

Guidance for Identifying Designated Record Sets under HIPAA Version 2

**Prepared by the
NCHICA Designated Record Sets Work Group
Privacy and Confidentiality Focus Group**

**Approved for Public Distribution
February 3, 2003**

**Endorsed by the North Carolina
Health Information Management Association**

Introduction

Patient rights in the healthcare industry has been a critical issue for several decades and continues to be a major issue addressed by both state and federal governments. One such right that the public has insisted upon is their right to access their own health information and amend health information when it is determined to be incorrect. In response to these concerns, federal regulations have been established which mandate the patient's right to access and amend his/her health information. These rights to access and amendment however are limited to health information contained in 'designated record sets' as identified by the health care provider or health plan.

Purpose and Scope

The purpose of this guidance document is to provide information that will aid health care providers and health plans in identifying groups of records called "designated record sets" that patients have the right to access and amend.

It is not the intention of this guidance document to address the process for handling patient requests related to access and amendment of health information. Guidance documents related to access and amendment are available in Practice Briefs published by the American Health Information Management Association (<http://www.ahima.org/journal/pb.html>) and a white paper published by WEDI-SNIP (<http://snip.wedi.org/public/articles/index.cfm?Cat=17>).

Designated Record Sets

Background

The U.S. Department of Health and Human Services (HHS) issued the final Privacy Rule, authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), on December 28, 2000¹. The Privacy Rule became effective on April 14, 2001, and compliance with the rule is required by April 14, 2003. On March 27, 2002, HHS issued a Notice of Proposed Rule Making that included proposed modifications to the final Privacy Rule. Modifications to the final rule were published on August 14, 2002 and they became effective on October 15, 2002. Compliance with the modifications is required by April 14, 2003. The Privacy Rule creates national standards to protect individuals' personal health information and gives patients increased access to their medical records.

The charge of the Designated Record Sets Subcommittee² was to analyze the provisions in the Privacy Rule related to access and amendment standards³ and to develop criteria for health care providers and health plans to use in identifying their designated record sets.

Definitions

Designated record set means:

- (1) A group of records maintained by or for a health plan or health care provider, that is:

¹ 45 C.F.R. Parts 160 and 164

² The NCHICA Designated Records Set Subcommittee members are: Sarah Brooks, MPA, RHIA (North Carolina Department of Health and Human Services); Jean Foster, RHIA (Pitt County Memorial Hospital); Cassina Hunt, RHIA (First Health Moore Regional Hospital). Endorsement review by the North Carolina Health Information Management Association done by Cornelia L. McClure, RHIA, CCS. Version 2 changes were made based upon input from Aimee N. Wall, UNC Institute of Government.

³ 45 C.F.R. §164.524 and 164.526

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/default.asp> and which is available from NCHICA upon request.

- (i) The medical records and billing records about individuals maintained by or for a **covered health care provider**;
 - (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a **health plan**; or
 - (iii) Used, in whole or in part, by or for the health plan or health care provider to make decisions about individuals.
- (2) For purposes of this definition, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a health plan or health care provider.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - (i) That identifies the individual; or
 - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information:

- (1) Includes individually identifiable health information that is:
 - (i) Transmitted by electronic media;
 - (ii) Maintained in the internet, extranet, leased lines, dial-up lines, private networks and those transmissions that are physically moved from one location to another using magnetic tape, disk or compact disk media; or
 - (iii) Transmitted or maintained in any other form or medium.
- (2) Excludes individually identifiable health information in:
 - (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g including records described at 20 U.S.C. 1232g(a)(4)(B)(iv) as follows:
 - (1) of students who are 18 years or older or are attending post-secondary educational institutions,
 - (2) maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity,
 - (3) that are made, maintained, or used only in connection with the provision of treatment to the student, and
 - (4) that are not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student.
 - (ii) Employment records held by a health plan or health care provider in its role as employer.

