

HIPAA “Access” Issues

Nebraska SNIP Privacy Workgroup

May 5, 2001

Alex M. (Kelly) Clarke

**Baird Holm Law Firm
1500 Woodmen Tower
Omaha, Nebraska 68102-2068
Phone: 402.636.8204
E-mail: aclarke@bairdholm.com**

HIPAA “Access” Issues

Nebraska SNIP Privacy Workgroup May 5, 2001

Alex M. (Kelly) Clarke

A. INTRODUCTION

1. **HIPAA is not Just Privacy.** HIPAA places substantial new rights in the hands of individuals about whom individually identifiable health information is gathered, exchanged and used.

- a. State Law precedent – 71-8401 to 71-8404. Other statutes related to specific types of licensed entities.
- b. Common law – The data belongs to the patient; the “record” belongs to the provider.
 - General recognition of patient access.
 - Limited recognition of therapeutic privilege – *Reserve Life Insurance Co. v. Bishop Clarkson Memorial Hospital.*
- c. Concept is not new – but approach and mechanics are.

2. **Covered Issues.** A study of HIPAA “access” issues involves the following topics:

- a. “*Designated record sets*” – The form and type of data that can be accessed and amended.
- b. The patient’s right to *inspect and obtain copies* of PHI maintained in designated record sets in the hands of (i) health care providers and health plans; (ii) health care clearinghouses; and (iii) business associates.
- c. The patient’s right to *amend* data maintained in designated record sets in the hands of (i) health care providers and health plans; and (ii) health care clearinghouses; and (iii) business associates.
- d. The patient’s right to an accounting of certain disclosures by covered entities and business associates.
- e. Effect of preemption and the interplay of HIPAA and Nebraska Law. Nebraska Law recognizes many of the same rights. How is Nebraska’s treatment different, and what rule applies in each case?

f. Mechanisms and safeguards to deal with patient access issues.

- Relationship to Notice of Privacy Practices.

- Covered entity response to HIPAA mechanics:

Receive requests	Record decisions
Put limits on requests	Retain results
Process requests	Verify identities
Act on requests	Communicate results
Resolve disputes	“Channel”

g. Checklist of policies. The area is policy rich. Covered entities and business associates need policies in place in advance, tied to Notice of Privacy Practices.

B. **DESIGNATED RECORD SETS**

1. **Significance.**

a. The right to inspect and copy is limited to info in designated record sets.

b. The right to amend is limited to info in designated record sets.

c. The obligation to produce or amend exists only so long as data is maintained in designated record sets.

d. **HOWEVER** – Data used to make decisions about individuals are to be put into designated record sets. Thus, all protected health information used to make decisions about individuals becomes a designated record set, whether or not you know it.

2. **Defined.** Section 164.501 sets forth the regulatory definition:

“(1) A group of records maintained by or for a covered entity that is:

(i) The medical record 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 covered entity to make decisions about individuals.

(2) For purposes of this paragraph, 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 covered entity.”

3. **Identifying Your Designated Record Sets.**

a. Providers and health plans – start with the listed records. These are not inclusive listings.

- Note – It is to your advantage to have listed the commonly understood compilations, because 99% of patients will ask for or about *them*.

b. This is a big issue.

- “[I]t is desirable that the category of records covered [as designated record sets] be readily ascertainable by the covered entity.” (65 Fed. Reg. 82606)

- The “other” category includes “categories of records . . . that are normally used and are reasonably likely to be used, to make decisions about individuals.” (*Id.*)

- Not limited to records used to make *health care* decisions about individuals, because other decisions (such as financial decisions) can “significantly affect individuals’ interests.” (*Id.*)

- Theme – “we believe individuals should have the right to access any protected health information that may be used to make decisions *about them . . .*” (*Id.* at 82605)

c. DRS not limited to records about an individual (although individual access may be). DRS includes records used or likely to be used to make decisions *about individuals*.

