



Standard Specification for Relationship Between a Person (Consumer) and a Supplier of an Electronic Personal (Consumer) Health Record¹

This standard is issued under the fixed designation E2211; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ϵ) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This specification covers the relationship between a person (consumer), organization, or custodian (or other authorized representative) and a managing (storing) organization (such as a web site or other organization). However, web-based personal (consumer) health records that are created by health-care providers or health plans are not within the scope of this specification. Further, this specification will not address personal (consumer) health records (PCHR) that are created and managed by patients on paper records, on personal computers, or on other media offline.

2. Referenced Documents

2.1 Other References:

Internet Healthcare Coalition ²

Health on the Net (HON) ³

Federal Trade Commission FTC ⁴

Hi Ethics Alliance ⁵

MedCertain ⁶

American Medical Association Guidelines for Medical and Health Information Sites on the Internet ⁷

AHIMA E-health Tenets ⁸

URAC (also known as the American Accreditation HealthCare/Commission) ⁹

3. Terminology

3.1 Definitions:

3.1.1 *consumer*—the person who provides information to be stored by the personal (consumer) health record (PCHR) supplier.

3.1.2 *disclosure statement*—a prominent notice that describes an organization's policies in order to enable a person to decide whether (s)he can trust this organization with health information.

3.1.3 *Gramm-Leach-Bliley Act*—federal legislation enacted in 1999 as part of the Financial Services Modernization Act that specifies for web activities that “opt-out” is the norm.¹⁰

3.1.4 *individually identifiable health information*—information that is a subset of health information, including demographic information collected from an individual, and that: (1) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and (3) that identifies the individual; or (4) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. **HIPAA¹¹**

3.1.5 *patient health record (PHR)*—the primary legal record created and maintained by the healthcare provider documenting the healthcare services provided to a person, in any aspect of healthcare delivery. This term is synonymous with medical record, health record, patient care record (primary patient care record), client record, and resident record. The term includes routine clinical or office records, records of care in any health-related setting, preventive care, wellness, lifestyle evaluation, research protocols, special study records, and various clinical databases. The records may be in paper-based or electronic form.

3.1.6 *personal (consumer) health record (PCHR)*—an electronic application through which individuals can maintain and manage their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment that allows the individual or other authorized persons to access and share such information.

¹ This specification is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.25 on Healthcare Data Management, Security, Confidentiality, and Privacy.

Current edition approved May 10, 2002. Published August 2002. DOI: 10.1520/E2211-02.

² <http://www.ihealthcoalition.org/>

³ <http://www.hon.ch/HONcode/Conduct.html>

⁴ <http://www.ftc.gov/reports/privacy3/fairinfo.htm>

⁵ <http://www.ihealthcoalition.org/ethics/ethics.html>

⁶ <http://www.medcertain.org/>

⁷ <http://www.ama-assn.org/ama/pub/category/1905.html>

⁸ www.ahima.org

⁹ www.urac.org

¹⁰ For a summary of the act, see www.senate.gov/~banking/conf/grmleach.htm.

¹¹ Information on legislation and standards can be found at <http://aspe.hhs.gov/admnsimp>.

3.1.7 *personal (consumer) health record (PCHR) supplier*—the company or organization that maintains or manages, or both, the personal (consumer) health record (PCHR) online service.

3.1.8 *personal identifiable information (PII)*—individually identifiable information about an individual collected online, including: (1) a first and last name; (2) a home or other physical address, including street name and name of a city or town; (3) an e-mail address or other online contact information, including but not limited to an instant-messaging user identifier, or a screen name that reveals an individual’s e-mail address; (4) a telephone number; (5) a Social Security number; (6) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or (7) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

COPPA¹¹

NOTE 1—This standard is based on the current Gramm-Leach-Bliley Act which specifies “opt-out” as the standard for e-commerce (and e-health) in the United States. The alternative of “opt-in” was considered for this standard but has not been adopted because it would not conform to current e-health legal considerations, practices, and accepted industry thinking.

4. Significance and Use

4.1 The purpose of this standard is to provide guidance to consumers, suppliers of PCHR applications, and the public at large regarding the PCHR. Because the PCHR is distinct from the provider-based PHR, the laws and conventions for provider-based patient health records may not apply to the PCHR.

5. Terms and Conditions

5.1 The PCHR supplier shall allow a consumer or other authorized individual easy access at any point in the PCHR application to the policies and standards to which the PCHR supplier site adheres, as well as their associated charges, if any.

6. Privacy, Security, and Confidentiality Notice/ Awareness / Disclosure of Policies

6.1 The PCHR supplier shall disclose its policies for establishing authorization to create, maintain, or access a PCHR for an individual other than the consumer and its policy for allowing the consumer to rescind such authorization by clearly identifying:

6.1.1 The entity collecting the data (PCHR supplier);

6.1.2 The uses to which the data will be put;

6.1.3 The recipients of the data; and

6.1.4 The steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data.

6.2 The PCHR supplier shall also identify applicable consumer rights, including any choice respecting the use of the data, the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.

6.3 Such a disclosure shall be clearly stated, shall be posted in a prominent location, and shall be readily accessible from both the site’s home page and any Web page where information is collected from the consumer. It gives consumers meaningful and effective notice of what will happen to the personal information they divulge.

6.4 The PHR supplier shall state its policies regarding its sharing and use of information from an individual’s PHR (for example, are there any conditions under which individually identifiable information is made available to or used by third parties?). PCHR suppliers shall also state their policies regarding access to the consumer’s PHCR by others than the consumer, for example, how a child’s record is handled when the child reaches the age of majority, and how an individual gains authorization to serve as custodian to a parent’s record when that parent is no longer competent to do so himself or herself.

6.5 Choice/Consent:

6.5.1 The PCHR contains both personal identifier information (PII) and individually identifiable health information (IIHI). The standard for PII is generally used as opt-out, meaning that a consumer must specifically request that such information is not shared.

6.5.2 For IIHI, PCHR suppliers shall allow consumers to choose if and how any personally identifiable information collected from them may be used. These choices shall be presented in a manner requiring that the consumer give specific permission for use of such data. Options for secondary uses of information shall be provided, that is, uses beyond the PCHR storage and management application. Such secondary uses may be internal, such as placing the consumer on a sponsor’s or other organization’s mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

6.6 Access/Corrections:

6.6.1 A PCHR supplier shall provide the consumer with the ability to access data within the PCHR in order to verify its correctness or to contest its accuracy and completeness, or both. Access policies shall describe the turnaround time related to such requests (time from request to access), shall specify associated charges, and shall include instructions for contesting and correcting inaccurate or incomplete data.

6.6.2 The PCHR supplier shall disclose its policies regarding when and how the PHR data may be accessed. In particular, a PCHR supplier shall provide instructions for the consumer on how to get a copy.

6.7 *Integrity*—A PCHR supplier must be able to assure data integrity through audit trails and other security methods and shall disclose its quality assurance policies regarding maintenance of data integrity. PCHR information must be captured following defined procedures and must be stored in such a way that it cannot be tampered with or distorted. A PCHR supplier’s policies shall describe how additions, deletions, and updates to PCHR data may be made and by whom (for example, what data is a consumer allowed to delete or modify and what data is a consumer’s healthcare provider allowed to delete or modify?).