# Interview With Douglas A. Grimm: Will Privacy Concerns Slow Electronic Health Record Adoption Rates?

*Regardless of whether health care reform is enacted this year, the widespread adoption of electronic health records continues, as federal stimulus programs and skyrocketing administration costs make switching patient records from file cabinets to computers a top priority. As crucial questions on electronic records' formats and standards play out, doctors, insurers and employers are closely assessing the means by which electronic records will impact their enterprises, with privacy and security regulations of paramount concern. Indeed, with online records breaches in the news and federal privacy rules set to surround more health-affiliated enterprises, stakeholders are racing to size up the advantages and attendant obligations that electronic records are introducing across the board.*

*We recently spoke about this with Pillsbury health care attorney Douglas A. Grimm, who advises caregivers, insurers and medical technology firms on regulatory, privacy, and fraud and abuse issues. He explains why trust in electronic records depends largely on time-honored standards of conduct and adherence to expanded and existing laws. A Fellow in the American College of Healthcare Executives and former hospital Chief Operating Officer, Grimm has extensive experience advising clients regarding the health care industry's complex business, compliance and IT challenges.*

*Q.* **The push for electronic or "paperless" health records has been around for years. What is adding momentum today?**

*Grimm:* While there are divergent views on the need for health care reform, technology always has bipartisan appeal. Few disagree that paper-based medical records cause a lot of the redundancy, errors and administrative overhead that reformers of all kinds want to reduce, making a fully electronic platform our inevitable destination. The recently-passed



Published in the January 2010 issue of Privacy & Data Security Law Journal.

American Recovery & Reinvestment Act of 2009 ("ARRA") provides for grants to health care providers seeking to migrate to electronic records systems. To receive funding, the Department of Health and Human Services requires these systems to meet "meaningful use" and "interoperability" tests. Specifications for these criteria are not yet finalized, but in a sign showing their importance, the Office of the Inspector General at HHS has already indicated that the agency's inspectors will make scrutiny and enforcement in this area a top priority. This means a great deal of care has to go into these funding proposals, as well as follow-through to ensure systems funded by the government actually perform as intended.

*Q.* **What will electronic health records look like — simply paper forms on a screen, or something more transformational?**

*Grimm:* Electronic health records technology is still in a relative infancy. Much like the Internet incrementally revolutionized business and personal communication with e-mail, instant messaging and video-conferencing; electronic records will evolve over time, with emphasis on consistent security and interoperability, more than any one technology. There are many proven formats to draw on. For example, records could be stored on "smart cards" that patients carry with them or housed in centralized data banks that authorized parties such as physicians and pharmacists could access and update. A mature electronic patient record system will consist of a combination of technologies, so expect regulators to focus on rules for keeping everything confidential and also "survivable," in the event of a computer crash or outage.

*Q.* **Few issues concern Americans more than ensuring that personal information, such as their health status or history, is protected. What are key security and privacy concerns surrounding electronic records?**

*Grimm:* No file system — whether stored manually or electronically — is 100 percent secure. Anything placed on a network is inherently at risk of being inappropriately viewed, duplicated, modified, deleted or inadvertently or deliberately transmitted via e-mail, wireless signals or portable

devices. Standards for privacy and security are set by the Health Insurance Portability and Accountability Act ("HIPAA") and its accompanying regulations. Hospitals, physicians' offices and other responsible institutions must follow HIPAA and mitigate privacy and security risks by implementing strong internal policy compliance programs, just as we have had in the paper records era.

Consider the "insider threat" scenario, for example. A doctor and former staffers at a Little Rock, Arkansas hospital were recently convicted of violating HIPAA privacy laws when they viewed a local celebrity's health information without authorization. The individuals used their office and home computers to access the health records of the celebrity after learning that she had been treated at their hospital. Accessing patient information for no legitimate reason is expressly forbidden by HIPAA. Nonetheless, the incident speaks volumes about human behavior being the biggest threat to any sensitive records system, paper or otherwise.

However, electronic records' transformational potential could help mitigate this type of risk by tracking and monitoring, in real-time, exactly which computers and user accounts are seeking to access certain kinds of information. The ability to log or block suspicious requests could prove an invaluable deterrent to health personnel or others, such as tabloid journalists, seeking to share private medical information without authorization. A paper file folder, in contrast, tells no tales regarding who viewed it last, who showed it to a friend, or who may have photocopied its contents. Ironically, while it is entirely possible that a file folder locked in a drawer is physically more secure than electronic information stored behind a firewall and subject to cyber attacks, the locked drawer's protection comes at the price of limiting access to information, a challenge for keeping records updated and useful for authorized parties.

*Q.* **Will electronic records trigger regulatory changes to assure greater privacy and safety?**

*Grimm:* More than "changing" applicable federal privacy laws, instead we are seeing their breadth and scope grow. Thus, they apply to a greater number of organizations. Recent legislation has extended HIPAA's reach

to not only health care providers, insurance plans, and data clearinghouses, but also to all of those entities that contract with the covered entities. Any distinction in the eyes of enforcers between these contracting firms — referred to as "business associates" under HIPAA, and traditional "covered entities" is erased. Thus, business associates will shoulder much more accountability and legal risk.

*Q.* **Any last thoughts?**

*Grimm:* Electronic records are putting each business in the same boat when it comes to privacy, security and accountability. Since electronic health records are designed to follow patients wherever they might seek care, HIPAA covered entities and business associates must act in concert, otherwise they will simply become the weakest link in the chain. Ideally, effective data protection practices will be further strengthened by the widespread adoption of electronic health records, and will unlock the means for caregivers to improve patients' lives and for administrators to significantly reduce overhead and administration costs.