

HIPAA Privacy

An innovative approach to self-implementation

WorkGroups[®]

Teleconference

Minimum Necessary

[Ver 2.0]

Rules, Resources and Policies

Wednesday, February 12,, 2003
10:00 a.m. – 11:00 a.m., CST



“Minimum Necessary”
– Setting the Stage –

Five Basic Features of Privacy Regulations

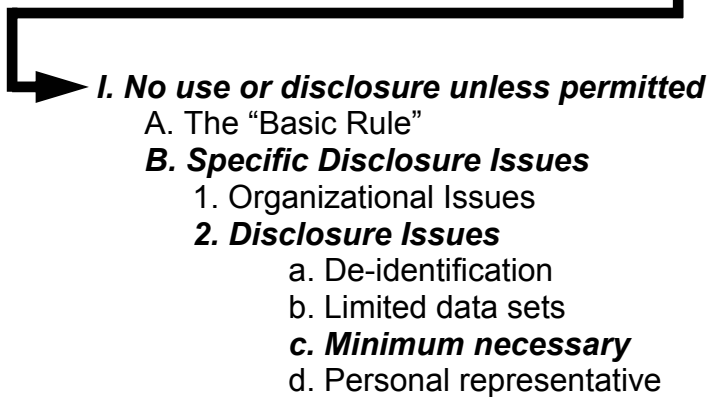
I. No use or disclosure unless permitted

II. Permitted uses & disclosures

III. Other Patient Rights

IV. Administrative Requirements

V. Technical Provisions



Analytical Outline
“Minimum Necessary”
Sections 164.502(b) and 164.514(d)

Section 164.502(b)

1. General Rule
2. Exceptions
 - treatment
 - individual
 - authorizations
 - to the Secretary
 - required by law
 - transaction & code sets

Section 164.514(d)

1. Requirement
2. Uses
 - identify who needs access
 - for each:
 - information to which access is needed
 - conditions appropriate to such access
 - reasonable efforts to limit the access
3. Disclosures
 - routine and recurring basis
 - implement policies and procedures (which may be standard protocols) that limit
 - all other disclosures
 - Develop criteria designed to limit
 - Review requests on an individual basis in accordance with such criteria.
 - reliance - may reasonably rely on “minimum necessary” representation:
 - to public officials
 - another covered entity

- a professional (workforce or business associate) to provide professional services to the covered entity
- Documentation or representations that comply with 164.512(i) (research)

4. Requests

- A covered entity must limit any request from other covered entities.
 - routine and recurring
 - must implement policies and procedures
 - all other requests
 - review the request on an individual basis to limit

5. Entire record

- may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506 Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations;

(iii) ~~As~~ Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of § 164.502(b), § 164.514(d), and § 164.530(c) with respect to such otherwise permitted or required uses or disclosures Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with an authorization that complies with § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f) or (g). ~~(f) (e), (f), and (g).~~

(2) Required disclosures. A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) Standard: minimum necessary.

(1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts¹ to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

¹ “We delete the word ‘all’ from the ‘reasonable efforts’ that covered entities must take in making a ‘minimum necessary’ determination.” Preamble, page 82544.

- (i) Disclosures to or requests by a health care provider for treatment;
- (ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i)² of this section, as required by paragraph (a)(2)(i)³ of this section, ~~or pursuant to an authorization⁴ under § 164.508⁵, except for authorizations requested by the covered entity under § 164.508(d)⁶, (e)⁷, or (f)⁸;~~
- (iii) Uses or disclosures made pursuant to an authorization under § 164.508;
- (iv) ~~(iii)~~ Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter⁹;
- (v) ~~(iv)~~ Uses or disclosures that are required by law, as described by § 164.512(a)¹⁰; and
- (vi) ~~(v)~~ Uses or disclosures that are required for compliance with applicable requirements of this subchapter.¹¹

² Permissive disclosures to the individual.

³ Refers to the requirements of §164.524 (“Access of individuals to protected health information”, page 82823) and §164.528 (“Amendment of protected health information”, page 82824).

⁴ In other words, the minimum necessary standard applies to all authorizations other than those initiated by the covered entity.

⁵ “Uses and disclosures for which an authorization is required”, page 82811.

⁶ “Authorizations requested by a covered entity for its own uses and disclosures”, page 82812.

⁷ “Authorizations requested by a covered entity for disclosures by others”, page 82812.

⁸ “Authorizations for uses and disclosures of protected information created for research that includes treatment of the individual”, page 82812.

⁹ “Compliance and Enforcement”, page 82801.

¹⁰ Page 82813. Note, however, that Section 512 applies only when and to the extent that “the use or disclosure meets and is limited to the relevant requirements of such other laws” Preamble, page 82525.

