Privacy / Security BREACH INCIDENT REPORT

Person Completing Report:
Date of Report:
Date of Incident:
Report Delivered To/Date:
Case Number Assigned:

Under the final rule, **breach** is defined as "an acquisition, access, use, or disclosure of protected health information in a manner not permitted…[and] *is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised* [emphasis added]." According to HHS, "breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that PHI has been compromised."

☐ This is an incident concerning fewer than 500 records. Estimated number of records:
☐ This is an incident concerning 500 records or more. Estimated number of records:

What type of PHI was involved: ☐ Paper PHI ☐ Electronic PHI ☐ Sensitive PHI

RISK ASSESSMENT REVIEW

1) What was the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification: (Could this information be used by an unauthorized recipient to further his own interests? Could it be re-identified relatively easily? Would it facilitate Identity Theft (SSN, credit card #, etc.)?)

2) Who was unauthorized person who used the protected health information or to whom the disclosure was made: (Is the recipient already *obligated* to protect PHI? Is recipient trustworthy? Identification also helps as mitigation—the recipient is already on the radar if the data is later misused.)

3) Was the protected health information actually acquired or viewed: Recovery of a lost laptop with PHI would present *potential* compromise. If forensic analysis shows the laptop was not accessed since prior to its loss, there is no actual compromise. PHI faxed to an individual would present an *actual* compromise. If recipient claims "I didn't read it," the weight that is given in consideration will depend on the trustworthiness of the individual (#2).)

4) To what extent has the risk to the protected health information has been mitigated: Recipient returns document and states he did not view it. A letter of attestation and/or a Non-Disclosure Agreement may prove useful as mitigating factors. Encryption as mitigation—YES! Must meet encryption standards. There is no "encryption-equivalent" available for paper documents.

List any attachments: (copy of PHI data, letters, depositions, attestations)

Privacy / Security BREACH INCIDENT REPORT

Person Completing Report:
Date of Report:
Date of Incident:
Report Delivered To/Date:
Case Number Assigned:

RESOLUTION OF EVENT

I. Describe actions taken on Response:

II. Additional actions to be taken:

III. Remediation of this event:

IV. Steps taken to prevent reoccurrence (include re-education and documentation).

Final Breach Determination

☐ Reported to Patient. Date:
☐ To Be Reported to HHS. Date:
☐ Breach Plan Implemented. Breach Reporting Needs to be Completed By: Date
☐ Not a Reportable Breach. Brief Explanation:

Final Resolution Date:
Completed By:
Contact Information:
Reviewed By: