HIPAA AND ATTORNEYS:

HOW IT APPLIES AND WHY YOU SHOULD CARE IN NEVADA

BY KELLY MCINTOSH, ESQ.

You've heard of HIPAA. You've seen headlines regarding data breaches at national retailers, pharmacies and insurers. You may have read reports of settlements for HIPAA breaches – a $4.8 million settlement (the largest to date) was announced by the U.S. Department of Health and Human Services (HHS) in May 2014. Perhaps you send, or your clients receive, documents titled "HIPAA Compliant Authorization." But have you considered how HIPAA applies to attorneys and what it means to be compliant? Understanding the scope of HIPAA and the requirements for compliance will help protect you and your clients from HIPAA violations.

HIPAA Basics

Generally, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), provides that a covered entity (and its business associates) may not use or disclose protected health information (PHI) regarding an individual without the individual's authorization, except as permitted by HIPAA. Covered entities include health plans, healthcare clearinghouses and healthcare providers who conduct electronic healthcare transactions. Business associates are persons or entities that create, receive, maintain or transmit PHI for covered entities, or whose services to a covered entity involve the use or disclosure of PHI. PHI is broadly defined to include information, including demographic information, about health status, provision of healthcare services or payment for healthcare services that identifies an individual or which could reasonably be used to identify an individual.

HIPAA permits certain disclosures of PHI, including (among others) those for treatment, payment, healthcare operations, public health activities and in the course of judicial or legal proceedings. As discussed below, although disclosures authorized by the individual are permitted, even an authorization must contain specific elements to meet the requirements of HIPAA.

Pursuant to HIPAA, HHS adopted standards for electronic healthcare transactions and the security and privacy of individually identifiable health information through two rules administered by the Office for Civil Rights (OCR) – the Privacy Rule[1] and Security Rule.[2] The Privacy Rule includes standards for covered entities and their business associates to conduct electronic healthcare transactions, protections for PHI and patient rights in regard to PHI. The Security Rule includes the administrative, physical and technical safeguards required to protect the confidentiality, integrity and availability of electronic PHI. Since the initial passage of HIPAA and adoption of the Security and Privacy Rules, additional modifications and rulemaking have strengthened the protections under HIPAA.

Most recently, the HIPAA Omnibus Rule,[3] published in January 2013, effective March 26, 2013, and requiring compliance with most provisions by September 23, 2013, significantly increased penalties associated with violations of HIPPA.

Are you a Business Associate?

Beyond the attorney-client relationship, relationships covered by HIPAA may occur in the course of a client representation. Attorneys may be business associates of covered-entity clients or may be subcontractors of business-associate clients. This occurs when PHI is created, received, maintained, or transmitted from or on behalf of a client that is a covered entity, business associate or subcontractor.

Clients likely to be covered entities include those in the healthcare industry, e.g. hospitals, physicians, health plans and pharmacies. Not always as obvious are clients who are business associates of covered entities or subcontractors of business associates. These clients are subject to HIPAA regulation because the services they provide to covered entities or business associates involve the use or disclosure of PHI. Clients in this category are wide-ranging and could include consultants, software vendors, document shredding or storage companies and accountants.

If you are a business associate or subcontractor of a business associate, HIPAA compliance is required. This includes protecting PHI pursuant to the Security and Privacy Rules, to the extent applicable, and entering into business-associate agreements. Business-associate agreements are required between covered entities and business associates and also between business associates and their subcontractors (and subcontractors' subcontractors throughout the chain of relationships where PHI is used or disclosed). The OCR has published sample business-associate agreement provisions available on its website.[4] Though not comprehensive for all arrangements, the sample provisions are a helpful resource for addressing the concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification and Enforcement Rules within business-associate agreements. Also keep in mind that if you are a business associate or subcontractor, you must enter into agreements with your subcontractors or service providers where PHI is used or disclosed – for instance with experts, consultants or shredding companies.

HIPAA Compliant Authorizations

The use of PHI is necessary or desired in many legal activities. The HIPAA Privacy Rule includes several methods for disclosure, either with or without the individual's permission. The use of court orders and subpoenas, among other methods for disclosure, are addressed in the Privacy Rule.[5] However, a covered entity is also permitted to release PHI pursuant to a proper authorization, which is often the most efficient method to obtain disclosure of PHI from a covered entity. The covered entity, not the person preparing an authorization, has the obligation to ensure compliance with HIPAA. However, if you prepare authorizations to send to covered entities for disclosure of medical records or other information containing PHI, it increases efficiency for all parties to ensure the following required elements are understood and included in your authorization:[6]

- **Information**: A description of the information to be disclosed, identifying the information in a specific and meaningful fashion.
- **Disclosing Entity**: The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- **Receiving Party**: The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- **Purpose**: A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- **Right to Revoke**: A statement of the individual's right to revoke the authorization in writing, how to revoke the authorization and any exceptions to the right to revoke.

continued on page 17

HIPAA AND ATTORNEYS

continued from page 15

- **No Conditions**: A statement that the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether or not the individual signs the authorization, unless an exception applies.[7]
- **Potential for Redisclosure**: A statement about the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected.
- **Plain Language**: The authorization is written in plain language.
- **Expiration Date**: An expiration date (e.g., on a specific date or after an amount of time, such as "2 years") or an expiration event that relates to the individual or the purpose of the use or disclosure.
- **Signature**: The signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
- **Copy to Individual**: If a covered entity seeks an authorization from an individual for use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

State Preemption

Another important consideration is to remember that HIPAA preempts state law only to a limited extent. Where state privacy law is more stringent than HIPAA, state law applies. In Nevada law, NRS Chapter 629 addresses healthcare record retention, disclosure and inspection rights, including provisions specific to genetic information. NRS 52.320 *et seq.* addresses medical records in discovery proceedings. Analysis of the interplay of state privacy laws and HIPAA is an important activity dependent on the circumstances involved in a matter.

If you use, receive, request or otherwise encounter individually identifiable health information in your legal practice, it is important to consider how HIPAA may apply to avoid penalties or other consequences for you and your clients. ■

1 45 CFR § 164.500 *et seq.*
2 45 CFR § 164.300 *et seq.*
3 The Omnibus Rule incorporates into the HIPAA rules provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009.
4 Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
5 *See* 45 CFR § 164.512(e).
6 This list is based on the requirements found in 45 CFR § 164.508. Authorizations for specific purposes may require additional provisions. The Privacy Rule requires additional provisions for authorizations for research-related purposes, for the sale of PHI, and for marketing purposes involving financial remuneration. The requirements for written consents involving the disclosure of alcohol or substance abuse records are found in 42 CFR § 2.31.
7 45 CFR § 508(b)(4) includes exceptions where treatment, enrollment, or eligibility may be conditioned on provision of an authorization. If an exception applies, the authorization must include the consequences to the individual of a refusal to sign the authorization.

KELLY MCINTOSH is an attorney in the corporate group of Holland & Hart LLP. Her practice is focused largely in the areas of transactional, regulatory and administrative healthcare matters. McIntosh is based in Reno, but represents clients in the healthcare industry throughout the state.