You discover a possible breach of a patient’s protected health information (PHI)

Are you a HIPAA Covered Entity?

Yes: HIPAA applies and you must follow the HIPAA breach notification rule (as well as any applicable state law that is more stringent than HIPAA).

No: HIPAA does not apply. Follow any applicable state breach notification rules.

Has a breach of PHI occurred?

Yes

Was the breach unintentional, inadvertent, or un-retainable?

Yes: No reporting is required. But follow the documentation requirements.

No: Was the PHI that was breached “unsecured”?

Yes, the PHI was unsecured.

1. You must provide notice to the affected individuals without unreasonable delay (and in no event more than 60 days after discovery of the breach).

2. You must enter the breach in a log of all breaches to be submitted annually to HHS in the manner specified on the HHS Web site http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

No, it was secured. No reporting is required, but follow the documentation requirements.

No

No: No reporting is required. But follow the documentation requirements.
Did the breach affect the PHI of more than 500 people?

Yes. You must notify HHS of the breach in the manner specified on the HHS Web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/b rinstruction.html/) without Unreasonable delay, but in no event more than 60 calendar days after discovery of the breach.

No. Then you have no further notification obligations beyond notifying the individual(s) and logging the breach for annual reporting to HHS.

Did the breach affect the PHI of 500 or more people living in a single state or jurisdiction?

Yes. Then you must notify prominent media outlets serving the affected state or jurisdiction without unreasonable delay (and in no event later than 60 days after discovery of the breach).

No. Then you have no further notification obligations beyond notifying the individuals and HHS.