- Pharmacy committee study/minutes.
- Surgery department study.
- QI/peer review records.
- Health plan payment adjudications.

4. **Conclusion.** Impossible to reconcile the various HHS statements into a rule that gives simple and manageable meaning to the term.

- a. All data used to make decisions about individuals = designated record sets, whether you call it such or not.
- b. All records used to make decisions about groups of individuals or other individuals = designated record sets, but may not be accessible by individuals.
- c. By defining and categorizing their own version of “designated record set” most covered entities will preempt patients from going on wide-ranging searches most of the time.
 - “We have your medical record.”
 - “We have your claims adjudication record.”
- d. Covered entities need to require that information used to make decisions about individuals is routinely placed into a *named* grouping of data included in the list of designated record sets.

C. **INDIVIDUAL’S RIGHT TO INSPECT AND OBTAIN COPIES**

1. **Scope and Limitations.**

- a. An individual’s right to access and copy his/her own protected health information is an exception to the usual requirement for consent, authorization or opportunity to object.
- b. The right is not absolute – limited by therapeutic privilege, timeframes, copying fees, and certain express exceptions.

2. **Right of Access.** Subject to three categories of *exception*, an individual has the right to inspect and obtain a copy of PHI about the individual *in a designated record set*.

3. **Exceptions.** There are three types of exception to this right –

- a. Exceptions in the granting clause itself:
 - Psychotherapy notes.
 - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
 - Certain information covered by CLIA to which access is prohibited by law.

(§ 164.524(a)(1)).

b. Discretionary exceptions that are *nonreviewable* – that is, the individual cannot contest or required dispute resolution at the covered entity.

- Exceptions in the granting clause described above.
- PHI about “inmates” in a correctional institution or a health care provider acting under the direction of a correctional institution if disclosing the PHI “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.”
- Information concerning research when the treatment is rendered as part of an ongoing research project and the institution has informed the individual in advance.
- Records which are subject to and may be excluded by operation of the Privacy Act, 5 U.S.C. § 552(a).
- PHI obtained from someone other than a health care provider “under a promise of confidentiality” where granting access would be reasonably likely to “reveal the source of the information.”

(§ 164.524(2)).

c. Discretionary exceptions for which the individual is entitled to a review – and the CE is obligated to have a review mechanism.

- Therapeutic privilege for the protection of the patient or another individual.
- PHI that refers to other persons (other than health care providers) if release is “reasonably likely to cause substantial harm to such other person.”
- Request by an individual’s “personal representative” where release is “reasonably likely to cause substantial harm to the individual or another person.”
- Standard – to invoke these discretionary exceptions, “*a licensed health care professional*” must determine “*in the exercise of professional judgment*” that the listed grounds exist.

4. **Duration of the Right of Access**. The right exists for so long as the covered entity maintains the information in a designated record set. We think that means – for so long as the covered entity maintains the information and it meets the definition of designated record set.

5. **Review Mechanism.** For reviewable denials, the individual has the right to have the denial reviewed “by a licensed health care professional who is designated by the CE to act as a reviewing official and who did not participate in the original decision to deny.”

- Decision of the reviewer is final as to both parties.
- Individual has no right to “appeal” within the covered entity.

6. **Time Limits.** The covered entity must act within the following timeframes:

a. *Within 30 days* –

- If it grants the request, it must inform the individual that it accepts the request and provide the access requested.
- If it denies the request (in whole or in part) it must give the individual a *written denial*.

b. *Within 60 days* – Grant or deny access for records that are not maintained or accessible to the covered entity on site.

c. *30 day extension* – A provider unable to take an action within the stated time limit is entitled to a one-time 30 day extension – but must furnish the individual with a *written statement of the reasons* for the delay and the date by which it will complete its action.

