The widespread adoption and use of electronic health records (EHR) continues to transform the health-care industry in the United States. According to The Office of the National Coordinator for Health Information Technology (ONC), an EHR is a digitalization of a patient’s medical charts and records. Ideally, this electronic record may then be shared among providers, collecting information and data about the patient along the way, resulting in a comprehensive patient medical history that is widely and readily available when needed. Partly as a result of the HITECH Act, the goal of encouraging EHR adoption has been substantially achieved, with 94 percent of hospitals using a certified EHR system.

The shift to EHR was initially supposed to take place in three stages, spanning several years. To accomplish that timeline, the HITECH Act created a series of staged incentives and financial penalties (estimated to cost roughly $30 billion) to usher physicians into compliance by 2015. Under these incentive programs, providers who demonstrate “meaningful use” of EHR can earn annual incentive payments. The term “meaningful use” may be understood as a compilation of defined goals and objectives that demonstrate a shift from paper recording to electronic recording. For example, if a particular electronic record includes sixteen menu options, a provider may have to meet eleven core requirements and then five of ten further options to substantiate meaningful use.

While this carrot-and-stick approach made sense in theory, the HITECH Act failed to account for the possibility that various EHR systems might fail to achieve (for a variety of reasons) a level of technical interoperability necessary to satisfy certain meaningful use criteria. The challenge of obtaining true interoperability of EHR systems has had the greatest impact on those providers faithfully following the timeline set forth under HITECH, and who are now hoping to complete Stage 3’s information sharing requirements. To do so, however, a provider must: 1) send an electronic summary for 50 percent of TOC (Transitions of Care) and referrals; 2) receive an electronic summary for 40 percent of TOC and referrals; and 3) perform
med/allergy/problem reconciliation for 80 percent of TOC and referrals.\textsuperscript{10} Satisfaction of these criteria can be accomplished only with EHR systems that are truly interoperable.

According to the Healthcare Information and Management Systems Society, interoperability is the “ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged.”\textsuperscript{11} Ideally, practitioners, hospitals, laboratories, pharmacies, and patients could all access and use EHR across organizational boundaries, and regardless of the software application or vendor utilized, to enhance the delivery of patient care.\textsuperscript{12} This ideal, however, is still far from reality. The trouble has less to do with identifying the problem than with solving it. At the federal level, a committee composed of representatives from The Office of the National Coordinator, CMS, and other stakeholders has struggled to promulgate workable rules governing interoperability.\textsuperscript{13} These proposed rules, in their many versions,\textsuperscript{14} have most often relied on a system of carrots over sticks, in the hope of luring physicians and health-care providers to adopt cross-platform EHR sharing. More recent regulations promulgated pursuant to the Medicare Access and CHIP Reauthorization Act of 2015 require health-care providers, as part of the meaningful use program, to attest that they have not taken steps that would result in limitations on the interoperability of their EHR.

Even if government efforts are successful in promoting comprehensive EHR sharing, significant policy concerns remain. Chief among them is the worry that the seamless sharing of information will facilitate access to private health information not just for providers and patients, but also for outsiders with nefarious intentions or motives. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)\textsuperscript{15} is intended to protect against this concern. Fundamentally, however, the massive amount of personal health information stored in EHR systems, including the related information sharing platforms, equates to a greater risk of large-scale disclosure and potentially more damage to patients if EHR security is compromised.

In addition to privacy concerns, widespread sharing of EHR raises a number of unexpected clinical and business concerns. For example, some now worry that physicians may have access to too much information for treatment purposes, unnecessarily complicating the process of diagnosing and treating routine ailments. Conversely, others worry that EHR vendors and institutional providers may be intentionally blocking the free exchange of health information to further their own business interests. In response to these concerns, ONC recently issued a report to Congress on the practice of health information blocking, including suggestions for a comprehensive response strategy.\textsuperscript{16} Part of the challenge lies with EHR vendors, who have had mixed reactions to the federally mandated move towards data sharing. Several EHR vendors formed a trade group, CommonWell Health Alliance, to allow their customers to share electronic records, while other large EHR vendors such as EPIC have been reluctant to join any trade groups, asserting that their customers have not expressed an interest in being part of a national data sharing organization.\textsuperscript{17} In the coming years, both the ONC and Congress will need to implement further rules and regulations to prevent information-blocking practices and encourage EHR interoperability while allowing providers and vendors to maintain their autonomy and market presence.

**Privacy and Security Concerns**

In addition to the challenges of data sharing, the transition of patient records from hardcopy files to EHR systems has raised new and complex challenges with respect to patient privacy. Whereas the security of physical records could often be managed effectively by storing records in locked rooms or cabinets and by limiting access, the electronic data files that comprise EHR systems are much more difficult to control. Modern EHR systems attempt to control access by using usernames and passwords, but such authentication measures are inherently at risk for loss, theft, or misuse. In addition, the nature of EHR date files themselves results in an increased risk of improper disclosure. Because EHR date files are stored in digital media, they often may be copied (with or without authority) to mobile storage devices, such as computer hard drives, flash drives, or DVDs, the loss or theft of which can be catastrophic from a privacy and security perspective. Unfortunately, stories of massive breaches of electronic data systems containing patient health information have become somewhat commonplace, with Anthem Inc.’s recent disclosure of tens of millions of patient records as just one.\textsuperscript{18}

