BREACH/INCIDENT INVESTIGATION REPORT

Report Date: _____ **(Estimated) Incident Date:** _____

Office Name: _____

Office Address: _____

Type of Incident – Check all that apply:

- ☐ Stolen/sharing of passwords used to obtain access to ePHI
- ☐ Hacking actual/attempted
- ☐ Unauthorized program downloaded
- ☐ Evidence of unauthorized data changes
- ☐ System failure – hardware or software
- ☐ Inability to access information
- ☐ Computer behaving as if someone else has control
- ☐ Ability to access information outside of assigned scope
- ☐ Evidence of entry of malware – see Ransomware Incident Response Worksheet, if applicable
- ☐ Acts of Nature – fire, tornado, hurricane
- ☐ Loss of facility keys/access code
- ☐ Email asking for account information
- ☐ Unauthorized destruction of data
- ☐ Inability to restore ePHI from back-up source/device.
- ☐ Other: _____

Description of the incident: How was the PHI was accessed, used, or disclosed? How was it was detected and reported? Who was involved (workers, Subcontractor BAs, etc.)? Was it stopped? How many patients?

_____

_____

_____

_____

List the elements of the investigation: Reports reviewed, people talked to, systems/facilities involved, etc. Attach additional sheets if necessary. Do not attach PHI.

_____

_____

_____

RISK ANALYSIS

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

1. Type and amount/volume of information.

Types of PHI involved* Include the amount and type of clinical information released (name, DOB, SSN, insurance, or financial information, etc.) and the nature of the service (mental health, infectious disease).

_____

_____

_____

*Risk increases when credit card, SSN, or insurance info is released due to identity theft, medical insurance fraud, and patient safety.

2. Who accessed the PHI?

Record who accessed or obtained the information. Was the recipient another CE or BA covered by HIPAA or other privacy rules or an unknown recipient?

_____

_____

3. How was the PHI accessed? How long was it accessed? Is it likely to be retained or was it briefly viewed?

Provide detail on what/who confirmed the incident occurred and how this determination was made. For instance, did you receive evidence from event/audit logs that show if the information was accessed, downloaded, or printed? Did you receive a confirmation that the information was destroyed and not used/further viewed or retained (e.g., fax sent in error)?

_____

_____

_____

4. To what extent has the risk of someone misusing the PHI been reduced or eliminated?
***Even if all items below are met, the incident may still be a reportable breach*.**
Select all that apply.

☐ Quick detection and response to the event.

☐ Information returned.

☐ Signed nondisclosure attestation, PHI is being destroyed, no copies retained, and no further use of the PHI will be made.

☐ Additional actions or details:

_____

_____

_____

5. Breach determination.

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

☐ **Not a breach because**:

- ☐ Data protected by encryption.
- ☐ Meets one of the following exceptions allowed by the Privacy Rule:
  - ☐ The PHI was unintentionally acquired, accessed, or used by a workforce member or person acting under the authority of a covered entity or a business associate. PHI will not be further used or disclosed in a manner not permitted under the Privacy Rule.
  - ☐ The PHI was inadvertently disclosed by a person 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. PHI will not be further used or disclosed in a manner not permitted under the Privacy Rule.
  - ☐ It would have been unrealistic for the unauthorized person to retain the PHI that was disclosed.
  - ☐ Signed nondisclosure attestation, PHI is being destroyed, no copies retained, and no further use of the information will be made.

☐ Other reason and/or additional details (skip to Breach Response):

_____

_____

_____

_____

☐ **Is a breach because**:

_____

_____

_____

_____

6. Breach Response – attach additional pages to track notification dates and obligations to CEs from Business Associate Agreements:

Date CEs/Patients Notified: _____ Date OCR Notified: _____

☐ The breach impacted 500 or more patients:

☐ OCR/HHS and a prominent media outlet MUST be notified at the same time patients are informed (if performed on behalf of the CEs).

Notify the OCR by filling out a report on the OCR's website: https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf.

Refer to the TMC Incident Assessment Guide in the Client Portal.

☐ Noticeable announcement posted in major print or broadcast media, if necessary (list media outlet):

Name: _____ Date: _____

☐ Posted on your website's homepage from (date): _____ to (date): _____
Should be posted for 90 days.

NOTE: Attach all supporting documentation and include a copy of the patient notification(s).

7. Unauthorized Access, Use, or Disclosure:

☐ Accounting of Disclosures entries made in all patient records on (date): _____

8. Corrective Action:

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

Things to consider: New/improved policies or procedures, sanctions imposed on workforce members involved in the incident/breach, new or re-training of workforce, replacing a business associate vendor, etc.

_____

_____

_____

_____

This report was prepared by (print name): _____

Preparer's role/title: _____

_____ _____

Preparer's Signature Date

_____ _____

Privacy Officer Name and Signature Date

Document any follow-up or post incident/breach status updates and notes here:

Date:	Note/Status:

SAMPLE BREACH NOTIFICATION LETTER TEMPLATE

This sample template may be used 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 sample is available on TMC's Client Portal.

Name of Practice: _____

Address: _____

Phone number: _____

Toll Free Info Line: _____

Dear Sir or Madame:

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 – see the TMC Incident Assessment Guide), an e-mail address, website, or postal address.

Sincerely,

Privacy Officer/Office Manager