PRIVACY BREACH ASSESSMENT

1) Was Private Information Involved? ☐ Yes ☐ No

2) Was the Private Information encrypted? ☐ Yes ☐ No

3) Description of breach:

a) What data elements have been breached? Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.

b) What possible use is there for the private information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

c) What was the date that the breach was discovered? _____

d) What is believed to be the date that the breach occurred? _____

2) Cause and Extent of the Breach

a) What is the cause of the breach?

b) Is there a risk of ongoing or further exposure of the information? ☐ Yes ☐ No

c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?

d) Is the information encrypted or otherwise not readily accessible? ☐ Yes ☐ No

e) What steps have already been taken to minimize the harm?

3) Individuals Affected by the Breach

a) How many individuals are affected by the breach? ☐

1. Who was affected by the breach:

☐ Employees

☐ Customer-owners

☐ Volunteers

☐ Contractors

☐ Service providers

☐ Other individuals/organizations

4) Foreseeable Harm from the Breach

a) Is there any relationship between the unauthorized recipients and the data subject?
☐ Yes ☐ No

b) Is any of the information or the individual whose information was compromised subject to additional protections, such as court orders, temporary restraining orders, protections from harm, etc.?

2. What harm to the individuals will result from the breach? Harm that may occur includes:

☐ Security risk (e.g., physical safety)

☐ Identity theft or fraud

☐ Loss of business or employment opportunities

☐ Hurt, humiliation, damage to reputation or relationships

☐ Other (please specify):

d) What harm could result to the organization as a result of the breach?

☐ Loss of trust in the organization

☐ Loss of assets

☐ Financial exposure

☐ Other (please specify):

e) What harm could result to the public as a result of the breach?

☐ Risk to public health

☐ Risk to public safety

☐ Other (please specify):

1. <u>Privacy Act Analysis</u>
    a. Determine whether the breached information was in the control and possession of a Federal agency. If not, the Privacy Act does not apply and the analysis below is not necessary.
    b. Determine if the incident poses a risk to individuals. The following factors shall be considered when assessing the likely risk of harm and level of impact for a potential or confirmed privacy breach:

i. Nature of the data elements breached in light of their context and the broad range of potential harms that may result from their disclosure to unauthorized individuals;

ii. Potential harm to reputation of individuals;

iii. Potential for harassment or prejudice;

iv. Potential for identity theft, including any evidence that breached information is actually being used;

v. Number of individuals affected;

vi. Likelihood that breach was the result of a criminal act or will result in criminal activity;

vii. Likelihood the information is accessible and usable by unauthorized individuals;

viii. Likelihood the breach may lead to harm; and

ix. Ability to mitigate the risk of harm.

c. If an identity theft risk is present, tailor the response to the nature and scope of the risk presented. Notice may not be required in all circumstances, so the response team should assess the situation and determine if notification to individuals is necessary. In some cases, notification may actually increase a risk of harm, in which case <Practice> should delay notification until proper safeguards can be instituted. The analysis of whether notification is necessary should be based on the following factors:

i. Number of individuals affected;

ii. Urgency with which individuals need to receive notice;

iii. Whether other public and private sector agencies need notification, particularly those that may be affected or may play a role in mitigating the breach;

iv. Contact information available for affected individuals (first-class mail shall be the primary means for providing notification, but telephone or email may be appropriate when there is an urgent need); and

v. Whether media outlets may be the best way to alert affected individuals and mitigate any risk.

d. Written notification should include the following elements:

i. Brief description of what happened, including the date of the breach and its discovery;

ii. Description of the types of information involved in the breach;

iii. Statement whether the information was protected, if such information would be beneficial and would not compromise security;

iv. Steps individuals should take to protect themselves from harm;

v. What <Practice> is doing to investigate and mitigate the breach; and

vi. Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address and postal address.

e. If the <Practice> response team determines that public notification through the media is necessary, it should also post notification of the breach on its website, with the same information required for written notification to the individual. The posting should provide answers to frequently asked questions and other talking points.

