



CRS Report for Congress

Electronic Personal Health Records

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

The Administration, Congress, foundations, and the private sector have undertaken various initiatives to promote the adoption of electronic health records (EHRs) as part of the national health information infrastructure. An electronic personal health record (EPHR) is a database of medical information collected and maintained by the individual patient. Commercial suppliers, health care providers, health insurers, employers, medical websites, and patient advocacy groups offer EPHRs. Congress has held hearings on electronic personal health records, and legislation has been introduced (S. 1456), ordered to be reported (H.R. 2406), and reported (S. 1693). Electronic personal health records are controversial among privacy advocates and patients, who are concerned about health information privacy and security, and misuse of individually identifiable health information. The extent to which electronic personal health records are protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule is discussed herein. This report will be updated.

Background. In 2004, the President and the Department of Health and Human Services (HHS) launched an initiative to make electronic health records available to most Americans within the next ten years, and to transform the health care system by lowering costs, reducing medical errors, and improving quality of care.¹ The President called on HHS to develop and implement a strategic plan to guide the nationwide implementation of health information technology that would, among other things, allow EHRs to be shared across healthcare systems and providers.² Many are concerned about the privacy and security of EPHRs; the potential for the exploitation of personal medical information

¹ Executive Order 13335: *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator*, (2004).

² *Health and Human Services and the National Coordinator for Health IT, The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care, Framework for Strategic Action* (July 21, 2004), [<http://www.hhs.gov/healthit/documents/hitframework.pdf>]; see GAO, *Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy*, GAO-07-238 (Washington, D.C.: Jan. 10, 2007).

by hackers, companies, or the government; and the sharing of health information without patients' knowledge or consent.³

Congress has held hearings on electronic health records,⁴ and legislation has been introduced to promote EPHRs. S. 1456 (Carper/Voinovich), the Federal Employees Electronic Personal Health Records Act of 2007, would require each carrier entering into a contract for a health benefits plan to establish and maintain electronic personal health records for individuals and family members enrolled in Federal Employee Health Benefits Plans. Health benefit plans would be required to comply with HIPAA privacy and security regulations and other relevant privacy and security laws. H.R. 2406 (Gordon) directs the National Institute of Standards and Technology (NIST) to increase its efforts in support of the integration of the healthcare information technology system and authorizes the Director of NIST to, among other things, focus on information management including electronic health records management. H.R. 2046 was ordered to be reported by the House Science and Technology Committee on October 24, 2007. S. 1693 (Kennedy), the Wired for Health Care Quality Act, would enhance the adoption of a nationwide interoperable health information technology system. S. 1693 was reported on October 1, 2007, by the Senate Committee on Health, Education, Labor, and Pensions (S.Rept. 110-187).

Philanthropies such as California Health Care Foundation, Robert Wood Johnson Foundation, the Markle Foundation, and many others have provided funding, leadership, and expertise to the EHR effort.⁵ Medical informatics, nursing informatics, and medical and nursing professional societies have also been involved.⁶ The private sector has been actively involved through the launch of tools and websites offering EPHRs.⁷

What Is an Electronic Personal Health Record (EPHR)? An electronic personal health record is a database of medical information collected and maintained by the individual patient.

In a personal EHR (PHR) model, patients are the dominant managers and custodians of their electronic medical records. The record consists of information fields into which data are entered either by the patient or through data export, or managed by the patient from records maintained by the patient's physician. One PHR model has patients subscribing to a web-based service that assists them in collecting data from

³ See, Health Privacy Project and Center for Democracy and Technology, *Letter to The Honorable Edward M. Kennedy, Chairman, Senate Committee on Health, Education, Labor and Pensions* (July 23, 2007), [http://www.healthprivacy.org/usr_doc/Wired_letter_7-23.pdf].

⁴ See, e.g., *Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative*: Hearing Before the Senate Subcomm. on Oversight of Gov't Management, the Federal Workforce, and the District of Columbia, 110th Cong. (Feb. 1, 2007).

