HIPAA Compliance from a Private Practice Purview

SWEEPING CHANGE CONTINUES to be the norm for health care regulations. Professionals in private practice play multiple roles within their businesses as they are responsible for policy creation, implementation, and management, as well as the day-to-day responsibilities of patient care. Registered dietitian nutritionists (RDNs) have access to assistance via resources provided by the Academy of Nutrition and Dietetics (Academy), particularly in terms of compliance with legislation collectively referred to as the HIPAA Omnibus Rule, which took effect September 23, 2013. Though the new rules are extremely broad in nature, and in some cases complex in detail, achieving compliance does not have to be burdensome, many RDNs agree.

Lucille Beseler, MS, RDN, LDN, CDE, an independent practitioner and member of the Nutrition Entrepreneurs dietetic practice group (DPG), said that despite the complexities, common sense remains the essence of the Health Insurance Portability and Accountability Act (HIPAA). "These requirements could be daunting to the private practice RDN that does not employ administrative staff, but then again all business operations can be difficult if you are going it alone," she stated, adding multiple resources exist to help practitioners achieve compliance.

In addition to resources provided via the Academy, information about HIPAA pertinent to RDNs is available online through the Academy's nonprofit associate, Healthcare Information Management and Systems Society. General information applicable to all health care providers is available through the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), as well as the American Medical Association. RDNs who operate their own practices can utilize these free resources when updating their own written policies and offer them as a reference to their employees.

*This article was written by **Brian Boyce,** an award-winning freelance writer in Terra Haute, IN.*

http://dx.doi.org/10.1016/j.jand.2014.05.016
Available online 19 July 2014

THE HIPAA OMNIBUS FINAL RULE

First enacted by Congress in 1996, HIPAA established standards and regulations to secure personal health data and protect insurance coverage during job changes, as well as to empower the federal government to intervene in issues of determined fraud and abuse. Components of the law included the Privacy Rule, Security Rule, and the Enforcement and Breach Notification Rule. Subsequent expansions in how health care professionals must safeguard Protected Health Information (PHI) have culminated in the Omnibus Final Rule.

"PHI is health information collected from an individual that is: (i) created or received by a CE (Covered Entity) or employer; and (ii) relates to past, present, or future physical or mental health condition of an individual, or payment for health care. Examples of PHI include a claim submitted to a health insurance company for payment or any part of a patient's medical record. It is important to remember that PHI is not just the entire medical record or claim; instead, it is any piece of information that identifies a patient tied to health care."[1]

As part of the ongoing shift toward managing health data electronically, the term ePHI refers to individual identifiable health information in an electronic form. The technology involved in storing or transmitting ePHI is thus subject to the same security requirements as that involving paper, from electronic health record (EHR) systems to flash drives and text messaging.

The Omnibus Final Rule serves as a revision of HIPAA, based on statutory changes under the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and the Genetic Information Nondiscrimination Act of 2008.[2]

Changes resulting from the Omnibus Final Rule have been termed sweeping in nature, not only for practitioners, but for those with whom the practitioner does work and their downstream vendors. Several Academy, federal, and other health care resources exist (Figure 1) to help answer specific questions about the impact on diverse areas from marketing and advertising to information technology systems. At one level, more responsibility is being placed on health care providers to hold their business associates accountable for patient privacy. Also, see Figure 2 for a list of key terms used in this article.

"In practice, all downstream vendors of a CE (Covered Entity) that handle PHI must now comply with HIPAA's BA (Business Associate) obligations. RDNs acting as CEs must enter a written agreement with their BAs, and BAs must enter written agreements with their sub-contractors to comply with the regulations."[1]

The new regulations further expand the scope of groups defined as BAs to include entities such as Patient Safety Organizations, health exchanges, and e-prescribing gateways.[2] This places the burden of compliance more directly on the BA to comply with HIPAA, as they too will now be accountable.[2] An example relevant to the RDN practice might be that of an independent billing company, which under the new law, is required to not only sign a BA with the RDN, but to do so with any of its own subcontractors who might have access to PHI.[2] The billing company would thus be responsible for ensuring that its own subcontractors comply with the law, thereby expanding the accountability.

