2 Breach Notification

By John Falcetano, CHC-F, CCEP-F, CCEP-I, CHRC, CHPC

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17, 2009 as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5). On January 25, 2013, modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act were issued—commonly known as the Omnibus Rule.

Key Definitions

In order to understand the Breach Notification requirement, it is important to understand the following definitions:

Access. The ability or means necessary to read, write, modify, communicate, or otherwise use data/information.

Authorized Person. An individual authorized by the entity or the entity’s Business Associate to acquire, access, or use Protected Health Information (PHI) that is within the individual’s scope of employment.

Limited Data Set. PHI that excludes 16 specific identifiers as defined in the HIPAA Privacy Rule, but includes zip codes, geographical codes, dates of birth, other date information, and any other code.

Organized Health Care Arrangement. A clinically integrated care setting in which individuals typically receive health care from more than one provider.
Unauthorized. An impermissible use or disclosure of PHI under the HIPAA Privacy Rule (subpart E of 45 CFR part 164).

Unauthorized Access. The inappropriate viewing of a patient’s medical or financial information without a direct need for diagnosis, treatment, payment, or other lawful use.

Unsecured Protected Health Information. PHI that is not secured through the use of a technology or methodology (such as encryption or destruction of data) that renders PHI unusable, unreadable, or indecipherable to unauthorized persons.

Protected Health Information (PHI). Individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in any medium such as magnetic tape, disc, optical file; or (iii) transmitted or maintained in any other form or medium (including but not necessarily limited to paper, voice, Internet, or facsimile).

Workforce Member. Employees, volunteers, students, medical residents, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of the entity, whether or not they are paid by the entity (including medical residents).

Breach (as defined in the Final Rule). A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been
Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

Exceptions. There are three exceptions to the definition of “breach.” The first exception applies to 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 business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Unsecured Protected Health Information. Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology on the HHS Web site (i.e., destroyed or encrypted).