¹¹ “We make an exception to the minimum necessary disclosure provision of this rule for the required and situational data elements of the standard transactions adopted in the Transactions Rule The minimum necessary requirements do apply to optional elements in such standard transactions This is particularly relevant to the NCPDP standards for retail pharmacy transactions ... in which the current standard leaves most fields optional. For this reason, we do not accept this suggestion.” Comments, page 82617.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

* * *

(d) (1) Standard: minimum necessary requirements. In order to comply with § 164.502(b)¹² and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information. ~~A covered entity must reasonably ensure that the standards, requirements, and implementation specifications of § 164.502(b) and this section relating to a request for or the use and disclosure of the minimum necessary protected health information are met.~~

(2) Implementation specifications: minimum necessary uses of protected health information.

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed¹³ and any conditions appropriate to such access¹⁴.

(ii) A covered entity must make reasonable efforts¹⁵ to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) Implementation specification: minimum necessary disclosures of protected health information.

(i) For any type of disclosure that it makes on a routine and recurring basis,¹⁶ a covered entity must implement policies and procedures (which may be standard protocols) that limit the

¹² § 164.502 “Uses and disclosures of protected health information: general rules” (b) “Standard: minimum necessary”, page 82805.

¹³ The “minimum necessary” standard is intended to reflect and be consistent with, not override, professional judgment and standards. For example, we expect that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed.” Preamble, page 82544.

¹⁴ “These role-based access rules must also identify the conditions, as appropriate, that would apply to such access. For example, an institutional health care provider could allow physicians access to all records under the condition that the viewing of medical records of patients not under their care is recorded and reviewed. Other health professionals’ access could be limited to time periods when they are on duty. Information available to staff who are responsible for scheduling surgical procedures could be limited to certain data. In many instances, use of order forms or selective copying of relevant portions of a record may be appropriate policies to meet this requirement.” Comments, page 82713.

¹⁵ “What is reasonable will vary with the circumstances. When it is practical to use order forms or selective copying of relevant portions of the record, the covered entity is required to do so. Similarly, this flexibility in the standard takes into account the ability of the covered entity to configure its record system to allow selective access to only certain fields, and the practicality of organizing systems to allow this capacity. It might be reasonable for a covered entity with a highly computerized information system to implement a system under which employees with certain functions have access to only limited fields in a patient records, while other employees have access to the complete records. Such a system might not be reasonable for a covered entity with a largely paper records system.” Comments, page 82714.

protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.¹⁷

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances¹⁸, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512¹⁹, if the public official represents that the information requested is the minimum necessary for the stated purpose(s)²⁰;

¹⁶ “We recognize that specific disclosures within a type may vary, and require that the policies address what is the norm for the type of disclosure involved.” Preamble, page 82544. Disclosures to health care providers for treatment purposes are not subject to these requirements. Preamble, page 82544.

¹⁷ “Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed. ... [C]overed entities may establish policies allowing for and justifying such a disclosure. Disclosure of the entire medical record absent such documented justification is a presumptive violation of this rule.” Preamble, page 82545.

Collection Agencies: “[W]hen a covered entity determines that a collection agency only requires limited information for its activities, it must make reasonable efforts to limit disclosure to that information.” Comments, page 82613.

Payments: “[I]t will be necessary to rely on the minimum necessary disclosure requirement to ensure that disclosures for payment purposes do not include information unnecessary for that purposes. In practice, the following is the information that generally will be needed: the name and address of the individual; the name and address of the payor or provider; the amount of the charge for health services; the date on which health services were rendered; the expiration date for the payment mechanism, if applicable (i.e., credit card expiration date); the individual's signature; and relevant identification and account numbers.” Comments, page 82617.

¹⁸ A request for the entire medical record absent ... documented justification is a presumptive violation of this rule.” Preamble, page 82545.

¹⁹ “Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.”, page 82813. For example, requests by agencies and officials responsible for public health activities (Subsection (b), page 82813), for health oversight activities (Subsection (d), page 82814), for law enforcement (Subsection (f), page 82815), etc. Note, however, that Section 512 applies only when and to the extent that “the use or disclosure meets and is limited to the relevant requirements of such other laws ...” Preamble, page 82525.

Court Orders: “[I]f the disclosure is pursuant to an order of a court or administrative tribunal ... a covered entity is not required to make a determination whether or not the order might otherwise meet the minimum necessary requirement.” Comments, page 82676.

Workers' Compensation: “Under the final rule, covered entities must comply with the minimum necessary provisions unless the disclosure is required by law.... The rule permits a provider to disclose information that is authorized by such a law to the extent necessary to comply with such law. Where the law is silent, the workers' compensation carrier and covered health care provider will need to discuss what information is necessary for the carrier to administer the claim, and the health care provider may disclose that information. We note that if the workers' compensation insurer has secured an authorization

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i)²¹ have been provided by a person requesting the information for research purposes.

