COSMOS
Navigate the Compliance Universe

# Health Care Privacy Compliance Handbook, 3rd Edition
# 2. Breach Notification

By John C. Falcetano, CCEP-F, CHPC, and Shawn DeGroot, CHC-F, CCEP, CHRC, CHPC[1]

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.[2] On January 25, 2013, modifications to the Health Insurance Portability and Accountability Act (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.[3]

## 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 that is within the individual's scope of employment.

**Breach (as defined in the Omnibus 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. Such an occurrence is *presumed* to be reportable—a **reportable 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. The "low probability of compromise" is based on a risk assessment of at least the following four factors:

- **Content** The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- **Person** The unauthorized person who used the protected health information or to whom the disclosure was made;
- **Access** Whether the protected health information was actually acquired or viewed; and
- **Mitigation** The extent to which the risk to the protected health information has been mitigated.[4]

The presumption that a breach is reportable means that it is the responsibility of the covered entity or business associate, as applicable, to prove that the breach was not reportable because there was a "low probability of compromise" based on the four-factor risk assessment.

**Business Associate.** Business associate means, with respect to a covered entity, a person, entity, or subcontractor who:

- On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or

activity regulated by HIPAA Administrative Simplification including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. § 3.20 , billing, benefit management, practice management, and repricing; or

- Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.[5]

**Covered Entity.** A covered entity is (1) a health plan, (2) a healthcare clearinghouse, or (3) a healthcare provider that transmits any health information in electronic form in connection with a transaction for which the Department of Health and Human Services (HHS) has adopted standards.

**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, business associate, or organized healthcare 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.

**Limited Data Set.** Protected health information 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 Healthcare Arrangement.** A clinically integrated care setting in which individuals typically receive healthcare from more than one provider.

**Protected Health Information.** 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).[6]

**Unauthorized.** An impermissible use or disclosure of protected health information under the HIPAA Privacy Rule.[7]

**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.** Protected health information that is not secured through the use of a technology or methodology (such as encryption or destruction of data) that renders protected health information unusable, unreadable, or indecipherable to unauthorized persons.

**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).

---