7. **Form.** The covered entity must produce the requested information in the form or format requested by the individual (presumably in a designated record set) “if it is readily producible in such form or format” or, if not, in a readable hard copy or such other form as may be agreed to between the covered entity and the individual.

a. If the same requested information appears in multiple designated record sets, it only needs to be produced in one of them.

b. If the requested PHI is available at multiple locations, it only needs to be produced once in response to a request. However, an individual can make any number of requests for PHI.

8. **Time and Place.** The covered entity must arrange with the individual for a *convenient time and place* to inspect or obtain a copy, or mail the copy at the individual’s request.

- Probably means convenient to the individual, not the entity.
- Issue – non-business hour reviews versus mailings.

9. **Fees.**

a. No handling or retrieval fee is permitted, notwithstanding the Nebraska statutory limit of \$20 per record.

b. CE can charge a cost-based copying fee provided it can document the costs and justify the types of costs allocated to copying. This can include the cost of supplies and the labor of copying (but not handling or retrieval), and presumably any other costs reasonably allocated (and supported through documentation) to the *copying* function.

- There are no real dollar limitations on what the copying cost can be under HIPAA.
- State Law imposes maximum .50¢ per page limit.

c. Postage.

d. Pre-agreed cost of preparing an explanation or summary.

e. Cost limits not applicable to copies prepared for person other than the individual or his/her representative.

10. **Documentation.** A covered entity must document and retain for 6 years the following:

a. The “designated record sets” that are subject to access by individuals. This is where the entity gets to name and identify them.

b. The titles of persons or offices responsible for receiving and processing requests for access by individuals.

c. The covered entity should document and retain the basis for constructing the cost-based copying fees and any other fees properly chargeable to the individual.

D. AMENDMENT OF PROTECTED HEALTH INFORMATION

1. **The Individual’s Right to Amend.** An individual has the right –

a. to require a *covered entity* to amend . . .

b. PHI or a record *about the individual* . . .

c. in a designated record set . . .

d. for as long as the PHI is maintained in the designated record set.

e. The covered entity retains the right to make the final decision, but must follow the stated process.

f. The scope of covered information is the same as for individual access to information. Thus, information (such as psychotherapy notes) which are not subject to individual access would not be subject to a request for amendment.

(§ 164.526).

2. **Denial of Amendment.** A CE may deny the request to amend under certain circumstances.

a. *Grounds for Denial* –

- If the information was not created by the covered entity (unless the individual provides a reasonable basis to believe the originator is no longer available to act on the requested amendment);
- The information to be amended “is not part of a designated record set”;
- The disputed information is information that would not be available for inspection under the access rule; or
- The information is “accurate and complete.”

b. *Notice* – If the covered entity denies the request to amend, it must give the individual written notice in plain language containing the following:

- The basis for the denial.
- Notice of the individual’s right to submit a written statement disagreeing with the denial and an explanation of how to do so. The covered entity may “reasonably” limit the length of a statement of disagreement and may prepare a written rebuttal. If it prepares a statement of rebuttal, it must furnish a copy to the individual.
- A statement that, even if the individual does not submit a statement of disagreement, he or she may request the covered entity to furnish the individual’s request for amendment and the covered entity’s denial with any future disclosures of the protected health information.
- A description of the covered entity’s internal complaint process and a description of how to complain to the Secretary.
- The name or title and the telephone number of the covered entity’s contact person designated to receive the complaint.

c. *Identifying Records* – The covered entity must identify the record or PHI that is the subject of the disputed amendment “*and append or otherwise link the following information to the designated record set*”:

- The request for amendment.
- The denial.
- The individual’s statement of disagreement (if any).
- The covered entity’s rebuttal (if any).

d. *Future Disclosures* – If the individual submits a written statement of disagreement, all of the appended or linked information (or an accurate summary of it) must be included *with any subsequent disclosure of the PHI*.

- Note – not just future disclosures of the designated record set, but any disclosure of the disputed information in any form.
- Would include disclosure of the PHI and of dozens of different designated record sets which might not have been discussed with the individual.
- No exception for treatment, payment or health care operations.

