# Lesson 9 | Breaches and Security Incidents

Updated 2020-09-12

## Breaches and Security Incidents

Data breaches and security incidents are often spoken of in the same context. While they are related, they are not the same. And the distinction between the two terms is very important in HIPAA.

- Security Incident is an event that puts corporate systems and data at risk. It is often, but not always, the result of not complying with security policies.
- A data breach is when covered information, under HIPAA it is PHI, is disclosed in an unauthorized manner or non-permissible way.

A security incident increases the risk of a data breach but it is not a data breach. An example might be a misconfigured server where a default account password might not have been changed. In order to determine if this incident resulted in a data breach, an investigation must be conducted to assess if the vulnerable server account was used to gain unauthorized access to data on the server or accessible from the server.

Every security incident and breach needs to be investigated, with the investigation and outcome well documented.

Under HIPAA, there are no reporting requirements for security incidents.

Under HIPAA, there are several reporting requirements for data breaches that covered entities must follow, listed below.

- Individuals. Individuals with data impacted by a data breach need to be notified within 60 days.
- Media. If more than 500 individuals are impacted by a breach, the media needs to be notified within 60 days.

- HHS. If more than 500 individuals are impacted by a breach, HHS needs to be notified within 60 days. If a breach impacts less than 500 individuals, HHS can be notified annually.

Business associates have slightly different reporting requirements than covered entities. Business associates are required to notify the covered entities they support within 60 days of a breach. Business associates should also assist covered entities in identifying the impacted individuals. The requirements of business associates are typically defined in a business associate agreement (BAA).

*Every security incident must be investigated and, if it is determined that a data breach has occurred, the proper notifications should be done as fast as possible and no later than 60 days from the determination that a data breach occurred.*