COSMOS
Navigate the Compliance Universe

Compliance Today - August 2021
Oh no! Breach by a business associate

By Mark J. Fox, CHC, CHPC, CHRC, and Thora Johnson

Mark J. Fox (mfox@acc.org) is Privacy and Research Compliance Officer at American College of Cardiology in Washington, DC. **Thora A. Johnson** (tajohnson@venable.com) is a Partner at Venable LLP in Baltimore, MD.

- linkedin.com/in/mark-fox-chc-chpc-chrc-5376559/
- linkedin.com/in/thora-johnson-390bba133/

Business associates perform functions on behalf of covered entities, such as health insurance issuers and most healthcare providers, that require the use and disclosure of protected health information (PHI).[1] The risk of a breach is real. A business associate that takes a proactive approach will allow both the business associate and the covered entity to respond more effectively and expeditiously under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule and other applicable federal and state law.

What must a business associate report to a covered entity

A business associate must report to its covered entities (1) security incidents of which it becomes aware, including a breach of unsecured PHI,[2] and (2) any impermissible use or disclosure of PHI of which it becomes aware, including breaches of unsecured PHI.[3] In order to effectively evaluate the need for notice from a business associate to a covered entity, it is important to understand the following definitions:

A "security incident" is "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[4] An "information system" means "an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

An impermissible use or disclosure of PHI is any use or disclosure of PHI that is not permitted by the agreement with the respective covered entity (otherwise known as a business associate agreement).[5]

A breach of unsecured PHI is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted" by the privacy rule that compromises the security or privacy of the PHI.[6] PHI is deemed to be unsecured PHI when it is "not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by" the secretary of the U.S. Department of Health & Human Services, such as encryption.

Importantly, though, the definition of "breach" has exceptions. Specifically:

1. The "unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority";

2. The inadvertent disclosure of PHI "by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates"; and

3. When the covered entity or business associate has "a good faith belief that an unauthorized person to whom the [impermissible] disclosure was made would not reasonably have been able to retain such information."[7]

In both the first and second exclusion listed above, the information cannot be further used or disclosed in a manner not permitted by the HIPAA Privacy Rule.