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Implementation Considerations

- 1) When are Designated Record Sets addressed in the Privacy Rule?
 - a) Right of Access
 - i) The final Privacy Rule provides individuals with a right of access to their protected health information. An individual has a right of access to inspect and obtain a copy of his/her protected health information in a designated record set (as identified by the organization) for as long as the health plan or health care provider maintains the protected health information.
 - ii) Appendix A contains the Privacy Rule that addresses right of access and all references to “designated record set(s)” have been highlighted.
 - b) Right to Amend
 - i) The final Privacy Rule provides individuals with a right to amend their protected health information. An individual has the right to request a health plan or health care provider amend protected health information in a designated record set (as designated by the organization), for as long as the health plan or health care provider maintains the protected health information.
 - ii) Appendix B contains the Privacy Rule that addresses right to amend and all references to “designated record set(s)” have been highlighted.
 - c) When identifying designated record sets, covered entities should consider the definition of ‘designated record sets’ only – not the circumstances under which a covered entity may deny a request for access or amendment. Once designated record sets are identified, covered entities must establish policies and procedures for denying access/requests for amendment of designated record sets. The Privacy Rule permits covered entities to deny an individual’s request for access or amendment under certain circumstances but denial is optional; therefore, any records that meet the definition of ‘designated record set’ must be included in a covered entity’s designation.
- 2) What type of information should be considered as Designated Record Sets?
 - a) Health information created and/or maintained by a health care provider. The following health information should be considered when specifying health care provider designated record sets:
 - i) Medical Records –
 - (1) Specify what constitutes the medical record in your organization (e.g., paper records stored in medical record folders maintained in Health Information Management Department; active medical records utilized by health care staff prior to client discharge).
 - (2) If your organization utilizes an electronic medical record for all or parts of the medical record, specify if the designated record set is the automated system or a copy produced from the automated system.
 - (3) Specify if copies of records from other health care providers will be included as part of the medical record designated record set. The following options should be considered.
 - (a) May want to specify they are part of the designated record set for access only.
 - (b) Individuals need to go to the source of the information to request amendments.
 - ii) Financial Records –

For the following, specify if the Designated Record Set is the automated system or a report produced by an automated system.

 - (1) Remittance advices and records of payments

- (2) Patient Statements
- (3) Claim Forms
- (4) Claims Adjudication records

- b) Health information created and/or maintained by a health plan including:
 - i) Eligibility information
 - ii) Enrollment records
 - iii) Record of claims submitted to or received by Health Plans
 - iv) Case or medical management records
 - c) Other records used by Health Plans and Health Care Providers to make decisions about individuals such as:
 - i) Raw test data from psychological tests
 - ii) Audiotapes (e.g., dictation tapes, taped sessions with patients/family that would not be considered psychotherapy notes)
 - iii) Psychotherapy notes (as defined)
 - iv) Videos/photographs of patients used for teaching purposes
 - v) Telemedicine
 - vi) Coding Worksheets
 - vii) Utilization Review Worksheets
 - viii) X-ray film
 - ix) Working notes summarized and dictated into the medical record
 - d) Health information specifically created and/or maintained by Business Associates when acting on behalf of your organization, as specified in a Business Associate Agreement.
 - i) For example, billing records maintained by a private billing service
 - ii) Do not include duplicative information that is also maintained by the health plan or health care provider
 - e) Health information in all types of media when such information is created and/or maintained for the purpose of making decisions about individuals
 - i) Paper
 - ii) Oral
 - iii) Video
 - iv) Electronic
 - v) Film
 - vi) Digital
 - f) "Legal Health Records" – Appendix C contains an excerpt of information published in the Journal of the American Health Information Management Association, Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." Journal of AHIMA 72, no.9 (2001): 88A-H. This information may prove useful as organizations define their designated record sets.
- 3) What type of information should NOT be in a Designated Record Set?
- a) Health information that is not used to make decisions about individuals.

