Annals of Health Law

Volume 19
Issue 1 *Special Edition 2010*

Article 38

2010

Breaking Down the Federal and State Barriers Preventing the Implementation of Accurate, Reliable and Cost Effective Electronic Health Records

Stephen J. Weiser
Meade & Roach LLP; Aegis Compliance & Ethics Center, LLP

Breaking Down the Federal and State Barriers Preventing the Implementation of Accurate, Reliable and Cost Effective Electronic Health Records

Stephen J. Weiser, J.D., LL.M.[*]

I. INTRODUCTION

Federal and state laws providing for written consent for re-disclosure of "sensitive health information" relating to mental health, HIV/AIDs, genetic information, and alcohol and substance abuse disorders results in substantial legal and economic barriers to the implementation of electronic health information exchange with respect to the creation of accurate and reliable electronic health records. Laws protecting sensitive health information also serve as a bar to the implementation of effective disease management programs and population-based studies that require the use of this electronic health information. The creation of a federal health care privacy law applicable to all states will eliminate such legal barriers and significantly reduce the costs of implementation of electronic health information exchanges. Increasing criminal and civil monetary penalties on the misuse of sensitive health information as well as bolstering the efforts of enforcement agencies will be required in order to address the concerns of individual and health care privacy advocates.

In a speech outlining his economic recovery plan, President Obama said, "We will make the immediate investments necessary to ensure that within five years all of America's medical records are computerized." The President has also stated that "digital medical records could prevent medical errors, save lives and create hundreds of thousands of jobs."[1] The American Recovery and Reinvestment Act of 2009 (ARRA) also invests $19 billion in computerized medical records that will help to reduce costs

[*] Meade & Roach, LLP, Aegis Compliance & Ethics Center, LLP. This article is dedicated to Max D. Brown, J.D., who has been my mentor. The comments and position are those of the author and in no way reflect the opinions of Meade & Roach, LLP and Compliance & Ethics Center, LLP.

1. Prescription Blog, http://prescriptions.blogs.nytimes.com/author/robert-pear/ (Jan. 17, 2009).

and improve quality while ensuring patients' privacy. In order to advance the use of technology in healthcare, the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of ARRA encourages hospitals and physicians to adopt an electronic health record (EHR)[2] system before the end of 2015. The act also provides funding for, among other things, an EHR infrastructure and technologies to allow for the electronic flow of information and the support of regional and sub-national efforts toward health information exchange.

The use of electronic health information, however, is not limited to health care providers. Another HITECH priority is the secondary use of electronic health record data research to identify strategies that enhance the use of health IT in improving the overall quality of health care, including both population health and clinical research, while protecting patient privacy.[3] For example, there has been a significant interest in the development of other types of electronic medical records by health insurers, including third party administrator and health management vendors in the Regional Health Information Organization (RHIO).[4] The RHIO is an organization that promotes the electronic exchange of patient information among participants. A RHIO generally consists of physicians, hospitals health plans, laboratories, consumers and others who seek to share electronic health information about patients in a community, state or region.[5] Support for EHRs and RHIOs will also come from HHS as a result of HITECH grants awarded to projects finding ways to improve electronic exchange and use of health information in a secure, private, and accurate manner while protecting patient privacy.[6]

II. THE HIPAA PRIVACY RULE AS A NATIONAL STANDARD PROMOTES ELECTRONIC HEALTH EXCHANGE

If the HIPAA Privacy Rule served as the uniform standard for health information privacy, the development of EHRs would flourish. The HIPAA Privacy rule established a set of basic national privacy standards that set a floor of ground rules for health care providers, health plans, and health care clearinghouses ("covered entities") in order to protect patients and

2. The term "electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

3. Advance For Health Information Executives, December 21, 2009.

4. Sheera Rosenfeld, Shannah Koss, and Sharon Siler, Avalere Health LLC, *Ihealthreports, Privacy Security and the Regional Health Information Organization* (prepared for California HealthCare Foundation) (2007).

5. *Id.*

6. *Id.*

encourage them to seek needed care.[7] Without consent or authorization, a covered entity or its business associate may use or disclose protected health information for its own treatment, payment[8] or health care operations.[9] The payment and health care operations identified by HIPAA include activities that may be more effectively accomplished through use of electronic medical records. Those activities include utilization review and concurrent and retrospective review of services. Other activities include conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment. Protected health information may be disclosed for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is for certain types of health care operations.

