contact info • Business associate info, if applicable	• # of individuals • Dates (breach & discovery) • Type: hacking/IT, improper disposal, loss, theft, unauthorized access/disclosure • Location: laptop, paper, mobile, etc. • Type of PHI: clinical, demographic, financial, other • Description (open-ended) • Safeguards in place	• Date notice provided • Was substitute notice required • Was media notice required • Actions taken in response to breach: long checklist including technological and policy changes, employee sanctions, re-training of workforce or BAs, help provided to individuals affected, and more



Notifying the media

When is notification required?

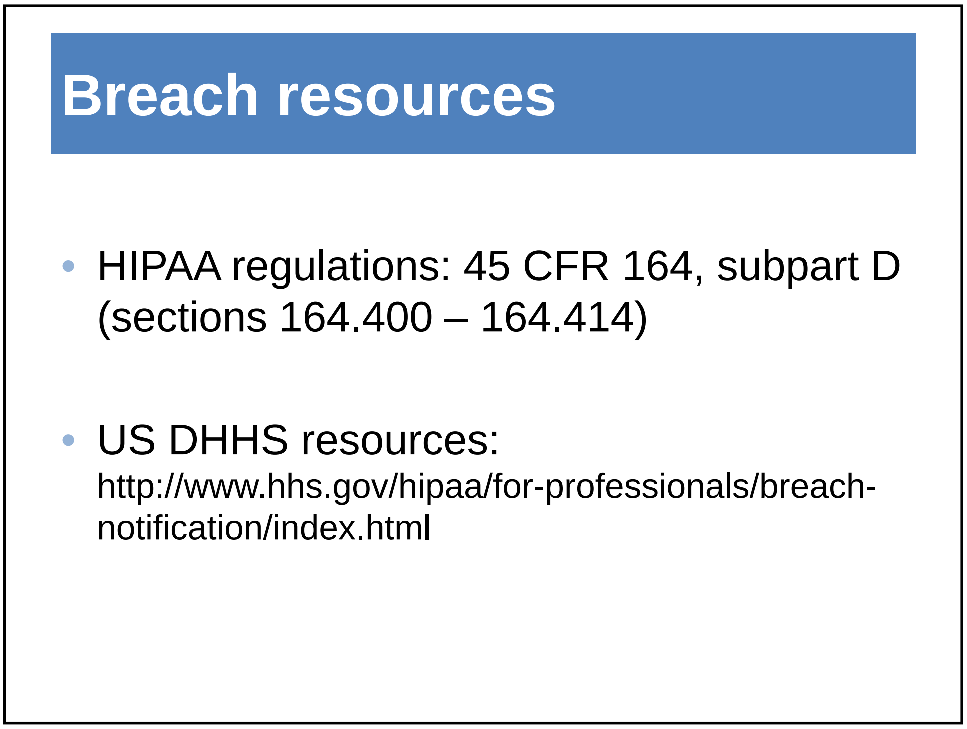
- Only when there’s a breach involving 500 or more people

How do you do it?

- Press release to appropriate media outlets serving the affected area

What should the notice include?

- Same information as the letter to individuals



Breach resources

- HIPAA regulations: 45 CFR 164, subpart D (sections 164.400 – 164.414)
- US DHHS resources: http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html