The CE refers to three specific groups—health plans, health care clearing houses, and health care providers that transmit PHI electronically. RDNs that transmit health information electronically, regardless of practice size or setting, are therefore considered CEs. The BA is defined under the law as a person or entity that is not directly employed as

- The Academy of Nutrition and Dietetics website for sample Business Agreement provisions and other sample Health Insurance Portability and Accountability Act (HIPAA) compliance documents: www.eatright.org/Members/content.aspx?id=7511
- Reimbursement representatives of each state affiliate and dietetic practice group. Check the Academy's Leadership Directory, under Policy Initiatives and Advocacy Leaders, for contact information: http://www.eatright.org/members/leadershipdirectory.aspx
- The American Medical Association's HIPAA Privacy and Security Toolkit: Helping Your Practice Meet New Compliance Requirements: www.ama-assn.org/go/hipaa
- The US Department of Health and Human Services (HHS) website: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
- The HHS Office for Civil Rights (OCR) has launched three training modules to educate health care providers about compliance with new HIPAA regulations:
  - (A) Patient Privacy: A Guide for Providers www.medscape.org/viewarticle/781892?src=ocr2
  - (B) HIPAA and You: Building a Culture of Compliance www.medscape.org/viewarticle/762170?src=ocr2
  - (C) Examining Compliance with the HIPAA Privacy Rule www.medscape.org/viewarticle/763251?src=ocr2

Figure 1. Registered dietitian nutritionist resources for maintaining Health Insurance Portability and Accountability Act (HIPAA) compliance.

part of the CE's workforce, but still generates, maintains, or transmits PHI, whether they or the CE actually view it or not. The American Medical Association explains that BAs include, but are not limited to, any individual or group that processes claims or administrative data, or performs data analysis, quality assurance, billing, legal, or accounting work that might involve PHI. [3] Attorneys and certified professional accountants, consultants, and essentially any outside group that handles PHI would be included.

The written agreement into which these CE must enter is referred to as the Business Associate Agreement (BAA) under the law. This contains the list of contractual requirements and establishment of permitted uses and disclosures of PHI. The BAA must provide that the BA will neither use nor further disclose the PHI in any manner other than that which is permitted by the law.

In the case of private practice RDNs, this would include any billing company or outside vendor contracted to schedule appointments, perform data analysis, or engage in any other activity that might bring them into contact with PHI. RDNs need to ensure their protocols are in sync with those of referring hospitals and physicians as well. However, the RDN as a CE would not necessarily have to enter into an agreement with vendors used by their own BAs, as that would now be the responsibility of the BA.

"The Omnibus Rule also requires BAs to enter into a BAA with all subcontractors. The CE is not required to enter into a BAA with the subcontractor of a BA."[1]

Documentation of these agreements places a shared burden on all involved as, under the new rules, a BA is directly liable and potentially subject to both civil and criminal penalties for making unauthorized uses or disclosures of PHI.[1] In turn, the BA is responsible for actions taken by their own subcontractors. The CE is thus responsible for ensuring that the BA is operating in a lawful manner.[1] The CE could be held accountable for failing to take reasonable steps to prevent breaches if a pattern of abuse were to occur.[1]

The HIPAA Omnibus rule establishes a four-tiered system of violations.[3] The lowest level of violations, where practitioners were determined to not have known about the breach, contain penalties ranging from $100 to $50,000. Cases where practitioners had a

- **Covered Entity (CE):** Health plans, health care clearing houses, and qualified health care providers who practice in connection with transactions for which the US Department of Health and Human Services has adopted standards under the Health Insurance Portability and Accountability Act.
- **Protected Health Information (PHI):** All individually identifiable health information held or transmitted by a Covered Entity or its Business Associate in any form or media—electronic, paper, or oral.
- **Business Associate (BA):** Any person or entity performing activities in conjunction with, or on behalf of, a Covered Entity. A member of the Covered Entity's employed workforce is not a Business Associate. Examples of Business Associates include: a third-party administrator that assists a health plan with claims processing; a Certified Public Accountant who services a health care provider and has access to Protected Health Information; an attorney whose legal services to a health plan involve access to Protected Health; an independent medical transcriptionist who provides services to an RDN.
- **Business Associate Agreement:** A Covered Entity's contract or other written arrangement with its Business Associate which describes the permitted use of Protected Health Information by said Business Associate; provides that the Business Associate will not use or further disclose the Protected Health Information other than as permitted or required by the contract or as required by law; and require the Business Associate use appropriate safeguards to prevent a use or disclosure of the Protected Health Information in any manner other than is provided for in the Business Associate Agreement.

Figure 2. Key HIPAA (Health Insurance Portability and Accountability Act) terms used in this article.

reasonable cause to know of the problem carry penalties ranging from $1,000 to $50,000. Cases involving willful neglect but containing correction can carry penalties ranging between $10,000 and $50,000, compared to those where willful neglect was left uncorrected, which can be up to $50,000. Violations of the same requirement or prohibition for any of the categories are limited to $1.5 million for any calendar year.[3,4]

Practitioners are also under new obligations regarding the Breach Notification Rule, which had heretofore been limited to notifying patients if breaches of security involving their information had been occurring for some time.[3,4] The new rules expand this obligation, and now breaches are presumed reportable unless a risk analysis comprised of four factors deems there to have been a "low probability of PHI compromise."[3] The four factors include:

- the nature and extent of the PHI involved;
- the person who obtained the unauthorized access and whether or not they had an obligation under HIPAA to protect confidentiality;
- whether or not the PHI was actually acquired or accessed; and
- the extent to which the risk has been mitigated via a signed confidentiality agreement.