3. **Timely Action**. A CE has 60 days to act. Action consists of granting the requested amendment or denying the requested amendment and providing a written denial.

a. If unable to act within 60 days, the CE may have a one-time 30 day extension.

b. The CE must furnish a written statement of the reasons for the delay and the date on which the CE will complete its action.

4. **Accepting the Amendment**. If the CE accepts the amendment –

a. It must timely inform the individual.

b. It must 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.

c. Make reasonable efforts to inform and provide the amendment within a reasonable timeframe to –

- Persons identified by the individual as having received the information prior to amendment, and
- Persons, *including business associates*, that the CE knows have the protected health information “and may have relied, or could foreseeably rely, on such information to the detriment of the patient.”

5. **Response to Amendment by Others**. If a covered entity is notified that an originating covered entity has amended PHI, the covered entity must also amend the PHI *and designated record sets*. The amendment is processed the same as if it had been originated with the second covered entity.

6. **Documentation**. The covered entity should document the following:

- a. The title of the individuals or offices responsible for receiving and processing requests for amendment.
- b. The paperwork surrounding the documentation, including each compliance step of the covered entity.
- c. These record should be retained for 6 years.

7. **Amendment v. Correction**. Amendment is always a separate entry; the process does not require altering any record in its stored or transmitted form. Existing records need not be “corrected” except as consistent with the covered entity’s policies and state law.

8. **Duration**. An individual can request amendment for so long as the record is maintained in a designated record set. The right to amend applies to records created *before* the HIPAA compliance date. (See 65 Fed. Reg. pp. 82736-82737).

9. **Requests in Writing**. The covered entity can only require that requests for amendment be submitted in writing and that they articulate a reason for amendment if it informs individuals in advance of this requirement.

- a. Critical to include in Notice of Privacy Practices.
- b. Also include in any instructions or policy or information furnished when a patient inquires about the process.

10. **Business Associate Contracts**. Business associate contracts must require the business associate to make protected health information available for amendment and incorporate amendments made by the covered entity or the business associate. (§ 164.504(e)).

E. **INDIVIDUAL'S RIGHT TO AN ACCOUNTING OF CERTAIN DISCLOSURES**

1. **Right to an Accounting.** Section 164.528 gives individuals a right to an accounting of disclosures of PHI, subject to the following exceptions and conditions:

- a. Only applicable to disclosures made within 6 years of the request.
- b. The accounting need not include disclosures for treatment, payment or health care operations.
- c. The accounting need not include disclosures to the individual.
- d. The accounting need not include disclosures in the form of inclusion in a facility directory or the persons involved in the individual's care or disclosures for notification purposes per § 164.510.
- e. The accounting need not include disclosures for national security or intelligence purposes.
- f. The accounting need not include disclosures to correctional institutions or law enforcement officials per the exceptions at § 164.512(k)(5).
- g. The accounting need not include disclosures that occurred prior to the compliance date for the covered entity.

These are not grounds for denial – these are types of disclosures as to which the granting clause in HIPAA does not give the individual a right to an accounting in the first place.

2. **Content of the Accounting.** An accounting must include the following information:

- a. The date of each disclosure.
- b. The name of each entity or person who received PHI and, if known, the address of such entity or person.
- c. A brief description of the PHI disclosed.
- d. A brief statement of the purpose of the disclosure “that reasonably informs the individual of the basis for the disclosure.” Alternatively, the CE can provide a copy of the individual's authorization (if that was the basis for disclosure) or a copy of the request where the disclosure is per one of the regulatory exceptions to consent/authorization under § 164.512.
- e. There is narrow authority to account only once for certain multiple disclosures to the same party for the same purpose.

