**Incident and/or Breach Report Form**

|  |  |
| --- | --- |
| **Date of discovery:** | **Date and time of occurrence:** |
| **Location of incident:** | **Incident first reported to:** |
| **Persons involved:** *(Names, job titles, departments, phone numbers of the responsible staff)* | **Type of data involved:** |
| **Number of individuals affected:** *(Estimate if unsure)* | **Application or system involved:** |
| **Description of incident:** *(Explain the circumstances)* | |
| **Type of incident:**  ☐ Unauthorized access ☐ Written disclosure of PHI ☐ Verbal disclosure of PHI  ☐ Electronic disclosure of information ☐ Security breach of PHI (failure to secure or lost/stolen PHI)  ☐ Improper destruction/disposal of PHI ☐ Other: | |
| **Description of what steps were taken to contain or remediate the incident:** | |
| **Author of incident report:** | **Author’s contact information:** |
| **The rest of this form is to be completed by the Privacy Officer** | |
| **Was the PHI encrypted using a FIPS 140-2 certified method?**  ☐ Yes ☐ No ☐ Unknown ☐ Other: | |
| **Was the PHI actually acquired or viewed?**  ☐ Yes ☐ No ☐ Unknown ☐ Other: | |
| **Was there a disclosure of PHI that violated the HIPAA Privacy Rule?**  ☐ Yes ☐ No ☐ Yes, but one of the three exceptions applies\* | |
| ***If there was no disclosure or if one of the three exceptions applies\* then there is not a reportable breach.*** | |
| **Name of person who determined “no breach”:** | **Person’s contact information:** |
| **Privacy Rule violation:** *(A description of Privacy Rule violation and any internal policies that were violated)* | |
| **Describe the nature and extent of the PHI involved, including the types of identifiers:** | |
| **Describe the likelihood of re-identification back to a patient:** | |
| **Method of disclosure:**  ☐ Verbal disclosure ☐ View only ☐ Paper / Fax ☐ Electronic ☐ Other: | |
| **To whom was the PHI impermissibly used or disclosed?**  ☐ A workforce member for the organization ☐ News media  ☐ Another business associate (vendor or consultant) ☐ Unknown (data stored on a lost or stolen device)  ☐ Covered entity ☐ Member of the general public  ☐ Wrong payer (not the patient’s) ☐ Hacker  ☐ Non-covered entity ☐ Other: | |
| **Was the impermissible use or disclose of the PHI:**  ☐ Unintentional or accidental ☐ Intentional ☐ Other: | |
| **Description what steps were taken to contain or remediate the incident:** | |
| **Determine the extent to which the risk to the PHI has been mitigated:** | |
| **Describe what preventive measures need to be enacted:** *(i.e. additional training, change of policy, etc.)* | |
| **Mitigation steps complete?**  ☐ Yes ☐ No ☐ Other: | **Sanction action taken?**  ☐ Yes ☐ No ☐ Other: |
| **Follow-up disposition:** | |
| **Additional comments:** | |

\*The three exceptions that a disclosure of PHI is not considered a breach are:

1. Unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate
2. Inadvertent disclosure of protected health information from one person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate
3. Unauthorized disclosures in which an unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information