HIPAA 101:

by Robyn Smith Ellis

Five Key Concepts Every Virginia Litigator Should Know

For attorneys practicing health law, consulting the Privacy Standards[1] of the Health Insurance Portability and Accountability Act (HIPAA) is almost an everyday event. Since these extensive and complicated rules were published in December of 2000, we have been advising health care providers and health plans ("covered entities"[2] under HIPAA) on the steps they should take to become compliant. For other attorneys, however, HIPAA has become a roadblock to patient information that used to be much more accessible.

HIPAA limits the use or disclosure of "protected health information"[3] or "PHI." PHI includes categories that are not generally thought of as medical information, such as names, addresses and Social Security numbers. Generally, PHI can be used or disclosed without patient authorization only for treatment, payment or health-care operations,[4] or for certain public purposes-such as health oversight activities and law enforcement.[5]

Prior to the implementation of HIPAA, the privacy of medical information in Virginia was governed only by the Virginia Patient Health Records Privacy Act.[6] HIPAA expressly supersedes any *contrary* provision of Virginia law unless Virginia law is more stringent (more protective of patient privacy rights than HIPAA.[7])

You May Be a "Business Associate"

Attorneys who represent covered entities have probably already been asked to sign business associate contracts.[8] A business associate is anyone who performs business functions on behalf of a covered entity which involve the use or disclosure of PHI.[9] A person who performs legal services for a covered entity and who receives PHI is a business associate.[10] HIPAA allows covered entities to disclose PHI to a business associate as long as the business associate gives "satisfactory assurances" that it will appropriately safeguard the information.[11] The satisfactory assurances must be documented in a written contract.[12]

If you are asked to sign a business associate contract, you should first consider whether your client is actually a covered entity. Although health plans are covered entities under HIPAA, not all plans that provide coverage for health care are covered. Accident and disability income insurance, supplements to liability insurance, liability insurance (including general liability and automobile liability), automobile medical payment insurance and workers' compensation coverage are not covered under HIPAA.[13] No business associate con-

tract is required when your representation involves only these types of coverage.

Where a business associate contract is required between a covered entity and its attorney, HIPAA proscribes certain elements of the contract.[14] In such a contract, a business associate agrees to comply with HIPAA.[15] A contract must establish the permitted and required uses and disclosures of PHI by the business associate.[16] The contract must also authorize termination of the contract by the covered entity if it determines that the business associate has violated a material term of the contract.[17] The contract must provide that the business associate will:

- Report any improper use or disclosure of PHI of which it becomes aware;
- Ensure that any agents, to whom it provides PHI, including subcontractors, agree to the same restrictions and conditions that apply to the business associate;[18]
- Give individuals access to their PHI;
- Make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services (HHS) for purposes of determining the covered entity's compliance with HIPAA; and
- At termination of the contract, if feasible, return or destroy all PHI that the business associate still maintains in any form and retain no copies of such information.[19]

Some covered entities want access to a business associate's premises as well as its internal practices, books and records regarding the use and disclosure of PHI.[20] HIPAA regulations require covered entities to take action if they know of a pattern or practice of a material violation of the regulations by their business associates.[21] Covered entities, however, have no duty to monitor the activities of their business associates.[22] Arguably, oversight rights such as the right to examine business associate premises and practices could be viewed as a self-imposed duty to monitor activities. For this reason, some health lawyers discourage their covered entity clients from including such provisions in their business associate contracts.

Because HIPAA governs the covered entity and not the business associate, attorneys as business associates are not subject to civil monetary penalties for a breach of the business associate contract.[23] HIPAA's criminal penalties may apply to anyone, however, who knowingly and in violation of HIPAA obtains an individual's PHI or discloses PHI to another person.[24] Penalties include significant monetary fines as well as imprisonment.[25]

Allowing Expert Witnesses To Review Medical Records Is Not As Simple As It Used To Be

HIPAA has created some impediments in allowing expert witnesses to review medical records. Business associate contracts must state that business associates will ensure that their agents agree to the same restrictions and conditions that apply to the business associate.[26] Must attorneys ask expert witnesses to agree to the same restrictions and conditions set forth in the business associate contract with their covered clients?

