BREACH-INCIDENT INVESTIGATION REPORT

Report Date: ____________________ **Date(s) Incident Occurred:** ________________ **Date Discovered:** ________________

Office Name: ____ **Office Phone:** (   ) ______________________

Office Address: ____

I. TYPE OF INCIDENT

Check all that apply or “Other”

□Unauthorized access or edits to PHI (email, EHR/PM, paper file)

□PHI given to wrong recipient (email, fax, patient, phone)

□Inappropriate disposal of PHI (not shredded or destroyed)

□Loss of facility access control (key, code)

□Facility damage impacting access to or availability of PHI (fire, tornado hurricane)

□Username/Passwords shared/stolen

□Hacking and/or phishing emails

□Loss or theft of device storing or accessing PHI

□Unable to restore back-up

□Virus, malware, ransomware (see Ransomware Incident Response Worksheet)

□Other type of issue: ____

□Business Associate involved: ____
Name of BA and what service it provides

II. DESCRIPTION OF THE INCIDENT

1. How was the PHI accessed, used, or disclosed? (e.g., email, phone, fax, EHR, other software) ______________________
____
____
2. How was the incident detected and reported? ____
____
3. Who was involved (workers, business associates, etc.)? ____
____
4. How many patients were impacted? ______________________ Was the issue/incident stopped? ____________________
5. List the people interviewed, the systems/facilities involved, and any reports or other information gathered about the incident. Attach additional pages or reports if necessary. Do not attach PHI. ____
____
____

III. RISK ASSESSMENT

Answer *all* of the following questions to determine if the incident is a reportable breach or if an exclusion might apply.

1. **Type and amount/volume of information.**
   List the types of information accessed, used, or disclosed (e.g., name, DOB, SSN, clinical, financial, insurance ID, etc.)* and the nature of the services provided to the patients (e.g., mental health, substance abuse, infectious disease). Attach additional pages if necessary._______

   ____

   ____

   ____

   *Risk of identity theft, medical insurance fraud, and the danger to patient safety increases if SSN, financial, or insurance information is released.

2. **Who accessed the PHI?**
   Record who accessed or obtained the information and for how long. Was the recipient another covered entity (provider) or business associate covered by HIPAA or other privacy laws, or an unknown recipient? List any protections that were in place prior to the incident (e.g., training, risk analysis, access controls to facility or systems, encryption)

   ____

   ____

3. **Was the information actually accessed or viewed, or did the unintended recipient only have the *opportunity* to access or view the information?**
   There must be proof that access/viewing did not occur (e.g., an envelope sent to an incorrect address was returned to the practice without being opened, or a report from IT showing no access to the system(s) occurred). If unknown, assume it has been accessed and viewed.

   ____

   ____

4. **What steps have been taken to reduce or eliminate the risk of the unauthorized recipient misusing the information? NOTE: *Even if all items below apply, the likelihood that the information could be compromised could still be high and be a breach. See the next section for more information.***

   □ Quick detection and control of the incident

   □ Information was returned/destroyed

   □ Signed non-disclosure attestation: PHI has been destroyed, and no further use/disclosure of the PHI will be made.

   □ Additional actions or details:

   ____

   ____

IV. BREACH DETERMINATION

Use the answers above with the HIPAA Breach Exclusions List, determine the likelihood that the PHI has been or will be used inappropriately.

□ **Incident determined not to be a breach.**

Describe how/why the decision was made. By law, the practice must provide proof to support the decision and actions taken after.