⁵ See, Markle Foundation, *The Connecting for Health Common Framework: Overview and Principles*, [<http://www.connectingforhealth.org/commonframework/docs/Overview.pdf>].

⁶ American Health Information Management Association, American Medical Informatics Association, *The Value of Personal Health Records* (February 2007). Retrieved on 2007-10-09. [<http://www.ahima.org/dc/positions/documents/MicrosoftWord-AHIMA-AMIAPHRStatement-final2-2007.pdf>].

⁷ See, *How to Choose a PHR Supplier*, at [http://www.myphr.com/resources/phr_search.asp].

one physician and then disseminating it to others. The “Continuity of Care” record proposed by the American Academy of Family Physicians as a standardized form of summarized electronic records would be a convenient data model. With a fully personal EHR system, only the consumer can download, view, combine, or process all his records. Patients would then be able to choose which records or parts of records they would export. Exported records could be provided on a read-only basis, protecting against alteration or entry of additional material. Employers, hospital systems, and EMR vendors are also rolling out hybrid models that enable web-based access for patients to portions of their records for personal health monitoring. Future models could mimic personal financial management software such as Intuit’s Quicken or Microsoft’s Money. [citations omitted]⁸

Who Offers EPHRs? Various types of EPHRs are offered by commercial suppliers (e.g., Microsoft); health care providers (e.g., the Department of Veterans Affairs); the federal government (e.g., HHS); health insurers; employers (e.g., Wal-Mart); employer consortiums (e.g., Dossia Health Care); medical websites (e.g., WebMD); and patient advocacy groups for cancer patients, children with special health needs, adults with disabilities, and health and weight management patients.⁹

What Forms Are EPHRs Maintained In? An EPHR may be web-based or in a database created on the patient’s own computer. EPHRs are maintained in electronic mediums. Three types of electronic personal health records exist:

(1) a provider-owned and provider-maintained digital summary of clinically relevant health information made available to patients; (2) a patient-owned software program that lets individuals enter, organize and retrieve their own health information and that captures the patient’s concerns, problems, symptoms, emergency contact information, etc.; and (3) a portable, interoperable digital file in which selected, clinically relevant health data can be managed, secured and transferred.¹⁰

What Information Is Included in an EPHR. This varies widely and depends on the data elements in the EPHR. Information in an EPHR may include personal identification, including name and birth date; emergency contacts; names, addresses, and phone numbers of physicians, dentists, and specialists; health insurance information; living wills, advance directives, or medical power of attorney; organ donor authorization; a list and dates of significant illnesses and surgical procedures; current medications and dosages; immunizations and their dates; allergies or sensitivities to drugs or materials; important events, dates, and hereditary conditions in the family history; results from a recent physical examination; opinions of specialists; important test results; eye and dental

⁸ Terry, Nicholas P.; Francis, Leslie P., *Ensuring the Privacy and Confidentiality of Electronic Health Records*; 2007 U. Ill. L. Rev. 681, 721 (2007).

⁹ See, [<http://www.healthvault.com/>]; [<http://www.capmed.com/>]; [<http://www.iHealthRecord.com/>]; [<https://www.mymedicalrecords.com/login.jsp>]; [<http://www.myhealth.va.gov>]; [<http://www.hhs.gov/familyhistory/>]; [<http://www.drinet.com/bcbsa.htm>]; [https://members.kaiserpermanente.org/kpweb/jsp/feature/about/about_yourhealth.jsp]; [http://www.walmartfacts.com/FactSheets/Dossia_Health_Care.pdf]; [<http://www.dossia.org/home>]; and [<http://www.webmd.com/phr>].

¹⁰ See, American Academy of Family Physicians, *An Introduction to Personal Health Records*, available at [<http://www.aafp.org/fpm/20060500/57anin.html>].

records; correspondence between the patient and the provider(s); educational materials; and any other information the patient wishes to include.

