COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 21, Number 7. July 08, 2021 Panel: Lay Groundwork for BA Breach Investigation, Notification

By Jane Anderson

Business associates (BAs) need to take specific steps to prepare in advance for security incidents and breaches so that they know how to respond—and meet key deadlines—in the event an incident occurs.

That's the word from three experts at a recent conference who addressed how BAs should lay the groundwork for their response in the event of a security incident,[1] regardless of whether it rises to the level of a breach of protected health information (PHI).

There are three types of situations that a BA might need to report to a covered entity (CE), explained Mark Joseph Fox, privacy and research compliance officer for the American College of Cardiology.

1. Impermissible use/disclosure, defined as any use or disclosure of PHI in a manner not permitted under the contract. There is no regulatory deadline for reporting an impermissible use or disclosure, but there may be contractual requirements contained in the business associate agreement (BAA).

2. Security incident, defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system not permitted under the contract. Again, there is no regulatory deadline for reporting a security incident, but there may be contractual requirements contained in the BAA.

3. Breach, defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the privacy rule that compromises the security or privacy of the PHI, except for good faith exceptions. The regulatory deadlines require the BA to report the breach no later than 60 calendar days from its discovery, but there may be additional contractual requirements contained in the BAA.