Reason:

- □ PHI was protected by encryption (unusable, unreadable, or indecipherable to unauthorized individuals)
- □ One of these Breach Notification Rule Exceptions have been met:
  - □ The PHI was unintentionally acquired, accessed, or used by a workforce member or person acting in good faith (e.g., not snooping) under the authority of a covered entity or a business associate. The PHI will not be further accessed, used, or disclosed by any person.
  - □ A workforce member at a facility operated by a covered entity or business associate who is authorized to access PHI inadvertently disclosed the PHI to another person at the same facility who is also authorized to access PHI. The PHI will not be further accessed, used, or disclosed by any person.
  - □ It would have been unrealistic for the unauthorized person to retain the PHI that was disclosed. (e.g., patient invoice returned by post office as undeliverable and unopened due to incorrect address)
  - □ Based on *all of* the answers to the 4 questions in the Risk Assessment section, above, it is determined that the **likelihood is low** that the PHI has been or will be used inappropriately. (e.g., not enough data elements were included to identify the patient and non-disclosure attestation signed by a trustworthy source.)
  - □ Other reason and/or additional details (skip to Corrective Action section):

____

____

Incident recorded in all patients' files on an Accounting of Disclosures Log. (Form is on the TMC Client Portal)

□ Date completed: ______________________ (This is not required in breach situations when notifications are sent)

□ **Incident IS a breach because:**

Briefly describe why one or more of the items above does not apply. Example: "Information included the patient's full name and SSN."

____

____

____

V. BREACH RESPONSE

Patients must be notified no later than **60 days** after a breach occurs.

- If you have outdated contact information for 10 or more patients, you must:
  - □ Post a notice in a prominent location on your website's homepage for 90 days **or** post a noticeable announcement in a major print or broadcast media where those patients most likely live, **AND**
  - □ 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.
- Date Patients Notified (first class mail): ____________________ (*prior* consent is required to notify via email)
  - □ The breach impacted 500 or more patients. If yes, the following actions are *required.*
    - □ Prominent media outlet MUST be notified at the same time patients are informed.

      Name of media outlet and date notified: ____
    - □ Notify the OCR by filling out a report on the OCR's website: https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf

      Date OCR Notified: ________________________
- All breaches of less than 500 patients must be reported to the OCR once per year before the end of February. (60 days after the end of each calendar year)

NOTE: Attach all supporting documentation (no PHI) and include a sample copy of the patient notification(s) and any other communications.

VI. CORRECTIVE ACTION

Describe actions taken after the incident or breach response to help reduce the likelihood of repeating the same or similar event in the future.

Things to consider:

New/improved policies and/or procedures	New security measures or software updates	Changing passwords
Sanctions imposed on workforce members	Replacing a business associate/vendor	Retraining or new training

____

____

____

____

____

____

Retain all documentation related to the incident/breach for 6 years.

This report was prepared by (print name): ________________________________

Preparer's role: ____

Preparer's Signature: ____ Date: ________________________________

Privacy/Security Officer's Name: ____

Signature: ____ Date: ________________________________

Use this page to track any post incident/breach response action items and their status.

Date:	Note/Status:

SAMPLE BREACH NOTIFICATION TEMPLATE

- This sample template may be used as a guide to notify patients impacted by a breach of PHI.
- Instructions in *italics* include breach notification requirements from **45 C.F.R. § 164.404**, *Notification to individuals*.

An electronic version of this document is available on the TMC Client Portal.

Name of Practice: ____________________

Address: ____________________

Phone number: ____________________

Toll Free Info Line (if required): ____________________

Dear [Patient Name]:

This letter is to inform you of a breach of your protected health information.

Provide a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

The following information was inappropriately accessed or shared:

A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
Do not include the PHI involved.

We are committed to the protection of your personal information and apologize for this event. We are taking the following steps to help prevent this from happening in the future:

A brief description of what the covered entity (or business associate) involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

Please closely monitor your credit reports and investigate and charges to any accounts that you have not authorized. By law, you can get a free copy of your credit report every 12 months from each credit reporting company at www.annualcreditreport.com.

Any steps individuals should take to protect themselves from potential harm resulting from the breach. While not required by federal law, the CE may consider offering credit monitoring. Some state laws require 1 year of credit monitoring.

Please feel free to contact us with any questions or concerns you may have about this situation. You may reach us at the number listed above, or [fill in other method].

Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number (if required), an e-mail address, website, or postal address.

Sincerely,
Privacy Officer/Office Manager