Insights

HIPAA Security...Integrity Matters

February 1, 2018

By: Stephanie T. Eckerle and Susan E. Ziel

The HIPAA Security Rule requires Covered Entities and their respective Business Associates to maintain certain Administrative, Physical and Technical safeguards to protect Electronic Protected Health Information ("e-PHI"). Specifically, these safeguards are designed to ensure the Confidentiality, Integrity and Availability of all e-PHI that is created, received, maintained or transmitted by the Covered Entity or its Business Associates.[1]

Whereas the Security Rule's Confidentiality requirements support those of the HIPAA Privacy Rule, the two additional goals -- Integrity and Availability -- are also equally important. According to the Security Rule, the term "Integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. The term "Availability" means that the e-PHI is accessible and usable on demand by an authorized person.[2]

HIPAA policies must specify the Administrative, Physical and Technical safeguards that have been adopted to safeguard the Integrity -- or the accuracy and completeness -- of a particular individual's e-PHI. At a minimum, these policies should incorporate the following:

1. A glossary of defined and capitalized terms that incorporates the definitions arising under HIPAA and any other more stringent requirements that hail from state law (e.g., Designated Record Set ("DRS"), e-PHI, Electronic Media, etc.) plus any Covered Entity-specific definitions which typically address, for example, such things as the "legal health record" which is different from the DRS and represents the official business record of the entity for evidentiary purposes;[3]

2. A provision that addresses the procedures for identifying and managing any erroneous or replaced e-PHI that has been relegated to an "obsolete" folder that technically remains a part of the legal health record;

3. A provision that incorporates the most stringent record retention requirements adopted by the covered entity, whether under HIPAA, state law or at the direction of the entity's legal counsel (e.g. legal hold) and/or professional liability carrier (e.g. litigation); and

4. A provision that addresses the procedures for identifying and managing the destruction of any data following the expiration of all mandated record retention requirements.

Adoption of these and other HIPAA policies safeguards not only the state of the Covered Entity's information systems but also the quality of those individuals who conduct patient care and related business operations on behalf of the Covered Entity, all in accordance with applicable requirements. If you have questions regarding HIPAA security, Business Associates, or any health care matter, please contact Susan E. Ziel, Stephanie T. Eckerle, or your regular Krieg DeVault attorney.

[1] 45 C.F.R. § 306(a).

[2] 45 C.F.R. § 164.304.

[3] The DRS includes all PHI whereas the legal health record typically only includes the PHI used to make Treatment decisions. For additional information, see AHIMA. "Fundamentals of the Legal Health Record and Designated Record Set." Journal of AHIMA 82, no.2 (February 2011): expanded online version.