What Compliance Involves

Part 1 of 3

By Mary R. Daulong, PT, CHC, CHP
With Alicia Nevins Mahoney and Teresa Daulong

WHILE WE TYPICALLY FOCUS ON ISSUES RELATED to payment compliance, it is paramount that we understand what other federal regulations apply to us as practitioners in the health care business arena. Understanding the laws, performing associated risk assessments, developing policies and procedures, educating the workforce, monitoring compliance with the statute, and enforcing their requirements is the only way we can mitigate our risk and safeguard our practices.

This article will focus on the Health Insurance Portability and Accountability Act (HIPAA), based on HIPAA questions posed or violations noted from 2016–2017.

Question: I have a cash-based practice, so I don't bill insurance companies. Am I required to comply with HIPAA?
Answer: Filing a claim is only one of the standard transactions that are tied to HIPAA's determination of a covered entity. There are three elements that must be considered when assessing whether an individual or entity is a covered entity:

1. Are you a health care provider? Per HIPAA: Heath care provider is any person or organization that furnishes, bills, or is paid for health care in the normal course of business. Health care is defined very broadly as care, services, or supplies related to the health of an individual.
2. Do you transmit information electronically? If a computer was used to communicate (send, receive, or store), it meets the definition of transmitting information electronically. Electronically includes but is not limited to:
   - Internet
   - Extranet
   - Leased lines

- Dial-up lines
- Private networks
- Magnetic tape
- Disks
- USB drives
- Faxes sent or received via a computer; stand-alone fax machines are not considered electronic transmissions and neither are telephonic voice messages

3. Do you transmit any of the following standard transactions?
    - Claims and encounter information
    - Payment and remittance advice
    - Claims status
    - Eligibility
    - Enrollment and disenrollment
    - Referrals and authorizations
    - Coordination of benefits
    - Premium payments
    - First report of injury
    - Health claims attachments

Remember, if you answered yes to any of the three elements you may be considered a covered entity and therefore must comply with HIPAA.

Question: Who should initiate a Business Associate (BA) Agreement (BAA)? The Business Associate or the Covered Entity (CE)?
Answer: Covered Entities should initiate the BA agreement so that they are certain that all the requirements set forth by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Omnibus Rule are in the agreement. They are[1]:

- Allowed and required disclosures: what the BA can and can't do with the data, as well as what they're required to do with the data
- Reference to "downstream" subcontractors: Ensure that they are responsible to abide by same terms as the BAs.
- BA's responsibility to safeguard the data: with reference to the security rule
- Reporting obligations: BA's methods for notifying CE of impermissible disclosures, which could include a data breach incident
- Satisfactory assurance from the Business Associate that it complies with HIPAA Security and Privacy as it pertains to BAs
- Termination clause: CE can terminate contract for violation of terms, and in the event of termination, the BA must return or destroy the data.

In addition to these provisions, there are optional elements such as:

- Liability and indemnification clauses for both parties
- Monitoring and auditing rights of the Covered Entity

Question: I have a Privacy Notice available for patients to read if they wish to; most don't. I heard that I must provide each patient with the notice before I ask them to sign our Acknowledgment of Receipt, is this true?
Answer: Yes, you are required to offer the Privacy Notice to all new patients and any active patients if the Notice is modified in any way. In addition to offering the notice, you must post it or have it readily available in the reception or common space so that a patient, visitor, etc., can access it without requesting it from you. Don't forget that you must also post the notice on your website, if you have one.

Your patients should never be asked to sign the Acknowledgment of Receipt without first having access to the Privacy Notice.

Question: I just started a private practice in Minnesota. Will I have to change my Privacy Notice or can I use the one I have from Wisconsin?
Answer: Your Privacy Notice should be reviewed to determine if state law is more stringent than HIPAA, and if it is you must follow the one that gives the patient the most protection and rights. In your case, Minnesota's Privacy Laws are more stringent than HIPAA's and you should adjust your Privacy Notice to comply with it.

Question: How do I prove that *all* my staff need access to both protected health information (PHI) and electronic protected health information (ePHI)?
Answer: HIPAA requires covered entities to develop role-based access policies and procedures to validate that access to PHI and ePHI is based on the individual's need to access either or both to do their jobs. If this is the case, you may list all of them with full access to PHI and ePHI.