(4) Implementation specifications: minimum necessary requests for protected health information.

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made²².

(iii) For all other requests, a covered entity must: ~~review the request on an individual basis to determine that the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.~~

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

from the individual for the release of protected health information, the covered entity may release the protected health information described in the authorization.” Comments, page 82708.

²⁰ “In complying with the request, however, the covered entity must make reasonable efforts not to disclose more information than is requested. For example, a covered entity may not provide a party free access to its medical records under the theory that the party can identify the information necessary for the request. In some instances, it may be appropriate for a covered entity, presented with a relatively broad discovery request, to permit access to a relatively large amount of information in order for a party to identify the relevant information. This is permissible as long as the covered entity makes reasonable efforts to circumscribe the access as appropriate.” Preamble, page 82530.

²¹ “Uses and disclosures for research purposes”, page 82816, which provides a mechanism for waiving or modifying authorization requirements in research activities.

²² “Covered entities’ policies and procedures must provide that requests for an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed. ... Covered entities may establish policies allowing for and justifying such a request. A request for the entire medical record absent such documented justification is a presumptive violation of this rule.” Preamble, page 82545.

(5) Implementation specification: other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section²³ apply, a covered entity may not use, ~~disclose~~ ~~discloses~~ or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

²³ The “minimum necessary” requirements.

§ 164.530 Administrative requirements.

* * *

(c) (1) Standard: safeguards. A covered entity must have in place appropriate²⁴ administrative, technical, and physical safeguards to protect the privacy²⁵ of protected health information.²⁶

(2) Implementation specification: safeguards.

(i) A covered entity must reasonably safeguard²⁷ protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.²⁸

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

²⁴ “This provision is not intended to incorporate the provisions in the proposed Security regulation into this regulation, or to otherwise require application of those provisions to paper records.” Comments, page 82746. But, “The proposed Security Rule included further details on what safeguards would be appropriate for electronic information systems.” Comments, page 82746.

“[W]e do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act.” Comments, page 82746.

²⁵ This rule addresses only privacy protection, while the proposed security rules (which applies only to electronic information) also addresses protection of data integrity.

²⁶ “Limitations on access to protected health information by the covered entities workforce will also be covered by the policies and procedures for “minimum necessary” use of protected health information, pursuant to § 164.514(d). We expect these provisions to work in tandem.” Preamble, page 82561.

Verification requirements (§164.514(h)) and firewall requirements for “component entities” (§164.504(c)(2)) are other aspects of “safeguards.” Verification was included in this section in the proposed rules.

²⁷ “We do not prescribe the particular measures that covered entities must take to meet this standard, because the nature of the required policies and procedures will vary with the size of the covered entity and the type of activities that the covered entity undertakes. (That is, as with other provisions of this rule, this requirement is “scalable.”) Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and requiring that doors to medical records departments (or to file cabinets housing such records) remain locked and limiting which personnel are authorized to have the key or pass-code. We intend this to be a common sense, scalable, standard. We do not require covered entities to guarantee the safety of protected health information against all assaults. Theft of protected health information may or may not signal a violation of this rule, depending on the circumstances and whether the covered entity had reasonable policies to protect against theft. Organizations such as the Association for Testing and Materials (ASTM) and the American Health Information Management Association (AHIMA) have developed a body of recommended practices for handling of protected health information that covered entities may find useful.” Preamble, page 82561.

²⁸ “This privacy rule does not require specific forms of proof for safeguards.” Comments, page 82746.

[Covered Entity's Name]		<i>Minimum Necessary – page 11</i>
[Department]	POLICY DESCRIPTION: Minimum necessary uses and disclosures	
[APPROVED: [Date]]	EFFECTIVE DATE: [Date]	
REFERENCE NUMBER:	PAGE: 11 of 10 <i>version February 3, 2003</i>	

<p>SCOPE: All Departments.</p>
<p>PURPOSE: To provide guidance regarding each individual's responsibility related to identifiable patient information. This policy addresses intentional or unintentional breach of patient confidentiality, including oral, written and electronic communication. This definition will safeguard patient privacy and help minimize exposure and/or liability to individuals, facilities, and the company. Each individual is responsible for adhering to this policy by using only the minimum information necessary to perform his or her responsibilities, regardless of the extent of access provided or available.</p> <p>To establish the requirements to protect patients' privacy rights and their individually identifiable health information as required by the Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and all Federal regulations and interpretive guidelines promulgated thereunder.</p>
<p>POLICY: Only individuals with a legitimate "need to know" may access, use or disclose patient information. This includes all activities related to treatment, payment and health care operations on behalf of <i>[Covered Entity's Name]</i>. Each individual may only access, use or disclose the minimum information necessary to perform his or her designated role regardless of the extent of access provided to him or her.</p>
<p>PROCEDURE:</p> <p><u>Definition</u></p> <p>For the purpose of this policy, protected health information means any individually identifiable health information collected or stored by <i>[Covered Entity's Name]</i>. Individually identifiable health information includes demographic information, financial information, and any information that relates to past, present or future physical or mental condition of an individual.</p> <p><u>Principles relating to the access, use and disclosure of patient information</u></p> <p>(A) Individuals acting on behalf of <i>[Covered Entity's Name]</i> must always use only the minimum amount of information necessary to accomplish the intended purpose of the use, access, or disclosure.</p> <p>(B) With respect to system access, patient privacy will be supported through authorization, access, and audit controls (<i>e.g.</i>, roles-based access) and should be implemented for all systems that contain identifying patient information. Within the permitted access, an individual system user is only to access what they need to perform his or her job.</p>

