INCIDENT ASSESSMENT GUIDE

Step 1:
Be sure that any exposure/danger to PHI has been stopped or removed. (e.g., a virus has been removed from a computer, a hacked user account has been disabled and the password has been changed)

Collect all the facts about the privacy/security incident and complete the Breach-Incident Investigation Report. Work with your IT Support to gather all technical facts and documentation. If your incident involved ransomware, complete the Ransomware Incident Response Worksheet, too. It may help to create a timeline of events included in the incident.

Step 2:
Review the Breach Exclusions document to determine your next steps and follow the instructions on the Breach-Incident Investigation Report.

Step 3:
If an exclusion applies to your incident (it is not a breach), document the details of how you came to that determination and record the incident in each patient's file who was impacted on an Accounting of Disclosures Log.

If you determine that your incident is a breach, follow the instructions and timeline for breach notification based on the number of patients involved in the breach. Use the information below together with the Breach-Incident Investigation Report.

BREACH NOTIFICATION

If the breached information contains extremely sensitive information (e.g., diagnoses of HIV, substance abuse, or mental health conditions) or if you suspect any information will be used inappropriately right away, you may call or provide an initial alert in addition to the required notice, below. A phone call is preferred to confirm identity before providing the alert.

You must notify patients whose information has been included in a breach no later than 60 days after it happens/you discover the incident/breach.

Your notice is required to include certain information and must be written in plain language. See the TMC sample notification letter.

Unless a patient has given you *prior* written consent to receive breach notifications via email, the notification must be sent via first-class mail to the patient's last known address or the last known address of their next of kin or personal representative.

OUT-OF-DATE CONTACT INFORMATION

- Less than 10 patients: you may call them or provide an alternative form of written notice.
- 10 or more patients:
  - Post a notice in a prominent location on the homepage of your business's website for 90 days or post a noticeable announcement in major print or broadcast media where the patients are most likely living, **and**

© 2021 Total Medical Compliance

- Include a toll-free number that remains active for at least 90 days where a patient, their next of kin or personal representative can find out if their information was involved in the breach.

500 OR MORE PATIENTS

If, at any time, the number of patients involved in the breach reaches 500, you must also notify:

- The OCR https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true at the same time you send the notice to patients, but within 60 days, **and**
- The media within 60 days, if 500 or more patients live in the same state or jurisdiction. This notice must contain the same information as the notice to individuals.

500 OR LESS PATIENTS

Everything above applies, except the OCR does not need to be notified right away, although it is recommended you do anyway, so you do not forget.

All breaches of less than 500 patients must be reported once per year before the end of February. (60 days after the end of each calendar year)

BUSINESS ASSOCIATES

Business Associates must notify a Covered Entity of a breach within 60 days of discovery, **OR** as specified in the Business Associate Agreement with that Covered Entity.
Business Associates are also required to report all security incidents to the Covered Entity (C.F.R. 45 § 164.314).

NOTIFICATION DELAYS – LAW ENFORCEMENT

If a law enforcement official states that sending or posting a breach notification would disrupt a criminal investigation or endanger national security, you must:

- If the statement is in writing, delay the notification as specified. Verify the statement is authentic.
- If the statement is made in person or via telephone:
    - Document the official's identity (name, badge # or ID) and details of the statement, **and**
    - Request the statement in writing, **and**
    - Delay the notification no longer than 30 days **unless** a written statement is received.

OTHER THINGS TO REMEMBER

- Some state laws require faster notifications.
- Some state laws require identity theft monitoring be provided to those impacted by a breach for a certain period of time.
- Certain office processes, policies, systems, software, or vendors may need to be modified to help prevent future incidents/breaches. Employees may need to be retrained or sanctions might be necessary.

The information provided in this guide is for educational and informational purposes and does not, and is not intended to, constitute legal advice.