Question: Do I need to obtain a patient's authorization if I receive a subpoena?
Answer: A HIPAA-covered entity may share a patient's protected health information if it has a court order. This includes the order of an administrative tribunal (court seal is a good way of determining if the subpoena was issued by the court/judge).

If the issuer is not a judge, then the covered entity must make certain that they only disclose the information specifically described in the order and that the Privacy Rule's notification requirements are met prior to responding to a subpoena and that the covered entity receives evidence that there were reasonable efforts to:

- Obtain a HIPAA-compliant authorization from the patient

- Notify the person who is the subject of the information about the request, so the person has a chance to object to the disclosure, or
- Seek a qualified protective order for the information from the court.

Question: What are the Patient Rights that came about via HITECH and the Omnibus Rule?
Answer: The newest Patient Rights are in italics below. These rights must be included in your Privacy Notice.

- Access to PHI
- Amend PHI
- Request limited use or disclosure
- Request an accounting for some disclosures
- Request confidential communication of PHI
- *Be informed of breach of privacy*
- Make complaints about noncompliance
- Revoke authorization
- *Be notified of opt-out options for marketing, fundraising, and sale of PHI*
- *Restrict PHI from health plans*
- Receive a paper copy of the Privacy Notice

Question: What do I have to include in a Breach Notification?
Answer: When notifying a patient of a breach, include the following information:

- A description of the breach (what happened)
- A description of the types of information that were involved in the breach (what data was shared)
- The steps that the affected individual(s) should take to protect themselves from potential harm
- A brief description of what the covered entity (CE) is doing to
    - Investigate the breach
    - Mitigate the harm
    - Prevent further breaches
    - Provide contact information at no cost to the individual

Also remember that the breach must also be reported to the secretary of the US Department of Health and Human Services (HHS). Breaches over 500 individuals require additional reporting to media outlets and websites. Timelines for reporting breaches vary by state so be sure to check your local reporting requirements.

Question: What is a Security Risk Analysis (SRA)?
Answer: The SRA is the first requirement under the Security Rule and, after initial completion, is required to be updated regularly (after a breach/incident, changes in infrastructure, or annually, etc.). It is an analysis of your practice focused on identifying issues, gaps, and vulnerabilities in the handling of ePHI. Two components, a review of the administrative infrastructure and scans for vulnerabilities in the IT infrastructure, make up the SRA. The intent is to protect the confidentiality, integrity, and availability of data by looking at the physical, technical, and administrative safeguards in place for ePHI.

The Office of the National Coordinator for Health IT (ONC) together with the Office for Civil Rights (OCR) and the Office of the General Council (OGC) have developed an SRA tool: www.healthit.gov/providers-professionals/security-risk-assessment-tool.

This tool is:

- Designed to assist providers as they perform a risk assessment.
- Designed for small- and medium-sized practices.
- Focused on the Security Rule only.

The tool is not all encompassing. You may have additional assessment needs regarding, but not limited to, the following areas:

- Privacy regulations (privacy official, notice of privacy practices [NPP], etc.)
- Encryption requirements (128/256-bit encryption, data at rest and in transmission)

Question: Do I have to encrypt my computers, emails, and text messages?
Answer: Yes, you must address Security Rule 164.312, which mandates encryption of data both at rest and in transmission. All data, including emails and text messages, that contain ePHI must be encrypted or otherwise addressed to meet the minimum encryption standards before transmission. The upside, however, is that stolen ePHI that is encrypted does not have to be reported (aka if you have an encrypted laptop or flash drive and it is stolen you do not have to report the ePHI as a security breach).

Question: Can my staff use personal devices (smartphone, iPad, etc.) for patient documentation?
Answer: Yes, your staff may use personal devices at work. However, you need to ensure that they also comply with all provisions under HIPAA, the Security Rule, and the HITECH Act. All the same rules apply as for your practice-owned computers, laptops, tablets, etc., including encryption, login monitoring, data backup, unique user identification, workstation security, and more. Additionally, you will need policies and procedures in place for personal device use.

REFERENCE

[1] *Abbreviated Summary from: securityMETRICS, Tod Ferran (CISSP, QSA).*