QUESTIONS 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). Providers express concern about the process in terms of legal obligations and clinical value, both of which can be addressed through education.

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 within state and local affiliations. These resources include contacts and other professional health care associations related to electronic health record (EHR) now second nature.

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

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. 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 late 1990s to address these concerns is as relevant today as it was at the time it was passed.

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
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. 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.

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. 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.

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.

Per the HIPAA security rule, covered entities must perform ongoing risk analysis concerning their practice. 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 also required. As technology continues 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 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