Meanwhile, patients are afforded more freedom over their own PHI under the new rules, to include their ability to restrict the disclosure of PHI to health plans if the services are paid for out-of-pocket. Individual patients are also afforded the right to obtain an electronic copy of their PHI which is maintained in any electronic system, within 30 days of requesting it, with one 30-day extension permitted,[3,4] thus eliminating the prior 60-day time frame for records maintained offsite. Patients must also be afforded access to the EHR and other electronic records in the electronic form and format requested by the individual if the records are "readily reproducible" in that format.[3] If they are not, a mutually agreed upon electronic format must be used, as hard copies are permitted only when the individual rejects all other readily reproducible electronic options.[3] The new rule also modifies the costs that may be charged to the individual for copies of their PHI to include labor and supply costs.[3]

The new law also expands its scope of coverage regarding the potential sale or utilization of PHI by CEs in marketing activities, with patient authorization now required for an expanded list of such activities. The rule also further limits the circumstances of when practitioners may provide marketing communications to their patients in the absence of the patient's written authorization.

As a general rule, the only time a CE may tell a patient about a third-party's product or service without the patient's written authorization is when:

- the CE receives no compensation for the communication;
- the communication is face-to-face;
- the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit);
- the communication involves general health promotion, rather than the promotion of a specific product or service; or
- the communication involves government or government-sponsored programs.

The CE is still permitted to give patients promotional gifts of a nominal value.[3]

Although the law itself applies equally to all qualifying health care providers, those in private practice might bear more responsibility for overseeing the changes than those working in a large institution. As a CE, RDNs in private practice have long been required to maintain and distribute their own Notice of Privacy Practices (NPP) to all patients, while their colleagues employed by institutions fell under the auspices of that organization's documents and policies. In addition, RDNs in private practice, much like medical doctors and other professionals in private practice, are largely responsible for educating themselves on the changes contained within the law.

In addition to the Omnibus Rule's revamping of a BA's definition, professionals in the medical field have also pointed to its modification of the term "breach."[3] Formerly, a breach of HIPAA was defined as an event that

compromised the security or privacy of the PHI such that the use or disclosure posed a significant risk of financial, reputational, or other harm to the affected individual.[3] Under the Omnibus Rule, the definition of breach has been expanded to include even just the risk of impermissible use or disclosure of PHI. The loss or theft of a laptop computer containing patient records that are not password protected or encrypted could therefore, potentially, be reported to a HIPAA officer.[3] Meanwhile, some concern has been expressed that HIPAA audits might occur with greater frequency as a result of the new law.[3] HHS has established a free, online guidance library with documents and explanations available at http://www.hhs.gov/ohrp/policy, which includes a section on investigations.

PRIVATE PRACTITIONERS KNOW HOW TO ADJUST

Carol Plotkin, MS, RDN, CDN, ACSM, owner of On Nutrition in Rochester, NY, agreed that the cheery tenacity of an entrepreneur is one well-equipped to handle change.

"The DPG offers a lot of support for private practice," she said of the Nutrition Entrepreneurs DPG, for whom she has served as a past private practice chair, as well as lead on the topic of reimbursement. As a private practitioner who coaches others in private practice, she emphasized the importance of staying abreast of changes in regulations.

And while those in private practice do bear the primary responsibility for achieving compliance, in some cases having a small operation makes it easier, she said. RDNs in large institutions might not have to handle the actual placement of an NPP on the organizational website and other such details, but in the case of her practice, she can control much of the risk for a potential HIPAA breach herself. Her practice includes just one other RDN. Her primary vendors are limited to an attorney and accountant, both of whom she works with directly and can monitor their access to PHI as well their compliance with the BAA. The EHR she uses is HIPAA-compliant and the company she uses keeps abreast of the changing regulations, and she keeps up to date with their activities, in addition to those of the health insurance payors with whom she works. Both the health insurance companies and EHR providers send routine updates concerning changes in regulations, including those pertaining to privacy and HIPAA. In addition to maintaining her own processes and written policies in place with partners and vendors, Plotkin said she's long avoided transmitting patient information via e-mail, and respect for patient privacy should prove the rule and guide for conducting business, regardless of the technological platform used.