- b) Copies of reports/documentation/forms wherein the originals are maintained in an 'official' record maintained by the organization
 - i) Copies produced from original records maintained by the organization should be limited and should not be disclosed outside the health plan or health care provider.
 - ii) Copies of health information that are maintained in more than one location must be protected but only the original document should be included in a designated record set.
 - iii) If the same protected health information is maintained in more than one location, the health plan or health care provider is required to produce the information only once.
 - c) Quality Improvement records
 - d) Risk Management records (including Incident Reports)
 - e) Cancer Registry information
- 4) What type of documentation is needed for identification of Designated Record Sets?
- a) Organizations must document the designated record sets that are subject to access by individuals. Documentation could include:
 - i) Type of record (e.g., medical record; X-ray films; hospital information system; account receivables).
 - ii) Basic content (e.g., demographics; assessments; diagnosis; billing claims data).
 - iii) Location of the record set (e.g., medical record department; business office; radiology).
 - iv) Specify any information in a designated record set that the patient will not have a right of access to or amendment of. When possible, provide a written indication (such as stamped statement) on each page that is not part of the designated record set. For example, the policy may state that the medical record is a designated record set with the following exceptions – pages stamped with "Not Part of Designated Record Set", Correspondence, Attestation Sheet, Coding Worksheet, Records from other agencies.
 - b) Organizations must document the titles of the persons or offices responsible for receiving and processing requests for access by individuals (e.g., Privacy Officer).
 - c) Organizations should maintain a system for tracking requests for access and/or amendment that includes the designated record set(s) included in the request.

Appendix A – HIPAA Privacy Rule

§ 164.524 Access of individuals to protected health information

§ 164.524 Access of individuals to protected health information.

(a) Standard: access to protected health information.

(1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42

U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) Unreviewable grounds for denial. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered healthcare provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered healthcare provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health

care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) Implementation specifications: requests for access and timely action.

(1) Individual's request for access. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) Timely action by the covered entity.

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) Implementation specifications: provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) Form of access requested.

(i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an

explanation of the protected health information to which access has been provided, if:

- (A) The individual agrees in advance to such a summary or explanation; and
- (B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) Time and manner of access. The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

- (i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;
- (ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
- (iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

(d) Implementation specifications: denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) Denial. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

- (i) The basis for the denial;
- (ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and
- (iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in §164.530(d) or to the Secretary pursuant to the procedures in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(3) Other responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by §164.530(j):

- (1) The designated record sets that are subject to access by individuals; and
- (2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Appendix B – HIPAA Privacy Rule

§ 164.526 Amendment of protected health information

§164.526 Amendment of protected health information.

(a) Standard: right to amend.

(1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

- (i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
- (ii) Is not part of the designated record set;
- (iii) Would not be available for inspection under §164.524; or
- (iv) Is accurate and complete.

(b) Implementation specifications: requests for amendment and timely action.

(1) Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) Timely action by the covered entity.

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) Implementation specifications: accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/default.asp> and which is available from NCHICA upon request.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

- (i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and
- (ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) Implementation specifications: denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

- (i) The basis for the denial, in accordance with paragraph (a)(2) of this section;
- (ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
- (iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
- (iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in §164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosures.

(i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) Implementation specification: actions on notices of amendment. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must

amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) Implementation specification: documentation. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by §164.530(j).

