Managing HIPAA Compliance Includes Legal and Ethical Considerations

Tony Peregrin

TECHNOLOGICAL ADVANCEments that affect how protected health information (PHI) is collected, housed, and transmitted may lead to justifiable concerns for patients and clients regarding the security of these data. PHI includes any information acquired by a health care professional, including registered dietitian nutritionists (RDNs), that could be used to identify the patient/client, including but not limited to name, Social Security number, medical test results, and treatment plan.[1]

In order to understand the laws and ethical standards established to ensure PHI, RDNs should be familiar with the core elements of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA, passed into law in 1996, requires health care providers to ensure patient/client confidentiality by following certain protocols, especially regarding PHI shared and sent via digital platforms.[2]

This article describes the fundamentals of HIPAA Privacy and Security Rules, outlines the legal and ethical considerations related to securing patient/client PHI, and examines patient/client data confidentiality issues through the lens of telehealth, particularly the expanded provisions provided by the Centers for Medicare and Medicaid Services (CMS) during the coronavirus disease 2019 (COVID-19) public health emergency.

The Continuing Professional Education (CPE) quiz for this article is available for free to Academy members through the MyCDRGo app (available for iOS and Android devices) and through www.jandonline.org (click on "CPE" in the menu and then "Academy Journal CPE Articles"). Log in with your Academy of Nutrition and Dietetics or Commission on Dietetic Registration username and password, click "Journal Article Quiz" on the next page, then click the "Additional Journal CPE quizzes" button to view a list of available quizzes. Non-members may take CPE quizzes by sending a request to journal@eatright.org. There is a fee of $45 per quiz (includes quiz and copy of article) for non-member Journal CPE. CPE quizzes are valid for 1 year after the issue date in which the articles are published.

https://doi.org/10.1016/j.jand.2020.11.012

HIPAA PATIENT/CLIENT CONFIDENTIALITY RULES

There are 2 HIPAA rules that RDNs need to recognize when developing their patient and client privacy plans: The HIPAA Privacy Rule and the HIPAA Security Rule. According to the CMS, the HIPAA Privacy Rule "sets national standards for when PHI may be used and disclosed."[3] The Privacy Rule protects all "individually identifiable health information stored or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."[1] The PHI referred to in this rule includes information about the "individual's past, present, or future physical or mental health condition, payment status, and provision of health care services. Counseling services as well as medical nutrition therapy (MNT) services would be PHI, as both are the provision of health care."[1]

While the HIPAA Privacy Rule covers PHI in broader terms, the HIPAA Security Rule specifically refers to electronic PHI, and establishes "national standards to protect individuals' electronic PHI that is created, received, used, or maintained by a covered entity."[1] The HIPAA Security Rule mandates administrative, physical, and technical safeguards to ensure the security of electronic PHI.

The requirements outlined in the HIPAA privacy rules apply to all health care providers who conduct digital transactions and are not limited to those who accept Medicare or Medicaid. By definition, a covered entity is any health provider, including RDNs, who transmits PHI in a digital form via a "standard transaction." Standard transactions could include claims and requests to obtain payment and inquiries by a provider to a health plan to determine patient/client coverage eligibility. (CMS has developed a Covered Entity Guidance tool to assist users in determining their covered entity status.[4])

"Covered entities under HIPAA could potentially include RDNs who are in private practice or providing services as part of a physician's office or hospital outpatient program," explained Marsha Schofield, MS, RD, LD, FAND, senior director of the Academy of Nutrition and Dietetics' Governance, Nutrition Services Coverage.

HIPAA COMPLIANCE

When evaluating HIPAA compliance, it is important to keep in mind that the provider, rather than the individual action, is considered a covered entity and must be HIPAA compliant. It is important to keep in mind that if the RDN is a covered entity then HIPAA applies to all services provided, including MNT, as HIPAA applies to the provider and not the service.[5] Regardless of the service provided, you as a provider, are bound to HIPAA. If the RDN is not a covered entity, HIPAA does not apply legally; however, HIPAA guidelines are considered best ethical practices.

If an RDN provides MNT services, broadly defined as "assessment, intervention, and reassessment" as outlined in the MNT Current Procedural Terminology codes,[5] for even 1 patient/client and transmits PHI electronically for a transaction that the US

Department of Health and Human Services (HHS) has adopted standards, the RDN must be compliant for all transactions.

"The bottom line is, if it's MNT, then it's MNT—you can't simply decide to call your services something else to get around HIPAA, legally or ethically" (or avoid HIPAA compliance), said Mara Bujnowski, MAEd, RD, manager, Academy of Nutrition and Dietetics' Advocacy and Communications, Nutrition Services Coverage. "HIPAA compliance pertains to the individual and encompasses all of your actions."

Whether the HIPAA Privacy and Security Rules apply to an individual RDN is not related to a specific type of patient/client, specifically self-pay vs insurance-covered services, rather it depends on whether the RDN is a covered entity under HIPAA. If the RDN is a covered entity, then HIPAA applies to all health care services provided by the RDN and all PHI must be protected in accordance with HIPAA.

"If an RDN electronically transmits a claim to an insurance company and issues a superbill for another patient, the RDN must be HIPAA compliant for both transactions," explained Bujnowski. "If an RDN transmits a bill electronically for a single patient or client, then HIPAA rules apply to all transactions conducted by the RDN's practice, including when the RDN is providing the patient with a superbill."

WHY IS HIPAA COMPLIANCE IMPORTANT?

The HIPAA Omnibus Final Rule, passed into law in 2013, incorporated many of the provisions in the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act to expand how health care professionals safeguard PHI.[2] The Omnibus Final Rule places more responsibility on health care providers to hold their business associates and downstream vendors (eg, an independent billing company) more accountable to ensure patient/client privacy, as mandated by HIPAA's business associates obligations.[2,6] Breaches of PHI are outlined in the Omnibus Final Rule in a 4-tiered system of violations that range from $100 to $50,000 in penalties.[7]

Beyond legal breaches of PHI, there are also ethical considerations. "There are two overarching considerations related to HIPAA compliance: legal and ethical," said Bujnowski. "While many RDNs understand that HIPAA compliance is an important component of practice, others may be confused regarding how compliance applies to them. If you are a covered entity as defined by HIPAA, then compliance applies to you. If you are not a covered entity, HIPAA standards still apply to you ethically. HIPAA is legislation which provides security provisions and data privacy meant to keep patients' medical information safe. While HIPAA compliance is a legal issue, following the guidelines set forth in HIPAA, ensuring PHI is protected, is also best ethical practice."

"It's important to note that even if an RDN is not considered a covered entity under HIPAA, laws could exist in the state in which the patient or client resides that regulate PHI beyond HIPAA. If the federal or state-level laws do not apply for a particular RDN, they still need to conform to standards of practice and the Academy's professional Code of Ethics," added Schofield. "In other words, HIPAA compliance, in terms of safeguarding PHI, is considered a best practice for the profession."

Principle 2 of the Code of Ethics for the Nutrition and Dietetics Profession—Integrity in personal and organizational behaviors and practices (Autonomy)—emphasizes the importance of "safeguard[ing] patient/client confidentiality according to current regulations and laws," and "implement[ing] appropriate measures to protect personal health information using appropriate techniques (e.g. encryption)."[8]

Principle 2 also calls for RDNs to "document, code and bill to most accurately reflect the character and extent of delivered services."[8] As stated earlier in this article, "RDNs can't circumvent HIPAA by calling the service they provide 'nutrition education' instead of MNT," said Bujnowski.

When PHI safeguards are mandated by your status as a covered entity under HIPAA and/or state laws, and to ensure adherence to the Code of Ethics, RDNs in private practice can fortify their PHI security plan by requesting patients and clients sign a Notice of Privacy Practices, and by implementing technology-based safeguards, including encryption and the use of HIPAA-compliant platforms and networks to keep accounts secure and protected; PHI experts also suggest developing emergency measure in case there is a data breach.

TELEHEALTH

In March 2020, the CMS announced expanded policies to broaden access to telehealth services due to limitations to in-person care imposed by the COVID-19 public health emergency.

According to the Academy, starting March 6, 2020 and for the duration of the COVID-19 pandemic, "RDNs who are Medicare providers can provide services already covered by Medicare via telehealth to patients in any health care facility and in their home. These services include MNT (97802, 97803, 97804, G0270) and DSMT [Diabetes Self-Management Training] (G0108, G0109) and are not limited to patients with COVID-19. These visits are paid under the Medicare Physician Fee Schedule at the same rate as regular, in-person visits."[9]

As part of this announcement, the HHS Office for Civil Rights agreed to waive penalties for HIPAA violations "against health care providers that serve patients in good faith through everyday non–public-facing communications technologies during the emergency."[9]

According to this HHS notice, RDNs may use applications that allow for video chats, such as Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Skype, and Zoom. RDNs are encouraged to notify patients/clients that these third-party applications potentially introduce privacy risks; all available encryption and privacy modes should be activated when using these applications. However, Facebook Live, Twitch, TikTok, and similar video communication applications are public-facing and should not be used to provide MNT services via telehealth, according to HHS.[9,10]

"While there is a relaxation of enforcement of HIPAA compliance during this public health emergency, best practice is to continue to protect the privacy and security of patients and clients," said Schofield. "In an effort to quickly ramp-up your ability to provide telehealth services at this critical time, some RDNs may take this opportunity

to use non–HIPAA-compliant platforms. However, your long-term plan should be HIPAA compliance. If you plan to continue to provide services via telehealth, you should have a plan in place to transition to working with compliant platforms."

"The relaxation of HIPAA enforcement does not change the RDN's fundamental responsibility to protect patients' privacy and confidentiality ethically," said Bujnowski. "While the relaxed enforcement of HIPAA during COVID-19 has been lifted to broaden patient access to care, the RDN's fundamental ethical responsibility to protect privacy and confidentiality of the patient's PHI has always remained the same," said Bujnowski. "Following HIPAA guidelines is a reliable/steadfast way to ensure PHI is safeguarded."

CONCLUSIONS

As credentialed nutrition and dietetics practitioners, RDNs should follow legal and ethical practices to ensure patient/client privacy and confidentiality. "Managing HIPAA compliance effectively and protecting a patient's PHI promotes the value of our profession and the services we provide, and helps move the profession forward," said Bujnowski.

Understanding the basics of HIPAA compliance begins with the knowledge that the individual must be compliant rather than the action. If an RDN provides MNT or transmits billing to an insurance company for 1 patient or client, then they must be compliant for all patients/clients in their practice. The standards outlined in HIPAA, some state PHI laws, and in the Code of Ethics were established to reduce the potential for PHI data breaches and other privacy risks. Together, these guidelines are considered best practices for effectively managing how PHI is collected, housed, and transmitted—whether or not the RDN is considered a covered entity under HIPAA.

References

1. Academy of Nutrition and Dietetics. Clearing up the HIPAA confusion for RDNS. *MNT Provider*. 2016;15(6):1-4.
2. Boyce B. HIPAA compliance from a private practice purview. *J Acad Nutr Diet*. 2014;114(9):1341-1346.
3. HIPAA basics for providers: Privacy, security, and breach notification rules. Medical Learning Network fact sheet. Centers for Medicare & Medicaid Services. Published September 2018. Accessed July 15, 2020. https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf.
4. Are you a covered entity? Covered entity guidance tool. Centers for Medicare & Medicaid Services. Accessed July 15, 2020. https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.
5. CPT and G codes for RDNs. Academy of Nutrition and Dietetics. Accessed July 15, 2020. https://www.eatrightpro.org/payment/coding-and-billing/diagnosis-and-procedure-codes/cpt-and-g-codes-for-rdns.
6. HIPAA changes: The omnibus rule. Academy of Nutrition and Dietetics. Accessed July 15, 2020. https://www.eatrightpro.org/payment/business-practice-management/hipaa-and-other-regulations/hipaa-changes-the-omnibus-rule.
7. HITECH Act Enforcement Interim Final Rule. US Department of Health and Human Services. Accessed July 15, 2020. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
8. Code of Ethics for the Nutrition and Dietetics Profession. Academy of Nutrition and Dietetics. Accessed July 1, 2020. https://www.eatrightpro.org/-/media/eatrightpro-files/career/code-of-ethics/coeforthenutritionanddieteticsprofession.pdf?la1/4 en&hash1/4 0C9D1622C51782F12A0D6004A28CDAC0CE99A032.
9. During COVID-19 emergency. CMS gives green light to MNT via telehealth for Medicare beneficiaries. Academy of Nutrition and Dietetics. Accessed July 1, 2020. https://www.eatrightpro.org/news-center/member-updates/coronavirus-updates/during-covid19-emergency-cms-gives-green-light-to-mnt-via-telehealth-for-medicare-beneficiaries.
10. Notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency. US Department of Health and Human Services. Accessed November 2, 2020. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

AUTHOR INFORMATION

T. Peregrin is an editor and writer for a Chicago-based medical association and a freelance writer in Chicago, IL.

STATEMENT OF POTENTIAL CONFLICT OF INTEREST

No potential conflict of interest was reported by the author.

FUNDING/SUPPORT

There was no funding for this article.