should be able to tell you whether there are laws or regulations in your state that affect the release of sensitive information.

Q I am the privacy and security officer for a small practice. I am currently working on updating our notice of privacy practices and our accounting of disclosures policy. I wanted to find out if any of the new finalized rules indicate that the accounting of disclosures covers disclosures for treatment, payment, and healthcare operations. I thought the new rule stated that with EMR all disclosures (for any reason) would need to be tracked for the previous three years from the date of the request. Is this correct?

A The accounting of disclosure requirements were not addressed in the HIPAA omnibus rule. This will likely be addressed in a future rule.

Q I have a follow-up inquiry regarding a question you answered in the November 2013 issue of BOH. The original question was from someone who was concerned about leaving information on a patient's voice mail that could allow an individual listening in to search the physician's name and identify the service. My question is: If the identified physician is a specialist who treats patients for infectious diseases, wouldn't that pose a potential risk of releasing PHI? It seems that the patient could be identified as being treated by an infectious disease specialist.

A Many infectious disease specialists treat a variety of conditions, so knowing a physician specializes in infectious disease would not necessarily provide information about the patient's diagnosis. If the specialist treats only one infectious disease, such as HIV, then the office should leave a message that does not include the doctor's name. For example, "This is Kathy calling from the clinic. John, please call me back at 123-456-7890. Thank you."

Q In the November 2013 issue of BOH, I read your response about leaving a voice mail for a patient. This got me thinking about whether it is appropriate to leave billing information on a patient's voice mail. If the patient called with a billing inquiry, would it be appropriate to leave the following message on the patient's voice mail?

"Hi, this is Dr. Smith's office returning your call. The bill in the amount of $30 was for the office visit that you had on November 15, 2013."

A Yes, this message is appropriate because it does not include any information about the patient's diagnosis or treatment.

EDITOR'S NOTE

Brandt, vice president of health information at Baylor Scott & White Health in Temple, Texas, provided these answers. She is also an advisory board member for **Briefings on HIPAA.** This information does not constitute legal advice. Consult legal counsel for answers to specific privacy and security questions. Email your HIPAA questions to Associate Editor Jaclyn Fitzgerald at *jfitzgerald@hcpro.com.*

Product watch

AG Mednet offers tool for secure transmission of clinical data

by Chris Apgar, CISSP

The movement of large files is essential in the world of clinical trials, especially when it comes to transmitting images like MRIs and CT scans, which are important tools in clinical research.

AG Mednet continues to assist hospitals and health systems around the world in securely de-identifying clinical data and transmitting it across country lines. This enables cross-border research efforts while ensuring the security of the data transmitted and stored.

AG Mednet supports a HIPAA and 42 *CFR* Part 2 compliant medical imaging network. Imaging trial sponsors, core labs, and clinical research organizations that collect imaging time points as part of clinical trial protocols can contract with AG Mednet's

automated system to assist with site compliance and the secure electronic transfer of scans internationally.

One of the keys to AG Mednet's success is its ability to de-identify patient data and images at the hospital before transmitting or storing the data on cloud servers. No identifiable data leaves the institution. This makes the exchanged data compliant with the HHS limited data set and de-identified data guidance issued November 26, 2012.

AG Mednet's system automatically checks data prior to transmission for compliance with standards that ensure the usability of the data for clinical trials and research. This supports the protection of privacy of patients even in countries with more stringent privacy laws than the United States. It also improves the quality of the data because it is not transmitted in an identifiable format that is de-identified elsewhere, which often leads to the possibility of data corruption.

It is often difficult to engage hospital and health system IT resources because of the significant demand for these resources at the institutional level. AG Mednet developed tools that require minimal intervention by the IT department and minimal allocation of resources at the local level. Data is transmitted and received by a front end, the Desktop Agent. The Desktop Agent fits within existing site infrastructure and workflow without the need for IT intervention.

Through the use of the Desktop Agent, data is transmitted through an institution's firewalls using standard ports. The data is encrypted using public key infrastructure and it is de-identified before being transmitted through the firewall. In AG Mednet's words, institutions "lease the onramp" transmitting data across the world.

AG Mednet stores the de-identified data for seven days before securely destroying it. AG Mednet offers secure cloud storage for customers with limited access to the data storage needed for clinical trials and research.

The cloud-stored data is accessed via thin client–data can be viewed and manipulated but it's not stored on local servers or workstations.

The HIPAA Security Rule was based on the National Institute of Standards and Technology (NIST) publications. In the international world of research, the commonly required standard is based on ISO 27001. The ISO standards are viewed as more of a regulatory requirement rather than a referenced set of standards.

AG Mednet is compliant with NIST and ISO standards so, as a vendor, AG Mednet is in a position to support international research rather than just U.S.–based research.

Privacy laws in countries such as the European Union and Canada are more stringent than the HIPAA Privacy Rule requirements. De-identification of data is critical when transmitting images of individuals residing in, say, France, with clinical researchers in the United States.

AG Mednet is required to adhere to the less stringent HIPAA Privacy Rule as well as international law. This allows for a seamless exchange of clinical data across the globe.

AG Mednet offers a service that supports clinical trials without the use of secure FTP, increasing the ability to send large volumes of data quickly in a way that protects the confidentiality and integrity of the data. For more information, go to *www.agmednet.com*.

EDITOR'S NOTE
Apgar is president of Apgar & Associates, LLC, in Portland, Ore.

Briefings on HIPAA 2013 index

Breaches