How Is Information Entered into an EPHR? Commercial vendors “allow a patient to enter personal data into a record that is maintained by the web site,” whereas health care providers generally “permit an individual to read their medical record, review test results, and submit health information.”¹¹ The patient may add supplemental medical information to the EPHR (e.g., social history, reproductive history, sexually transmitted disease history, alternative treatments, appointments, claims data along with clinical care, pharmaceutical, and laboratory records).

With Whom Are EPHRs Shared? Each supplier may have different policies and practices regarding how they may use data they store for the individual. HIPAA-covered entities are required to provide a Notice of Privacy Practices describing the uses and disclosures that the covered entity is permitted to make for treatment, payment, and health care operations, a description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information (PHI), and a statement that other uses and disclosures will be made only with the individual’s written authorization. Non-HIPAA covered entities that offer EPHRs are not bound by the HIPAA Privacy Rule. Other laws may apply such as state medical confidentiality laws, federal and state consumer protection laws, federal and state unfair trade and deceptive practices laws, information security laws, Gramm-Leach-Bliley (when EPHRs are offered by financial institutions including insurance companies), state security breach notification laws, and contract law.

Are EPHRs Protected By the HIPAA? The HIPAA Privacy Rule and the HIPAA Security Rule are applicable to the privacy and security of EPHRs. HIPAA¹² was enacted primarily to “improve portability and continuity of health insurance coverage in the group and individual markets.”¹³ Part C of HIPAA¹⁴ requires the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.¹⁵ HIPAA-covered entities — health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically — are required to use standardized data elements and comply with the national standards.¹⁶ Failure to comply may subject the covered entity to civil or criminal penalties.

¹¹ Joy L. Pritts, *Health and the National Information Infrastructure and the NHII Personal Health Dimension*: Hearing Before the National Committee on Vital and Health Statistics before the National Health Information Infrastructure Workgroup, (Jan. 22, 2003), available at [<http://ihcrp.georgetown.edu/privacy/pdfs/prittsnvsh103002.pdf>].

¹² P.L. 104-191, 110 Stat. 1936 (1996), *codified in part* at 42 U.S.C. §§ 1320d *et seq.*

¹³ H.Rept. 104-496, at 1, 66-67, *reprinted* in 1996 U.S.C.C.A.N. 1865, 1865-66.

¹⁴ 42 U.S.C. §§ 1320d - 1320d-8.

¹⁵ 42 U.S.C. §§ 1320d-2(a)-(f). (National standards for transactions to enable the electronic exchange of health information, unique identifiers, code sets, security, electronic signatures, and transfer of information among health plans.)

¹⁶ 42 U.S.C. § 1320d-4(b).

HIPAA also addressed the privacy of individually identifiable health information and required adoption of a national privacy standard.¹⁷ HHS issued final Standards for Privacy of Individually Identifiable Health Information, known as the Privacy Rule, on April 14, 2003.¹⁸ The HIPAA Privacy Rule is applicable to health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically. The rule regulates protected health information that is “individually identifiable health information”¹⁹ transmitted by or maintained in electronic, paper, or any other medium.²⁰ The definition of PHI excludes individually identifiable health information contained in certain education records and employment records held by a covered entity in its role as employer.

The HIPAA Privacy Rule limits the circumstances under which an individual’s protected health information may be used or disclosed by covered entities. A covered entity is permitted to use or disclose protected health information without patient authorization for treatment, payment, or health care operations.²¹ For other purposes, a covered entity may only use or disclose PHI with patient authorization subject to certain exceptions.²² Exceptions permit the use or disclosure of PHI without patient authorization or prior agreement for public health, judicial, law enforcement, and other specialized purposes.²³ In certain situations that would otherwise require authorization, a covered entity may use or disclose PHI without authorization provided that the individual is given the opportunity to object or agree prior to the use or disclosure.²⁴

The HIPAA Privacy Rule also provides for accounting of certain disclosures;²⁵ requires covered entities to make reasonable efforts to disclose only the minimum information necessary; requires most covered entities to provide a notice of their privacy practices;²⁶ establishes individual rights to review and obtain copies of protected health information;²⁷ requires covered entities to safeguard protected health information from

¹⁷ HIPAA required a privacy standard that would address the rights of the subject of individually identifiable health information, the procedures established for the exercise of such rights, and authorized or required uses and disclosures of such information. P.L. 104 — 191, Title II, § 264, Aug. 21, 1996, 110 Stat. 2033, 42 U.S.C. § 1320d-2 (note).