2. State Data Breach Analysis

   a. Identify the state of residence of all individuals affected by the breach.

   b. Consult individual state data breach statues to determine if a state's particular data breach statute is applicable to <Practice>.

   c. Consult individual state data breach statutes to determine if a breach has occurred under a state's particular data breach statute.

   d. Consult individual state data breach statutes to determine breach notification steps to take in accordance with a state's particular data breach statute.

3. HIPAA/HITECH Analysis

   a. Determine whether the breached information was Protected Health Information (individually identifiable health information as defined by HIPAA). If not, HIPAA/HITECH breach reporting requirements do not apply and the analysis below is not necessary.

   b. If breached information was PHI, determine whether the PHI was secured or unsecured. Unsecured PHI is defined as PHI that is not secured through a means that HHS has approved as rendering the PHI unusable or unreadable to unauthorized persons.[1] If PHI was secured, no reporting is necessary under HIPAA and you can proceed to Step 2.

[1] As of the date of drafting, the following guidance was provided – COVERED ENTITY should review published guidance periodically to see if additional guidance was issued:
1) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and are judged by HHS to meet this standard.

c. If PHI was unsecured, it constitutes an official breach under HIPAA if it "compromises the security or privacy of the PHI" and does not meet one of the exceptions to breach.

   i. Compromises the security or privacy – this means that it poses a significant risk of financial, reputational or other harm to the individual. Sections 2 and 4 of the Privacy Breach Questionnaire should assist with this analysis. Key factors to consider:

      1. To whom was the information disclosed?
      2. What type of information was breached?
      3. How easily can the information be redistributed?

   ii. Exceptions to breach (these factors are fairly subjective and any analysis resulting in the conclusion that a disclosure meets one of these exceptions should be documented and retained for seven years):

      1. Good faith and unintentional acquisition, access or use by a person working under the authority of a covered entity or business associate, which is within the scope of authority and does not result in further use or disclosure.
      2. Disclosures between persons at the same covered entity, business associate or organized health care arrangement if persons are authorized and information will not be further used or disclosed.
      3. Disclosure where the covered entity or business associate has the good faith belief that the information could not have been retained (for example, a person drops their jump drive overboard on a moving cruise ship).

---

i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

ii) Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140- 2. These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated.

2) The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

d. If the disclosure is found to meet one of these exceptions, or is not found to compromise the security or privacy of the PHI, proceed to Step 2. If the disclosure does not meet one of the exceptions to breach, and it is found to compromise the security or privacy of the PHI, the next step is to determine how to mitigate the breach and protect the individual. Part of the mitigation and protection efforts would include notification, but they may also include instituting additional security measures, changing a person's account number, notifying police of the breach and other appropriate measures.

e. After determining and instituting mitigation and protection efforts, <Practice> must fulfill its obligations to notify the affected individuals of the breach. Notice must be provided within 60 days of discovery[2], unless authorized to delay by law enforcement personnel. First, <Practice> should determine how notice should be sent to the individual. The following rules apply:

    i. If contact information is sufficient and no more than 500 residents in the state are affected, written notification should be sent by first class mail.

    ii. If contact information is not sufficient for more than 10 individuals, notification must also be on the <Practice> home page and in major media (print or broadcast).

    iii. If more than 500 residents are affected, notification must also be made to major media, even if contact information is sufficient for all affected persons.

f. Notice should be carefully drafted to include the following required information, without any unnecessary information that may result in additional questions or concerns from affected individuals:

    i. Brief description of the breach, including the date of the breach and date of discovery.

    ii. Description of the types of PHI involved.

    iii. Steps the individual should take to protect themselves.

    iv. Brief description of steps <Practice> is taking to mitigate, investigate and protect (careful not to disclose information that could hamper any ongoing investigation).

    v. Contact procedures for questions or additional information, including a toll-free telephone number, email, Web site or address.

g. If more than 500 persons are affected, notice must also be provided to the U.S. Department of Health and Human Services. If 500 or less are affected, the notice should be kept in an annual log of breaches.

[2] Discovery is defined as when the breach is known or should reasonably have been known.

4. Breach Analysis Follow-Up: Once the breach analysis is complete and notice is provided, <Practice> should review policies, procedures and security measures to incorporate any necessary updates or changes.