Breach Notification Risk Assessment

|  |
| --- |
| Incident Risk Evaluation |
| Reporter  |  |
| Date of Incident |  |
| Assessor |  |
| Summary of Incident |  |
| Was protected PHI impacted? |  |
| Describe the PHI involved, impacted |  |
| Was the PHI rendered unusable/unreadable to unauthorized individual?* No, PHI was secured. No breach reporting required. Describe the protection mechanism that was in place to make the PHI unusable
* Yes, the PHI was unsecured and was used/read. Breach reporting is required
 |  |

|  |
| --- |
| Breach Analysis |
| Was there an acquisition, access, use or disclosure of PHI by unauthorized person?Describe who acquired it, how it was accessed and what was disclosed |  |
| Could the PHI disclosure result in an adverse manner or to further the unauthorized person interest? |  |
| Has any mitigation steps been implemented? |  |
| Does your state laws require notification of a breach?Describe your state laws and document whether you’ve complied. |  |
| Address the federal HIPAA law:* Written Individual notice (first-class mail, e-mail) no later than 60 days of discovery
* Media notice if 500 or more residents are affected no later than 60 days of discovery
* Notice to the Secretary if 500 or more individuals are affected no later than 60 days of discovery
* Notice to the Covered entity or Business associate no later than 60 days from the discovery
 |  |