Many RDNs are probably unaware of all the specifics involved in the Omnibus Rule, she said, adding that the Academy's numerous resources on the topic, coupled with regular interaction with one's DPG, help offset the need to hire extra staff to produce documents that are already available for download. And while the widespread changes sweeping through the field of health care do indeed bring more regulations, they are also raising public awareness and reimbursement opportunities for nutrition-related services. The emphasis on wellness and access to nutritional services is a big plus, she said, pointing out her role in the DPG is to help members learn how to bill third-party payors and insurance companies. Compliance with insurance and government regulations, including those involving HIPAA, open the door to a lot more revenue opportunities in the long run, she said.

RESOURCES AVAILABLE FOR EDUCATION AND COMPLIANCE

Thorough compliance with the regulations would include the conducting and documentation of a risk analysis, defined by HHS as an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI in a practice; a review of the practice's policies and procedures for when PHI is potentially compromised; ensuring that the PHI contained within a practice is encrypted so it cannot be lost or stolen; modification of a practice's EHR system so as to flag information a patient does not want shared; having the ability to send patients their health information in a completely secured format; and reviewing contracts with applicable vendors to ensure HIPAA compliance on their end and updating the practice's NPP.[5]

Achieving and maintaining compliance is an ongoing process and one that must be tailored to the unique needs of each organization. The OCR's Final Guidance on Risk Analysis offers an outline for the process, including the role of ePHI, which is any patient health information transmitted electronically, to include that which involves potentially unsecure wireless networks. Available online, the guide is among the tools offered by HHS to assist with compliance.

"The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements. An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment."[6]

The Security Management Process standard in the Security Rules requires organizations to implement policies and procedure to prevent, detect, contain, and correct violations, and risk

analysis is one of the four requisite implementation specifications. A thorough risk analysis should include the role of ePHI and identify all vendors who create, maintain, or transmit it, as well as all potential security threats to those systems.[6]

In addition to the bill itself, which can be found in its entirety online, the OCR has created three training modules to educate health care professionals about compliance with HIPAA regulations (Figure 1). Completion of these modules might qualify as continuing education credits for the RDN or dietetic technician, registered.

Meanwhile, Academy resources available online include a checklist for HIPAA compliance, sample Business Associate Agreement Provisions, Sample HIPAA Notice of Privacy Practices, and Sample Acknowledgement of Receipt of Notice of Privacy Practices forms. In addition, Lindsey Hoggle, MS, RDN, PMP, director of Nutrition Informatics for the Academy, said the Academy is preparing an Electronic Health Records/Personal Health Records Nutrition Best Practices Implementation Guide that will address some of the issues facing private practitioners, in particular with regard to exchanging patient information.

Beseler observed that most RDNs in private practice keep abreast of these changes, like others in the field, through Academy resources, newsletters produced by insurance carriers, the AMA, and colleagues. In her office-based practice, simple steps toward compliance include avoiding paper sign-in sheets and the unsecured transmission of ePHI. Appointment confirmation should be done in a manner compliant with a patient's requests, via their home or cell phone as opposed to a work phone, she added.

Beseler said that in her assessment, on the whole, RDNs are HIPAA-compliant and the cost of adjusting to the new rules will be minimal if colleagues use available resources. Compliance with the new HIPAA regulations is, thus, a little more for the private practitioner to handle, but part of the process with which they've become accustomed as entrepreneurs, and something with which multiple resources are available to help.

References

1. Academy of Nutrition and Dietetics. *MNT Provider*. HIPAA: What You Need to Know. 2013 Expanded Issue. Volume 12, No. 5/6.
2. US Department of Health and Human Services. New Rule Protects Patient Privacy, Secures Health Information. http://www.hhs.gov/news/press/2013pres/01/20130117b.html. Published January 17, 2013. Accessed March 5, 2014.
3. American Medical Association. HIPAA Privacy and Security Toolkit: Helping Your Practice Meet New Compliance Requirements. http://www.ama-assn.org/go/hipaa. Accessed October 29, 2013.
4. Bendix J. What the HIPAA Omnibus rule means for your practice. Contemporary OB/GYN website. http://contemporaryobgyn.modernmedicine.com/contemporary-obgyn/news/what-hipaa-omnibus-rule-means-your-practice. Published June 1, 2013. Accessed October 29, 2013.
5. Gomes N, Daly M. What practices need to do now to prepare for HIPAA Omnibus changes. Physicians Practice website. http://www.physicianspractice.com/blog/what-practices-need-do-now-prepare-hipaa-omnibus-changes. Published September. 6, 2013. Accessed November 2, 2013.
6. US Department of Health and Human Services. Final Guide on Risk Analysis. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html. Accessed March 5, 2013.