Appendix C - Guidelines for Defining the Health Record for Legal Purposes

<p><u>Legal Health Record</u></p> <p><i>The legal business record generated at or for a healthcare organization. This record would be released on request.</i></p>	<p>The LHR is the documentation of the healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare provider organization. The LHR is individually identifiable data, in any medium, collected and directly used in and/or documenting healthcare or health status. The term includes records of care in any health-related setting used by healthcare professionals while providing patient care services, for reviewing patient data, or documenting observations, actions, or instructions. Some types of documentation that comprise the legal health record may physically exist in separate and multiple paper-based or electronic/computer-based databases (see examples listed below).</p> <p>The LHR excludes health records that are not official business records of a healthcare provider organization (even though copies of the documentation of the healthcare services provided to an individual by a healthcare provider organization are provided to and shared with the individual). Thus, records such as personal health records (PHRs) that are patient controlled, managed, and populated would not be part of the LHR.</p> <p>Copies of PHRs that are patient owned, managed, and populated by the individual but are provided to a healthcare provider organization(s) may be considered part of the LHR, if such records are used by healthcare provider organizations to provide patient care services, review patient data, or document observations, actions, or instructions. This includes patient owned, managed, and populated "tracking" records, such as medication tracking records and glucose/insulin tracking records.</p> <p><i>Examples of documentation found in the LHR:</i></p> <ul style="list-style-type: none"> • advance directives • anesthesia records • care plan • consent for treatment forms • consultation reports • discharge instructions • discharge summary • e-mail containing patient-provider or provider-provider communication • emergency department record • functional status assessment • graphic records • immunization record • intake/output records • medication orders • medication profile • minimum data sets (MDS, OASIS, etc.) • multidisciplinary progress notes/documentation • nursing assessment • operative and procedure reports • orders for diagnostic tests and diagnostic study results (e.g., laboratory, radiology, etc.) • patient-submitted documentation • pathology reports • practice guidelines or protocols/clinical pathways that imbed patient data • problem list • records of history and physical examination • respiratory therapy, physical therapy, speech therapy, and occupational therapy records • selected waveforms for special documentation purposes • telephone consultations • telephone orders
---	---

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/default.asp> and which is available from NCHICA upon request.

<p><u>Patient-Identifiable Source Data</u></p> <p><i>An adjunct component of the legal business record as defined by the organization. Often maintained in a separate location or database, these records are provided the same level of confidentiality as the legal business record. The information is usually retrievable upon request. In the absence of documentation (e.g., interpretations, summarization, etc.), the source data should be considered part of the LHR.</i></p>	<p>Patient-identifiable source data are data from which interpretations, summaries, notes, etc., are derived. Source data should be accorded the same level of confidentiality as the LHR. These data are increasingly captured in multimedia form. For example, in a telehealth encounter, the videotape recording of the encounter would not represent the LHR but rather would be considered source data.</p> <p>Examples of patient-identifiable source data:</p> <ul style="list-style-type: none"> • analog and digital patient photographs for identification purposes only • audio of dictation • audio of patient telephone call • diagnostic films and other diagnostic images from which interpretations are derived • electrocardiogram tracings from which interpretations are derived • fetal monitoring strips from which interpretations are derived • videos of office visits • videos of procedure • videos of telemedicine consultations
<p><u>Administrative Data</u></p> <p><i>While it should be provided the same level of confidentiality as the LHR, administrative data are not considered part of the LHR (such as in response to a subpoena for the "medical record.")</i></p>	<p>Administrative data are patient-identifiable data used for administrative, regulatory, healthcare operations, and payment (financial) purposes.</p> <p>Examples of administrative data:</p> <ul style="list-style-type: none"> • authorization forms for release of information • birth and death certificates • correspondence concerning requests for records • event history/audit trails • patient-identifiable claim • patient-identifiable data reviewed for quality assurance or utilization management • patient identifiers (e.g., medical record number, biometrics) • protocols/clinical pathways, practice guidelines, and other knowledge sources that do not imbed patient data
<p><u>Derived Data</u></p> <p><i>While it should be provided the same level of confidentiality as the LHR, derived data are not considered part of the LHR (such as in response to a subpoena for the "medical record.")</i></p>	<p>Derived data consists of information aggregated or summarized from patient records so that there are no means to identify patients.</p> <p>Examples of derived data:</p> <ul style="list-style-type: none"> • accreditation reports • anonymous patient data for research purposes • best practice guidelines created from aggregate patient data • MDS report • OASIS report • ORYX report • public health records • statistical reports

Appendix C citation:

Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." Journal of AHIMA 72, no.9 (2001): 88A-H.

Table reprinted with permission from the American Health Information Management Association. Copyright© 2002 by the American Health Information Management Association. All rights reserved. No part of this table may be reproduced, reprinted, stored in a retrieval system, or transmitted, in any form or by any means, electronic, photocopying, recording, or otherwise, without the prior written permission of the association.

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/default.asp> and which is available from NCHICA upon request.