In the face of these increased risks, the law continues to place tremendous emphasis on the privacy and security of patient health information. For example, the Virginia General Assembly has tasked the State Health Commissioner with ensuring that patient privacy is an overriding goal of licensure and enforcement efforts related to
The HIPAA Security Rule. As the variety of electronic, paper, or oral. The HIPAA Security Rule personal health information from, electronic data reporting system operated by laboratories or 

Among those laws governing the privacy and security of EHR, HIPAA is the starting point. Together, the HIPAA Privacy Rule and Security Rule protect the use, disclosure, and security of personal health information, which includes individually identifiable health information held or transported by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The HIPAA Security Rule establishes minimum security standards for protecting electronic personal health information, including that found in EHR. But implementing the HIPAA Security Rule in the context of EHR is far from simple.

The term EHR, when used broadly, includes information or data beyond that traditionally stored in a patient’s health record, and frequently includes information existing in multiple data sources. For example, electronic records containing personal health information may be found in a provider’s primary EHR system (i.e., the electronic medical record), billing system, email or messaging exchange servers, or even personal mobile devices carried by practitioners. A provider may also have access to, and acquire personal health information from, electronic data reporting systems operated by laboratories or diagnostic imaging centers, or a health information exchange open to other providers. In sum, “an EHR system consists of a plethora of integrated component information systems and technologies,” all or part of which may include electronic personal health information subject to the HIPAA Security Rule. As the variety of electronic data systems containing personal health information continues to proliferate, providers and their attorneys must be increasingly vigilant to the requirements of the HIPAA Security Rule.

**Discovery of EMR During Litigation**

The unique nature of EHR also presents practical and legal challenges in the context of litigation discovery. Most obvious are the privacy and security concerns, and in particular compliance with HIPAA and analogous state laws, the burden of which falls primarily on the recipient of a discovery request. Second, discovery requests seeking patient health information often seek records or information found in a variety of sources including the EHR, but also including other sources that fall outside the patient’s “medical record” as traditionally conceived. Identifying and gathering the requested information from a variety of sources, some electronic, some paper, and some more nebulous, e.g., information accessible from a health information exchange or stored in the “cloud,” can be difficult. And finally, the design of EHR data systems often does not lend itself to production in a traditional hardcopy format. EHR systems are designed primarily to store patient health information and display it for use on a screen, not to format and print that data for production in response to a subpoena.

Prior to the advent of EHR, responding to a subpoena for a patient’s health record was relatively straightforward. Assuming the health-care provider maintained all records related to the care of patients in a system of hardcopy files, which was the norm, responding to a subpoena required little more than photocopying the file. Even today, Virginia state law conceives of health record storage and production through this document-centric view, permitting a provider to charge a reasonable fee for production of health records which “shall not exceed $0.50 per page for up to 50 pages and $0.25 a page thereafter . . . .”

The reality, however, is that EHR data systems are frequently not organized or easily reproducible as a comprehensive set of printed documents. Rather, EHR systems store data that may be displayed on a screen in a variety of formats depending on the needs of the provider. In addition, EHR systems often store data that is not intended for routine display to the end user, such as metadata identifying who accessed or viewed the records, who entered data to the record and when it was entered, and whether (or when) an authorized user responded to an alert or pop-up messages. The ability of EHR systems to store more data at a lower cost, in combination with the recent emphasis on evidence-based medical decision making, has also resulted in a massive increase in the amount of patient information stored by providers. Collectively, these factors can make it extremely difficult (and costly) for providers to identify all of the electronic patient information that may be responsive to a broadly

Prior to the advent of EHR ... responding to a subpoena required little more than photocopying the file.
worded subpoena, and to produce that information in a paper format that may have never been contemplated by those who designed the underlying software.

Conclusion
In a perfect world, widespread implementation of EHR would result in better medical decision making by providers and better care for patients. The jury is still out on whether EHR has, or ever will, accomplish that goal at a reasonable cost. The potential benefit of making more health information available to more people brings many challenges, including those discussed in this article. In the coming years, health-care providers and others in the industry will continue to wrestle with the fundamental questions raised by EHR: What information is needed? Who needs access to that information? How can the privacy and security of the information be reliably safeguarded? And, of course, how much money should, or can, be spent to achieve EHR’s promise of better health care?

Endnotes:
12 Id.
19 Virginia Code Ann. § 32.1-19(C) (emphasis added).
20 Virginia Code Ann. § 32.1-127.1:01, et seq.
21 See, e.g., 18 VAC 90-20-300(A)(2) (defining unprofessional conduct for licensed nurses to include any violation of the Virginia Health Records Privacy Act).
23 See, e.g., The Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Electronic Health Information (April 2015).
26 Virginia Code Ann. § 8.01-413.

Molly E. Trant is a senior corporate counsel for Riverside Health System. She works closely with her business colleagues at Riverside Health System to provide legal advice on general health-care and regulatory matters, corporate governance, and transactional matters.

Jeremy A. Ball is a director in McCandlish Holton PC’s Health Care Practice Group. He represents health systems, hospitals, nursing facilities, physician practice groups, ancillary health care providers, and managed care health insurance plans in a variety of transactional, regulatory, and reimbursement matters.