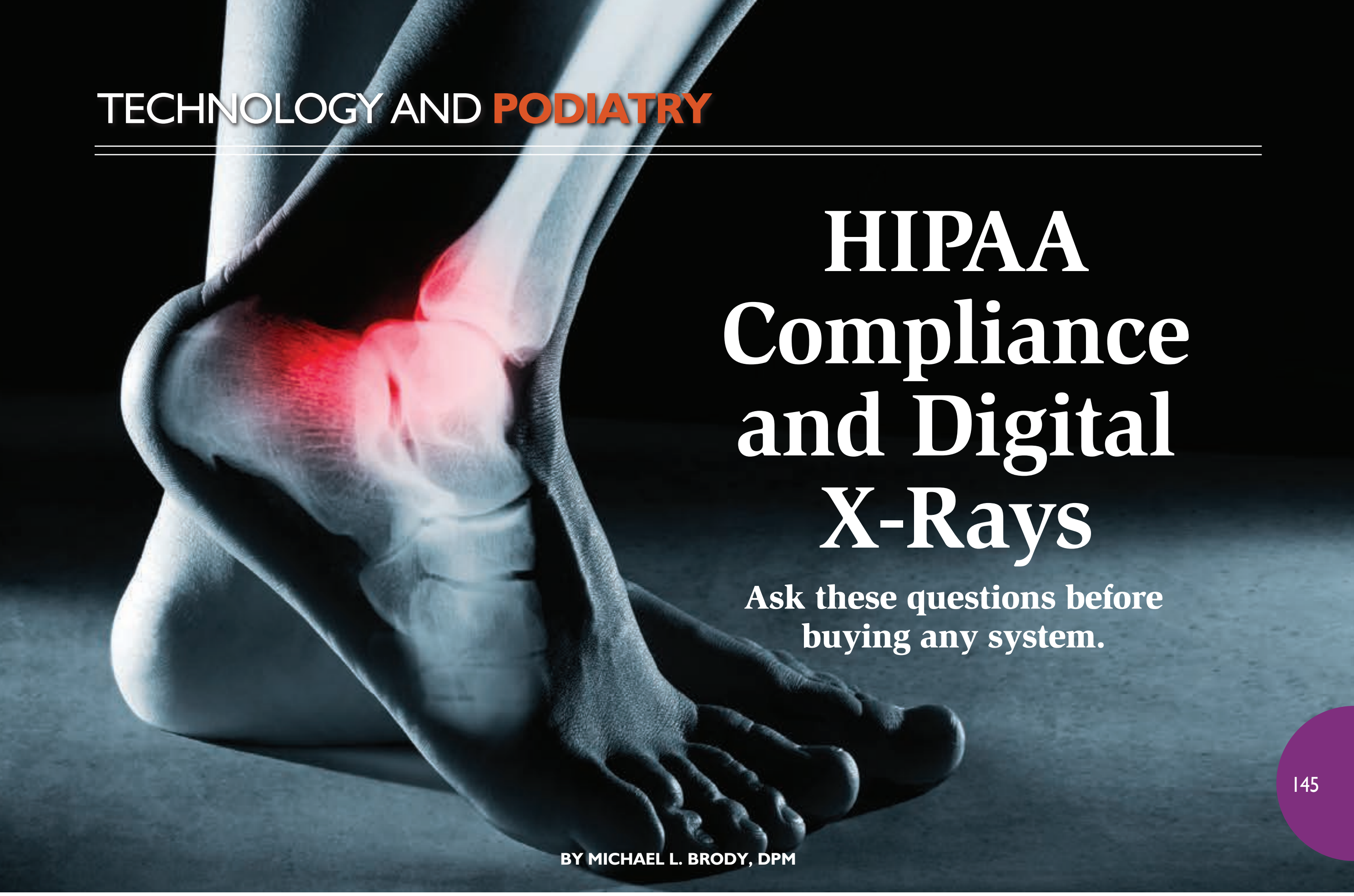

HIPAA Compliance and Digital X-Rays

Ask these questions before buying any system.

BY MICHAEL L. BRODY, DPM

***Editor's Note:** The following article is an extended response to a recent query posted on PM News.*

***Query:** If all the devices on the network and the network itself are HIPAA-compliant, does software that runs on the devices and has access to ePHI need to be HIPAA-compliant?*
—Mark Tuccio, DPM, Jamestown, NY

Response: What does HIPAA compliance mean when it comes to software? HIPAA—The Health Insurance Privacy and Portability Act. When you talk about software, it is usually more the portability portion which is being talking about.

HIPAA is the acronym of the Health Insurance Portability and Accountability Act of 1996. The main purpose of this federal statute was to help consumers maintain their insurance coverage, but it also includes a separate set of provisions called Administrative Simplification. This section of the act is aimed at improving the efficiency and effectiveness of the healthcare system. The key components of Administrative Simplification include:

1) Standardized electronic transmission of common administrative and financial transactions (such as billing and payments).

2) Unique health identifiers for individuals, employers, health plans, and healthcare providers.

3) Privacy and security standards to protect the confidentiality and integrity of individually identifiable health information.

Every single EHR and practice management program we use today is HIPAA-compliant.

Let's look at each of the three components.

1) This rule requires our billing software to talk seamlessly with claims clearinghouses and with insurance companies. Every single EHR and practice management program we use today is HIPAA-compliant or else we would not be able to financially run our practices.

2) If you have an NPI, you are compliant with this.

3) These are the policies and procedures that you have in your office.

When a software developer says they are HIPAA-compliant, they are ONLY talking about #1 above. #2 requires you to get an NPI number, and #3 requires you to implement physical technical and physical safeguards to protect your data.

A software program such as a digital x-ray system may have tools to better enable you to implement technical security. Here are the questions to ask the vendor to see how many tools they have put into place:

1) Can you show me the audit logs built into your software?—If the software does not have audit logs, then I do not see how the program can claim it is HIPAA-compliant (EHR systems that are Certified for Meaningful Use have the logs)

2) What type of encryption is built into your system?—If you are

Continued on page 146

© Vadimrysev | Dreamstime.com

HIPAA Compliance (from page 145)

looking at Certified EHR software, you don't have to ask this question—Digital x-ray systems are NOT certified for Meaningful Use

3) What type of tools are built into your system to allow me to do backups?—If the software does not have encryption, that is okay. You can use third-party tools to encrypt your computer. It is not needed to be in your software. If the software does not have a back-up utility but you know where the data is stored, you can use third party tools to backup your data.

4) What controls do you have in place to require me to change my password on a regular basis?—This can be in the software or can be a policy that you have and you can change passwords regularly without the software requiring it.

5) How easy is it for me to change my password? What controls do you have in place to require me to use strong passwords?

6) Can I de-activate a user account without deleting it?

7) Can I set the software up for users to have their own username and password?

So, call the vendor and say, "I am very interested in seeing how your software is HIPAA-compliant. Please demonstrate those features to me." If they start verbally explaining anything, stop them and say, "I want to see a demonstration in the software." Let them show you 'how' their software is HIPAA-compliant, and if the things they show you have nothing to do with the items above, be curious about what they are showing you. **PM**

What controls do you have in place to require me to change my password on a regular basis?

Dr. Michael Brody has presented webinars for the e-Health initiative, (www.ehealthinitiative.org/) and is active in the EMR workgroup of the New York E Health Collaborative (www.nyehealth.org/). He has provided consulting services to physicians for the implementation of EHR software and to EHR vendors to assist in making their products more compatible with CCHIT and HIPAA guidelines. Dr. Brody is a member of AAPPM.