UAHCC Incident Form

Risk Evaluation

Incident Description:

Date of Incident:	**Covered Entity Involved:**	**OIT Security Member Involved:**
Date of Discovery:	**How was incident discovered?**	

Describe the nature of the incident:

Location of Information:

☐ Laptop ☐ Desktop Computer ☐ Network Server ☐ Email ☐ Paper

☐ Electronic Medical Record ☐ Other (specify):

Estimated # of individuals affected:	**Type of affected individual(s):**
	☐ Patients ☐ Research Participants ☐ Others (specify):

Personal Information Involved:

☐ Name ☐ Date of Birth ☐ Social Security Number ☐ Address ☐ Bank Account Information

☐ Clinical Information: __diagnosis/conditions __ lab results __ medications __ other treatment information

☐ Other (specify):

Type of Suspected Breach:

☐ Theft ☐ Loss ☐ Improper Disposal ☐ Unauthorized Access ☐ Unauthorized Disclosure

☐ Hacking/IT Incident ☐ Other (specify):

Safeguards in Place:

☐ Firewalls ☐ Packet Filtering (router-based) ☐ Secure Browser Sessions ☐ Strong Authentication

☐ Encrypted Wireless ☐ Physical Security ☐ Logical Access Control ☐ Anti-Virus Software

☐ Intrusion Detection ☐ Biometrics ☐ Other (specify):

Did a Breach Occur & is Notification Required? (must occur within 60 days of discovery of breach)

Did the suspected breach involve PHI?

☐ Yes (continue with questions) ☐ No (no notification required)

Was the PHI secured?

☐ Yes: ☐ Encrypted (no notification required) ☐ Destroyed (no notification required)

☐ No (continue with questions)

Was the use or disclosure of PHI permitted by the HIPAA Privacy Rule?

☐ Yes (no notification required) ☐ No (continue with questions)

Did the use or disclosure of PHI fall within any of the exceptions to breach reporting? If none of these, continue with questions. If any one of these exceptions applies no notification is required.

☐ Disclosure of limited data set (unless it contained DOB or zip code)

☐ Unintentional/good faith acquisition, access, or use of PHI by employee or BA

☐ Inadvertent disclosure by an authorized individual to another within the same entity or BA if PHI is not further used or disclosed

☐ Disclosure in which an unintended recipient could not reasonably retain the information, based on good faith belief of entity or BA

Was this use or disclosure of PHI due to the activities of a whistleblower (an individual exercising his/her established rights to file a complaint against the covered entity)?

☐ Yes (no disciplinary action can be taken against the individual using/disclosing the information and notification may not be required due to the agency/group to whom the PHI was disclosed) ☐ No

Probability of Compromise of PHI from Incident:

Is there a low probability that the PHI involved was compromised? If yes, then the incident is not a breach and notification is not required.

The following four factors will be considered:

Risk Score: Score each factor:
1 = low probability
2 = medium probability
3 = high probability

• Nature and extent of PHI involved, including the types of information (identifiers included), likelihood it could be re-identified, and if it could be used in a manner adverse to the individual; examples: SSN, credit card number, amount of information	**1 2 3**
• The unauthorized person who used the PHI or to whom an improper disclosure was made	**1 2 3**
• Whether the PHI was actually acquired or viewed (accessed)	**1 2 3**
• The extent to which the risk to the PHI was/has been mitigated; examples include satisfactory assurances (confidentiality agreement) from recipient or information destroyed	**1 2 3**
• Other considerations as deemed appropriate:	**1 2 3**

Single score >1=notification

Probability of Compromise Conclusion:

Notification

☐ **UA Security Officer**	Who was notified?	Date of notification:
	Method of notification (phone, email, letter, etc.):	
☐ **UA Privacy Office**	Who was notified?	Date of notification:
	Method of notification (phone, email, letter, etc.):	
☐ **Data Custodian**	Who was notified?	Date of notification:
	Method of notification (phone, email, letter, etc.):	
☐ **UAS (Systems Office notified to determine cyber insurance reporting)**	Who was notified?	Date of notification:
	Method(s) of notification (phone, email, letter, etc.):	
Check those notified: ☐ UA President ☐ UA Provost ☐ Strategic Communications ☐ Strategic Communications ☐ UAS (Systems Office – Cyber Insurance ☐ UA CIO ☐ UA Security Office ☐ UAHCC Dean ☐ UAHCC HIPAA Privacy Officer ☐ UAHCC HIPAA Security Officer	Date & Method of Notification?	By Whom?
	☐ No. Provide reason for not issuing notification (i.e., incident excluded from breach notification requirements, no significant harm or negative impact to the	

<table>
<tr><td rowspan="3">☐ Individual(s) Affected by Incident</td><td colspan="2">individual(s), low risk score, etc.)</td></tr>
<tr><td colspan="2">☐ Yes
- Method of notification (phone, email, letter, etc.):
- Date of notification:
- Number of individuals notified:
- Date of Substitute Notice (if required):</td></tr>
<tr><td colspan="2">Information to include in notification:
☐ Date of breach
☐ Date of discovery of the breach
☐ Description of the information inappropriately accessed, collected, used or disclosed
☐ Risk(s) to the individual caused by the breach
☐ Steps taken to control or reduce harm and protect against further harm
☐ Steps to be taken in the future to further protect the individual
☐ Steps the individual can take to protect him/herself
☐ Whether notification about the incident has been made to a regulatory agency
☐ Privacy contact information
☐ Organization contact information for further assistance
☐ Other information:</td></tr>
<tr><td rowspan="2">☐ Department of Health and Human Services</td><td>Who was notified?</td><td>Date of notification:</td></tr>
<tr><td colspan="2">Reason for notification:
☐ Breach affects more than 500 individuals
☐ Annual notification (added to the breach log)
☐ Other (describe):</td></tr>
<tr><td rowspan="2">☐ Local Media</td><td>Who was notified?</td><td>Date of notification:</td></tr>
<tr><td colspan="2">Reason for notification:
☐ Breach affects more than 500 individuals
☐ Other (describe):</td></tr>
<tr><td rowspan="3">☐ Law Enforcement Authorities</td><td>Who was notified?</td><td>Date of notification:</td></tr>
<tr><td colspan="2">☐ Notification Delayed due to Law Enforcement Investigation. Must obtain notice from Law Enforcement stating that the notification is to be held, and notice as to when notification can be made.</td></tr>
<tr><td colspan="2">Reason for notification:
☐ Identity Theft
☐ Criminal Activity
☐ Other (describe):</td></tr>
<tr><td rowspan="2">☐ HR/other oversight body for possible disciplinary action</td><td>Who was notified?</td><td>Date of notification:</td></tr>
<tr><td>Outcome:</td><td>Date carried out:</td></tr>
</table>

☐ **Other** (describe)**:**	Who was notified?	Date of notification:
	Reason for notification:	

Accounting of Disclosures

Does incident require entity to account for the disclosure?

☐ Yes (logged in accounting of disclosures log)

☐ No (not required to account for disclosure)

Additional Information

List additional information relevant to the incident:

What has been learned from the disclosure?

How can this be prevented from occurring in the future?

What actions were taken in response to this breach?

☐ Security and/or Privacy Safeguards ☐ Mitigation ☐ Sanctions ☐ Policies and Procedures

☐ Other (specify):

Recorded By:	Date: