

## Emerging Technology and the Health Insurance Portability and Accountability Act

**Q**UESTIONS PERTAINING TO patient privacy multiply at the same great speed as technologic innovation. Advances in communication technology offer significant opportunities for patients and providers alike while simultaneously posing new risks for security breaches. Evidence is mounting that US health care patients want to use new communication technologies in conjunction with their treatments, particularly by way of electronic messaging and web-based portal programs involving their electronic health record (EHR).<sup>1-4</sup> Providers express concern about the process in terms of legal obligations and clinical value, both of which can be addressed through education.<sup>1</sup>

Addressing a patient's expressed desire for electronic communication-related services can help registered dietitian nutritionists (RDNs) expand market share, lower costs, improve health outcomes, and enhance patient satisfaction. The Academy of Nutrition and Dietetics offers members a number of educational resources and materials in the area of compliance, as do most other professional health care associations. These resources include contacts within state and local affiliate programs, dietary practice groups, and multiple other options that can be found on the Academy of Nutrition and Dietetics website ([www.eatright.org](http://www.eatright.org)). Case studies specifically designed to address these concerns are also available online and can serve as models for other practices.<sup>2-4</sup> The security of protected health information and electronic protected health information (e-PHI) in conformance with the Health Insurance Portability and Accountability Act (HIPAA) is an ongoing

topic for health care professionals throughout the country and RDNs can benefit from participating in those discussions.

Surveys indicate one reason patients favor these advances is the potential savings offered in terms of time and money.<sup>1</sup> Research suggests that when patients control their EHR by electronic means it confers positive feelings of empowerment, activation, and control over their health.<sup>5</sup> Patient activation—skills and confidence that equip patients to become actively engaged in their health care<sup>5</sup>—has been strongly correlated with improved outcomes, suggesting that informed and competent patients are less costly than those without knowledge.

### EXAMPLES OF OPPORTUNITIES TO ENHANCE SERVICES

Electronic-based strategies improve communication and outcomes across the country. Reports of successful implementation of such strategies are becoming more common every day.<sup>2</sup>

In one example, primary care physicians in New York documented significant reductions in hemoglobin A1c levels among patients with both pre-diabetes and diabetes, as well as reduced cholesterol levels ranging from 15 to 50 points, when involved in a preventative health care program centered around using EHRs and secure web portals.<sup>2</sup> Using the EHR system's patient registry functionality, the providers track progress on key health indicators such as weight loss, blood pressure, and cholesterol levels while patients are participating in wellness-oriented weight loss and fitness programming.

In a separate case at Blackstone Valley Community Health Care, a federally qualified, Joint Commission-accredited health center in Rhode Island serving more than 11,000 patients, clinicians, and staff reported that the use of a specialized and secure web-based portal system reduced call volume and

improved documentation quality by electronically routing communications to the EHR. Patients reported high levels of positive feelings about the electronic alternative to using the facility call center.<sup>3</sup>

Likewise, a case study<sup>4</sup> examining a Delaware-based family practice's partnership with the Delaware Regional Extension Center to create a secure web portal for the purposes of allowing patients to schedule appointments, request prescription refills, pay bills, and review lab results reported significant levels of satisfaction. Since first adopting the EHR in 2008, the portal has grown to include new features, like a secure messaging function that allows staff to triage messages and requests. Meaningful use is defined as the use of certified technology in EHR implementation to improve quality, safety, efficiency, and reduce health disparities, engage patients and caregivers, improve coordination of care and public health, and maintain privacy and security of protected health information.<sup>6</sup> Meaningful use objectives addressed include the provision of patient-specific education resources, clinical summaries, and access to the EHR.<sup>4</sup> Clinicians involved reported that modern patients are accustomed to electronic communication to the point that it is now second nature.<sup>4</sup>

### HIPAA COMPLIANCE

For those with concerns about whether a health care professional can or cannot use electronic communication technology while working with patients, the simple answer is yes, they can.<sup>7,8</sup> The better question is, How?

First enacted by Congress in 1996, HIPAA was born about the same time e-mail came into common public use, well before the texting capacities of most 21st century smartphones. Since then, the law originally drafted in the days of paper health records and office memos has expanded in multiple areas

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

<http://dx.doi.org/10.1016/j.jand.2016.05.013>

- HIPAA - Privacy and Security in a Digital World <http://www.eatrightpro.org/resource/news-center/in-practice/nutrition-informatics/hipaa-privacy-and-security-in-a-digital-world>
- Smart Business Practice and Management <http://www.eatrightpro.org/resources/practice/getting-paid/smart-business-practice-and-management>
- The Office of the National Coordinator for Health Information Technology maintained by the US Department of Health and Human Services <https://www.healthit.gov/>
- The US Department of Health and Human Services <http://www.hhs.gov/hipaa>

**Figure.** Additional resources.

to address the changing technology landscape, including the advancement of the HIPAA Omnibus Rule in 2013. Per the rule, the term *e-PHI* has been added to the legal lexicon involving privacy, referring to electronic protected health information.<sup>7</sup> The Office of Civil Rights of the US Department of Health and Human Services maintains and enforces the HIPAA security rule as it pertains to e-PHI with comparable rigor as to paper.<sup>7</sup>

The first step in HIPAA compliance involving electronic communication is achieving meaningful consent from patients, which necessitates that patients fully understand the methods and manner in which information will be transmitted. Meaningful consent occurs when patients make informed decisions and the choice is properly documented and maintained as a matter of record. It also requires the decision be made with full transparency and education, is made after a patient has had sufficient time to review the materials and process, is commensurate with the circumstances requiring such transfer, is not used as a condition of receiving treatment, is consistent with patient expectations, and is revocable by patients.<sup>9</sup> The wishes of patients who state an objection to the use of electronic communication when handling their information must be respected, and informing a patient of the potential risks involving potential breaches is also required.

The Office of the National Coordinator for Health Information Technology contained within the Department of Health and Human Services recommends a 7-step process by which to achieve and maintain HIPAA

compliance while handling e-PHI: select the compliance team; document the process, findings, and actions; review existing security and perform ongoing security risk analysis; develop an action plan; manage and mitigate risks; attest for meaningful use; and monitor, audit, and update security on a regular basis.<sup>10</sup>

When using a mobile device to transmit protected health information securely, the Department of Health and Human Services recommends a proactive approach: use a password or other user identification, install and enable encryption, install and activate remote wiping and remote disabling, disable and do not install or use file sharing applications, install and enable a firewall, install and enable security software, keep your security software up to date, research mobile applications before download, maintain control over the system, use adequate security to send or receive health information over public Wi-Fi networks, and delete all stored health information before discarding or reusing the mobile device.<sup>8</sup>

Per the HIPAA security rule, covered entities must perform ongoing risk analysis concerning their practice.<sup>7</sup> Breaches, or potential breaches, of privacy must be reported to the involved individuals, and depending on number of patients involved, the Office of Civil Rights.<sup>11</sup>

As technology continue to advance, the need for RDNs to maintain and enhance their knowledge of electronic systems will continue to grow. The US Department of Health and Human Services offers multiple toolkits and videos on these topics as they pertain to health care professionals at [www.hhs.gov](http://www.hhs.gov).

[hhs.gov](http://www.hhs.gov). The use of such freely available resources, as well as documented case studies that can serve as templates (see the [Figure](#)), will help with the successful incorporation of electronic communication into health care practice.

## References

1. Better together: High tech and high touch. Consumer Healthcare Survey results. [http://accountablecare.doctors.org/wp-content/uploads/2015/11/CAPP-SHP-Consumer-Survey-Full-Presentation\\_103015.pdf](http://accountablecare.doctors.org/wp-content/uploads/2015/11/CAPP-SHP-Consumer-Survey-Full-Presentation_103015.pdf). Accessed February 15, 2016.
2. Dr. Reed uses health IT to help her patients improve health and wellness. <https://www.healthit.gov/providers-professionals/dr-reed-uses-health-it-help-her-patients-improve-health-and-wellness>. Accessed February 22, 2016.
3. Meaningful use case study: Patient portal increases communication between patients and providers. <https://www.healthit.gov/providers-professionals/blackstone-valley-community-health-care-case-study>. Accessed March 1, 2016.
4. Meaningful use case study: Patient portal implementation improves quality of patient care and strengthens preventative care. <https://www.healthit.gov/providers-professionals/dover-case-study>. Accessed March 1, 2016.
5. EHR incentives and certification: What is meaningful use? <https://www.healthit.gov/providers-professionals/ehr-incentives-certification>. Accessed May 15, 2016.
6. Lassere M, Baker S, Parle A, Sara A, Johnson K. Improving quality of care and long-term health outcomes through continuity of care with the use of an electronic or paper patient-held portable health file (COMMUNICATE): Study protocol for a randomized controlled trial. *Trials*. 2015;June 4;16:253.
7. Summary of the HIPAA Security Rule. <http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/>. Accessed February 15, 2016.
8. How can you protect and secure health information when using a mobile device? <https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device>. Accessed February 19, 2016.
9. Patient consent for electronic health information exchange. <https://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange>. Accessed February 20, 2016.
10. Chapter 6: Sample seven-step approach for implementing a security management process. <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-6.pdf>. Accessed February 21, 2016.
11. Submitting notice of a breach to the secretary. <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>. Accessed February 20, 2016.