HHS has clarified that only those agents to whom a business associate delegates a function, activity or service that is within its business associate contract must agree to abide by the restrictions and conditions in the business associate contract.[27] Where a covered entity contracts with a lawyer and the lawyer discloses PHI to an expert witness in preparation for litigation, the lawyer has no responsibility regarding the uses or disclosures by the expert witness. The witness is not undertaking the functions, activities or services that the lawyer has agreed to perform.[28]

Although HHS believes that a lawyer has no responsibility related to uses and disclosures of an expert witness, it has not addressed whether the covered entity would have such responsibility. The cautious covered entity will require all expert witnesses to also sign a business associate agreement. If the expert witness is not a subcontractor or agent of the attorney, then HHS would likely consider the witness to be a business associate of the covered entity.[29]

Another option is to treat the expert witness as if he or she is an agent of the business associate attorney. The expert witness is not a business associate of the covered entity because the covered entity does not hire or work with the expert or release information to him or her. Therefore, the business associate attorney could release information to the expert as long as the expert agrees to the same restrictions and conditions that apply to the business associate with respect to PHI.[30] As long as the witness has either a business associate contract with the covered entity or agrees to the restrictions in the attorney's business associate contract, the confidentiality of PHI is protected.

Virginia Has New Requirements for Subpoenas *Duces Tecum* of Medical Records

HIPAA permits disclosures for judicial and administrative proceedings under certain circumstances.[31] A health-care provider may disclose medical records in response to an order of a court or administrative tribunal, provided that the covered entity discloses only the information expressly authorized by such order.[32] A health-care provider may also disclose records in response to a subpoena, discovery request or other lawful process that is not accompanied by an order if the covered entity receives "satisfactory assurances" from the party seeking the information that reasonable efforts have been made either to ensure that the individual has been given notice of the request or to secure a qualified protective order.[33]

A health-care provider receives "satisfactory assurances" that an individual has been notified of the request if it receives a written statement and documentation demonstrating that the party requesting such information has made a good-faith attempt to provide written notice to the individual; that the notice includes sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and that the time for the individual to raise

objections to the court or administrative tribunal has elapsed.[34] Further, the provider must ensure that either no objections were filed or all objections filed by the individual have been resolved by the court or the administrative tribunal.[35]

A provider receives "satisfactory assurances" that a protective order has been secured if the provider obtains a written statement and documentation demonstrating that the parties have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.[36]

Virginia has modified the rules regarding subpoenas *duces tecum* for medical records to comply with HIPAA's subpoena requirements.[37] The revised *Code of Virginia* § 32.1-127.1:03 includes a requirement that the return date on a subpoena *duces tecum* be set no earlier than fifteen days from the date of the subpoena and makes changes to the required notices to patients and providers.[38] One new requirement states that when no motion to quash has been filed within fifteen days of the subpoena, the party who issued the subpoena has the duty to certify to the health care provider that the time for filing a motion to quash has elapsed and no motion was filed.[39] Where a motion to quash has been filed, the attorney issuing the subpoena must certify in writing to the health care provider that all motions to quash have been resolved and the effect of those resolutions.[40] These changes in the law have been made to provide some consistency between HIPAA and the Virginia subpoena rules. Prior to issuing a subpoena *duces tecum* for medical records, attorneys should refer to revised § 32.1-127.1:03(H).

Workers' Compensation Cases Are Treated Differently

Under HIPAA, health care providers may disclose PHI to comply with workers' compensation laws and other statutory programs that provide benefits for work-related injuries or illness without regard to fault.[41] Virginia law requires health-care providers attending an injured employee to furnish a copy of any medical report to the employee, employer or insurer upon request.[42] Therefore, disclosure of records requested by subpoena in a workers' compensation case is necessary to comply with workers' compensation law and is not governed by HIPAA. The Virginia Workers' Compensation Commission's position is that HIPAA does not apply to workers' compensation.[43]

Another HIPAA requirement that does not appear to apply in the context of workers' compensation cases is the "minimum necessary" requirement. Generally, when health care providers release medical records, they must restrict the release of information to the "minimum necessary to accomplish the intended purpose of the use, disclosure or request."[44] However, where information must be released in order to comply with state law, no minimum necessary determination is required.[45] Because Virginia law requires providers to furnish medical reports to employers or workers' compensation insurers upon request, the provider arguably is not bound by the "minimum necessary" requirement.

Your Medical Records Release Authorizations Must Comply with HIPAA

Pre-HIPAA medical records releases are very unlikely to comply with HIPAA. HIPAA requires that authorizations be in "plain language"[46] and contain at least the following elements:[47]

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- The name or other specific identification of the person, or class of persons, authorized to make the requested use or disclosure.
- The name or other specific identification of the person, or class of persons, to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure.
- An expiration date or an expiration event.
- Signature of the individual and date.

The authorization must also contain statements adequate to place the individual on notice of all of the following:[48]

- The individual's right to revoke the authorization in writing, and either (1) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (2) to the extent that this information is included in the covered entity's notice of privacy practices, a reference to this notice;
- The ability or inability of the health care provider to condition treatment on the authorization by stating either (1) the covered entity may not condition treatment on whether the individual signs the authorization when the HIPAA prohibition on conditioning of authorizations applies;[49] or (2) the consequences to the individual of a refusal to sign the authorization when the covered entity can condition treatment on failure to obtain such authorization;[50] and
- The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by HIPAA.

It is possible for an attorney to draft his own compliance authorization, but the easiest method of accessing your client's medical information, depending on the number of treating providers involved, may be to have your client sign the HIPAA authorization that each provider has already prepared. In the alternative, your client is able to receive the information directly without signing an authorization.

Conclusion

Virginia litigators who deal with medical information in their cases should comprehend, at a minimum, these HIPAA concepts. Understanding, for example, why clients who are covered by HIPAA have asked you to sign a cumbersome business associate agreement or why covered health-care providers are requiring patients to sign extensive medical releases before giving their attorneys those records

HIPAA regulations require covered entities to take action if they know of a pattern or practice of a material violation of the regulations by their business associates.

will hopefully ease some frustrations with these covered entities who seem to be making everything so complicated now. All attorneys should sympathize with healthcare providers and health plans and understand that HIPAA is a complex set of rules that most providers and plans would prefer not to follow. ⚖

Endnotes:

1 65 FR 82462 (Dec. 28, 2000), later amended at 67 FR 53266 (Aug. 14, 2002) and 68 FR 8381 (Feb. 20, 2003); 45 *CFR* Part 160 and Part 164, Subparts A and E.

2 45 *CFR* § 160.102

3 45 *CFR* § 160.501

4 45 *CFR* § 164.502(a)(1)(ii)

5 45 *CFR* § 164.512

6 *Virginia Code* § 32.1-127.1:03

7 42 USC § 1320d-7, 45 USC 160.203(b)

8 45 *CFR* § 164.504(e)(1).

9 45 *CFR* § 160.103

10 45 *CFR* § 160.103

11 45 *CFR* § 164.502(e)(1)(i)

12 45 *CFR* § 164.502(e)(2)

13 *See* definition of "health plan" at 45 *CFR* § 164.103, which excludes those items listed in 42 USC § 300gg-91(c)(1).

14 45 *CFR* § 164.504(e)(2)

15 The Department of Health and Human Services has no direct regulatory authority over business associates.

16 45 *CFR* § 164.504(e)(2)(i)

17 45 *CFR* § 164.504(e)(2)(iii)

18 This requirement is discussed further below in Section II.

19 45 *CFR* § 164.504(e)(ii)(A)-(I)

20 HIPAA only requires such things to be available to the Secretary of HHS. 45 *CFR* § 164.504(e)(ii)(H).

21 45 *CFR* § 164.504(e)

22 *See* FAQ, "Is a covered entity liable for, or required to monitor, the activities of its business associates?" http://answers.hhs.gov/

23 *See* FAQ, "Can the Secretary sanction a business associate for HIPAA Privacy Rule violations?" http://answers.hhs.gov/

24 42 USC § 1320d-6

25 *Id*.

26 45 *CFR* § 164.504(e)(2)(ii)(D)

27 65 FR 82506 (Dec. 28, 2000).

28 *Id*.

29 45 *CFR* § 160.103

30 45 *CFR* § 164.504(e)(2)(ii)(D)

31 45 *CFR* § 164.512(e)

32 *Id*.

33 *Id*.

34 *Id*.

35 *Id*.

36 *Id*.

37 Virginia House Bill 2463, 2003 Session; *Virginia Code* § 32.1-127.1:03.

38 *Virginia Code* § 32.1-127.1:03(H)(1) & (2).

39 32.1-127.1:03(H)(5)

40 32.1-127.1:03(H)(8)

41 45 CFR § 164.512(l)

42 *Virginia Code* § 65.2-604(A).

43 http://www.vwc.state.va.us/printable/hippa_privacy.doc, April 1, 2004

44 45 *CFR* 164.502(b).

45 45 *CFR* 164.512(a); 45 CFR 164.502(b)

46 45 *CFR* § 164.508(c)(3)

47 45 *CFR* § 164.508(c)(1)

48 45 *CFR* § 164.508(c)(2)

49 *See* 45 *CFR* § 164.508(b)(4)

50 *See id*.

Robyn Smith Ellis is an associate at Gentry Locke Rakes & Moore LLP in Roanoke. She focuses her practice in the areas of health-care law, employment law and estate planning and administration. She received her undergraduate degree from the University of Virginia and her law degree from the Marshall-Wythe School of Law of the College of William and Mary.