3. **Time Period.** The covered entity has 60 days from receipt of a request for an accounting in which to comply with the request.
 - a. There is no denial or review process – the CE simply decides whether the request for an accounting is for disclosures for which an accounting is required and complies with the 60-day timeframe.
 - b. The CE can have a one-time 30 day extension upon written notice to the individual giving the reasons and the time by which the accounting will be produced.
4. **Fees.**
 - a. No charge for the first accounting in any 12-month period.
 - b. A “reasonable, cost-based fee” for each subsequent request for an accounting by the same individual within the 12-month period – conditioned upon *informing the individual in advance* of the free structure, and affording the opportunity to withdraw or modify the request to reduce fees.
 - Presumably must give this notice when fielding the *first* request, so that the person can ask broadly for a single, free accounting the first time and avoid fees for supplemental requests.
 - Include the fee structure and the right to a single free accounting once each 12 months in the Notice of Privacy Practices.
 - Also include in any explanation, request form or policy furnished to patients who inquire.
 - c. Must be able to support a cost-based fee for the accounting.
5. **Documentation.** The CE must document the following:
 - a. Documentation of the information required to be included in the accounting itself.
 - b. A copy of the actual written accounting that is furnished to the individual.
 - c. The titles of persons or offices responsible for receiving and processing requests for an accounting.
 - d. The “reasonable cost-based fee.”
 - e. Six year retention period. Note – this can be a 6 year extension on the normal retention period for designated record sets.

F. APPLICATION TO HEALTH CARE CLEARINGHOUSES

1. **As a Business Associate**. When a clearinghouse creates or receives PHI as the business associate of another covered entity, it is not subject to the access, amendment or accounting requirements of HIPAA as a covered entity, but it is subject to these rules as a business associate governed by the business associated agreement.
2. **As a Covered Entity**. When a clearinghouse creates or receives PHI other than as a business associate of a covered entity, it is covered by the access, amendment and accounting rules, the same as any other covered entity. Here, the rules apply directly, not through a business associate agreement.

G. POLICIES, MECHANICS AND SAFEGUARDS

1. **Policies**. At a minimum, complying with patient access requirements appears to require policies on the following subjects:
 - a. Defining and listing DRSs – both by name and content.
 - Legal effect – not much; any information, including information you do not think to include in a DRS becomes a DRS if it is PHI used to make decisions about individuals. The dietician’s notes in the kitchen, although never part of the medical record, are DRS subject to access rules, even though no one will think to mention them.
 - Practical effect – huge; individuals are likely to accept the covered entity’s list of designated record sets and to request only them.
 - Just be prepared to individually analyze any request for PHI used to make decisions about individuals which does not fit one of your defined designated record sets.
 - b. Policy on verification of identity –
 - Of individuals themselves when requesting access.
 - Of personal representatives acting on behalf of individuals.
 - Of recipients of amended PHI or of statements of disagreement.
 - c. Notice of Privacy Practices. This subject is one part of the covered entity’s required notice, but it is a critical part because it gives advance notice to individuals of your policies.
 - d. Other policies to assure advance notification of individuals in order to preserve certain covered entity rights, for example – the right to require that requests for amendment be submitted in writing and state the basis for the

request, or the fee structure for requesting multiple accountings in a 12-month period.

- e. Policies on fees, fee structure, and supporting documentation of cost loaded into permissible fees. This includes identifying fees that can be permissibly included.
- f. Comprehensive policy on access and copying.
- g. Comprehensive policy on amending protected health information.
- h. Comprehensive policy on maintaining and furnishing accounting of disclosures.
- i. Record retention policy.
- j. Policy setting forth mechanism to resolve internal questions – for example:
 - Is a disputed record a designated record set; is it used to make decisions about individuals?
 - Whether the originator of disputed information is still available to process amendments.
 - Covered entities will want documentation of the reasons they reach internal conclusions that affect responses to individuals in the event of survey by the Secretary or complaint to the Secretary.
- k. Policies on processing requests in organized health care arrangement or in an affiliated health system designated as a single covered entity.