¹⁸ 45 C. F.R. Part 164 Subpart E — Privacy of Individually Identifiable Health Information.

¹⁹ 45 C.F.R. § 160.103.

²⁰ See *South Carolina Medical Assoc. v. Thompson*, 327 F.3d 346 (4th Cir. 2003)(HIPAA could be interpreted to include non-electronic medical records).

²¹ 45 C.F.R. § 164.506.

²² 45 C.F.R. § 164.508.

²³ 45 C.F.R. § 164.512(a) - (l).

²⁴ 45 C.F.R. § 164.510.

²⁵ 45 C.F.R. § 164.528.

²⁶ 45 C.F.R. § 164.520.

²⁷ 45 C.F.R. § 164.524.

inappropriate use or disclosure; and gives individuals the right to request changes to inaccurate or incomplete protected health information.²⁸

The HIPAA Privacy Rule would govern the use and disclosure of the EPHR to the extent that the supplier of the EPHR is a HIPAA-covered entity and the information contained within the EPHR is “protected health information” as defined in the rule.²⁹ The rule defines a covered entity as health plans, health care clearinghouses, and health care providers who transmit certain transactions electronically. As noted above, a variety of suppliers offer EPHRs, some of which would be considered a “covered entity” for purposes of the rule.³⁰ Moreover, the information typically included within an EPHR would appear to consist of the kind of “individually identifiable health information” encompassed by the rule. As noted earlier, EPHRs generally include information collected from an individual that is created or received by a covered entity that relates to the individual’s health or condition, health care treatment or payment, and that identifies the individual. For example, information in an EPHR typically includes contacts, names, addresses, and phone numbers; health insurance information; advance directives; lists and dates of significant illnesses and surgical procedures; medications and dosages; immunizations; allergies; family history; physical examination results; opinions of specialists; tests results; eye and dental records; and correspondence. When the supplier of the EPHR is a HIPAA-covered entity, information in the EPHR would likely be deemed protected health information.

Where HIPAA does apply, supplemental personal information added by the individual to the EPHR would also become protected health information available for use or disclosure by the covered entity pursuant to the rule. Suppliers of EPHRs that are governed by the rule are permitted to use and disclose the EPHR for treatment, payment, and health care purposes without patient authorization. They are required to allow patients to request restricted use and disclosures of the EPHR. They are also required to obtain patient authorization to use or disclose the EPHR for many other purposes.

Note also that EPHRs provided by covered entities would also be subject to the HIPAA Security Rule. This rule requires covered entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information the covered entity creates, receives, maintains, or transmits. The purpose of the requirements is to protect against any reasonably anticipated threats or hazards to the security or integrity of such information, as well as to protect against any unauthorized uses or disclosures of such information.³¹

²⁸ 45 C. F.R. § 164.526

²⁹ *See supra* note 11.

³⁰ Commercial suppliers (*e.g.*, Microsoft and WebMd) and healthcare providers who do not bill electronically for their services, personal health records providers who provide services directly to patients, and regional health information organizations (RHIOs) are not considered “covered entities” and therefore would not be subject to the HIPAA Privacy Rule. *See* Kirk J. Nahara, *The Healthcare Privacy Debate Heats Up*, *The Privacy Advisor* 3 (Sep. 2007).

³¹ 45 C.F. R. Parts 160 and 164 (subparts A,C). *See* CRS Report RL34120, *Information Security and Data Breach Notification Safeguards*, by Gina Marie Stevens.