A. State and Federal Privacy Laws as EHR Barriers

State laws that are more stringent than HIPAA continue to apply due to the HIPAA Privacy Rules preemption requirements permitting stricter state laws to govern the release of health information.[10] Many states afford special statutory protection to certain diagnoses or conditions or "sensitive health information." In one survey, states identified those areas which provide the greatest challenge for the release of health information through an electronic data exchange.[11] The types of "sensitive health information" that states reported as challenging electronic data exchange programs are: mental health, substance abuse, HIV/AIDS, communicable diseases, genetic testing, and disability."[12]

---

7. Rules and Regulations, 65 Fed. Reg. 82,464 (Dec. 28, 2000).

8. *See* Definitions, 45 C.F.R. § 164.501 (Payment).

9. *See id.* (Health care operations).

10. 45 C.F.R. § 160.202. The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain healthplan reporting, such as for management or financial audits.

11. *State E-health Activities in 2007: Findings From a State Survey*, The Commonwealth Fund and National Governors Assn., Feb. 15, 2008 (hereinafter *State E-Health Activities*).

12. *Id.* States also reported other restrictions relating to other conditions including

Laws protecting "sensitive health information" have certain statutory restrictions in common. Specific individual written consents must reference the nature of the information being disclosed, the parties receiving the information, and the purpose of the disclosure. This requirement poses a problem under those circumstances in which the entity requesting consent does not know the identity of future vendors or business associates to whom sensitive health information will have to be disclosed. Specific statutory requirements also give the individual the right to revoke the consent at any time. Further, re-disclosure of such information to any third party also requires a separate written consent from the individual. It is this last requirement that presents the most significant barrier to the disclosure of sensitive health information by health plans and group health plans that wish to engage in electronic health care operations.

While mental health records are generally protected at a higher level of confidentiality than other health records, some states have gone further in restricting the use of mental health information by health insurers. For example, Massachusetts statutes specifically prevent Blue Cross Blue Shield (BCBS) of Massachusetts and commercial indemnity plans from releasing mental health information without advance written consent of the subscriber.[13] Massachusetts statutes prohibit the disclosure of all mental health medications, such as antidepressants, anti-anxiety agents, and antipsychotic medications, without additional patient consent.[14] HIV/AIDS and sexually transmitted diseases are another category with special privacy concerns. In addition, in regards to the protection of HIV/AID medical conditions, Massachusetts insurance regulations require health plans to obtain advance written consent for the release of any AIDS-related information, and a specific detailed consent form is mandated.[15] This requirement covers medications specific to combating HIV and prescriptions for antibiotics or other medications in dosages that are used only to treat AIDs-related conditions.[16]

In addition, state and federal laws provide additional protection to genetic information which may not be disclosed without the written consent of individuals.[17] Health Insurers may not use the information for a non-

health information relating to adolescents and school-based health information.

13. Lawrence K. Gottlieb, Elliot M. Stone, Diane Stone, Lynne A. Dunbrack & John Calladine, *Regulatory And Policy Barriers To Effective Clinical Data Exchange: Lessons Learned From Meds Info-ED*, 24 HEALTH AFFAIRS 1197, 1197-1204 (2005).

14. *State E-Health Activities*, *supra* note 11.

15. *Id.*

16. *Id.*

17. Pub.L. No. 110-233, 122 Stat. 881. For an example of a state law restricting disclosure of genetic information see Illinois Genetic Information Privacy Act: 410 ILCS 513/1, et seq.

therapeutic purpose as it relates to a policy of accident and health insurance. For underwriting, disclosures of genetic test information may not be made available to the health insurer, without individual specific written permission.[18]

Substance abuse and chemical dependency records require special consideration beyond what has been identified for mental health law and HIV/AIDS records. EHR systems must provide mechanisms that enable facilities to manage the extra layer of protections for this information required under federal regulations as well as many state laws. Release of these records requires special authorization clearly indicating the patient's consent. When released, these records must include a written statement prohibiting re-disclosure by the recipient.

B. Practical Implications for Covered Entities

Because many states require written consent for the re-disclosure of sensitive health information to any third party, including a covered entity's business associate, health care providers, health plans and group health plans may find that such laws provide significant barriers to the creation of an EHR that may be used for health care operations such as disease management programs.

In the implementation of a RHIO, a health insurer or third party payer consent form may be required for the release of sensitive health information. Given the "real-time" release of information by medical information systems, complying with State laws governing sensitive health information renders electronic health data exchange impossible.[19] Without a written consent, the transmitter of electronic health information must either obtain the consent of the individual for release of the specific sensitive health information or filter the information out of the exchange.

Filtering data has been used to address these regulatory barriers in the creation of EHRs. For example, one clinical data exchange used prescription claims data to deliver patient medication history to emergency department clinicians. The project established a drug list of more than 150 medications that could indicate the treatment of HIV/AIDS, mental health disorders, or substance abuse.[20] The resulting drug filter had to take into account sensitive drug information that varied because of the differences in which health plans interpreted state laws. A single filtered drug list had been a goal but would have resulted in defining a large "lowest common denominator" list, preventing the release of medication history that would be clinically useful.

18. *Id.*
19. Gottlieb et al., *supra* note 13.
20. *Id.*

Clinicians expressed concern that the sensitive drug filter would limit the usefulness of the data exchange. Specifically, they noted that information regarding mental health medications is both critical to medical decision making and often difficult to ascertain accurately from patients.[21] Furthermore, the data exchange could not alert the clinician that a sensitive drug was filtered, because this would violate the spirit, if not the letter, of the regulations.[22]

Data filtering also denigrates the integrity of RHIOs and other data cooperatives seeking to establish trends in health care as well as the implementation of disease management programs. In addition because an individual has the right to revoke an authorization to release records in writing or verbally, and institutions must have mechanisms to track and comply with this requirement.

III. PROPOSED SOLUTIONS

A. Federal Privacy Standards Governing Electronic Health Information Exchange

When the HIPAA Privacy Regulations were proposed numerous comments, particularly from plans and providers, argued that the proposed preemption provisions were burdensome, ineffective, or insufficient, and that complete federal preemption of the "patchwork" of state privacy laws is needed.[23] For example, in 2006, the unsuccessful H.R. 4157 bill would have created a Uniform Health Information Law and would allow HHS to pre-empt state privacy laws when deemed necessary in the interest of information sharing.

If the Obama administration or any subsequent administration wants to achieve the goal of accurate and reliable computerized medical records by 2015, then the federal government will have to resolve the limitations that State laws have placed on sensitive health information. Such a law would obviate the need for providers and payers to obtain a special consent to disclose sensitive health information for certain types of health care operations. For example, federal laws and regulations could establish a single consent that would allow for unlimited downstream releases of "sensitive health information" for certain purposes and clarify that the authorization can describe generally the entities to which the sensitive health information may be disclosed.

Of course, the health care advocacy community will require substantial

21. *Id.*
22. *Id.*
23. 65 Fed. Reg. 82,579 (Dec. 28, 2000).

assurance with respect to protecting the concerns of vulnerable individuals. One way to deal with the concerns of health care privacy advocates would be to impose greater statutory penalties on the misuse of sensitive health information, along with greater support for federal and state enforcement agencies. Criminal and civil penalties would need to be substantially increased to serve as a deterrent to the employer, health insurer, or health care provider that improperly uses of discloses sensitive health information.

B. State Level Solutions

Until there is a national health care privacy standard, it may be up to State legislatures to take steps to adopt changes to the laws governing sensitive health information for the purpose of improving the quality of care and the reliability of electronic health information exchange.

While the implementation of State level solutions does not appear to be practical, the Research Triangle Institute has suggested several state and multi-state approaches for updating state laws that apply to electronic health information exchange.[24] Proposed amendments to state law fell into three broach categories: amending state law to mirror federal law, amending state law to remedy state-specific concerns, and amending or drafting new state law to address consistency issues more broadly.[25] Despite the efforts to come up with state specific or multi-state solutions, it appears that adopting a federal standard is the most economically efficient and practical solution to consolidation of the maze of state and federal health care privacy laws aimed at the protection of sensitive health information.

24. Linda L. Dimitropoulos, Privacy and Security Solutions for Interoperable Health Information Exchange, (2007) *available at* http://www.rti.org/pubs/fip_execsumm.pdf.

25. *Id.*