[Covered Entity's Name]	<i>Minimum Necessary – page 12</i>
[Department]	POLICY DESCRIPTION: Minimum necessary uses and disclosures
[APPROVED: [Date]]	EFFECTIVE DATE: [Date]
REFERENCE NUMBER:	PAGE: 12 of 11 <i>version February 3, 2003</i>

(C) Consistent with the Privacy Officer Policy, the privacy officer has the responsibility of facilitating compliance with these principles in conjunction with the Compliance Officer.

(D) Each individual is responsible for attending ongoing education and training on patient privacy and patient rights as directed.

(E) Each individual is responsible for compliance with these policies and principles.

(F) Enforcement will be consistent with the [Covered Entity's Name]'s sanctions and facility human resources policies and procedures.

The minimum necessary limitation on uses, disclosures and requests does not apply to:

(A) Disclosures to or requests by a health care provider for treatment;

(B) Uses or disclosures made to the individual;

(C) Uses or disclosures made pursuant to an authorization;

(D) Disclosures made during an investigation by the Department of Health & Human Services into [Covered Entity's Name]'s privacy practices;

(E) Uses or disclosures that are required by law; and

(F) Uses or disclosures for the required and situational data elements of the standard transactions adopted in the Transactions Rule. Note, however, that the minimum necessary requirements do apply to optional elements in such standard transactions.

Limiting uses to the minimum necessary amount of PHI

(A) *Routine and recurring uses:* The following procedure will be used to limit routine and recurring uses of PHI to the minimum amount necessary for the purpose:

(1) Those persons or classes of persons, as appropriate, in the workforce who need access to protected health information to carry out their duties will be identified;

(2) For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access will be determined; and

(3) Reasonable efforts will be taken to limit the access of such persons or classes identified to the PHI determined to be the minimum necessary.

[Covered Entity's Name]	<i>Minimum Necessary – page 13</i>
[Department]	POLICY DESCRIPTION: Minimum necessary uses and disclosures
[APPROVED: [Date]]	EFFECTIVE DATE: [Date]
REFERENCE NUMBER:	PAGE: 13 of 12 <i>version February 3, 2003</i>

(B) *Non-routine uses*: For all other uses:

(1) Criteria will be developed for each department that are designed to limit the PHI used to the information reasonably necessary to accomplish the purpose for which access for use is sought; and

(2) Requests for non-routine and non-recurring uses will be reviewed on an individual basis in accordance with such criteria.

Limiting disclosures to the minimum necessary amount of PHI

(A) *Routine and recurring disclosures*: For any type of disclosure that is made on a routine and recurring basis, standard protocols will be implemented by each department that limit the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure.

(B) *Non-routine disclosures*: For all other disclosures:

(1) Criteria will be developed for each department that are designed to limit the PHI to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(2) Requests for disclosure will be reviewed on an individual basis in accordance with such criteria.

Reliance on the requester to determine what is the minimum necessary information

(A) *[Covered Entity's Name]* may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(1) Making disclosures to public officials that are otherwise permitted without an authorization or for treatment, payment or health care operations, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(2) The information is requested by another covered entity;

(3) The information is requested by a professional who is a member of *[Covered Entity's Name]*'s workforce or is a business associate of *[Covered Entity's Name]* for the purpose of providing professional services to *[Covered Entity's Name]*, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(4) In the case of disclosures for research purposes, documentation or representations that comply with the applicable requirements of the Research Disclosure Policy have been provided by a person requesting the information for research purposes.

[Covered Entity's Name]	<i>Minimum Necessary – page 14</i>
[Department]	POLICY DESCRIPTION: Minimum necessary uses and disclosures
[APPROVED: [Date]	EFFECTIVE DATE: [Date]
REFERENCE NUMBER:	PAGE: 14 of 13 <i>version February 3, 2003</i>

Limiting requests to the minimum necessary amount of PHI

(A) *General:* Any request for PHI will be limited to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(B) *Routine and recurring requests:* For a request that is made on a routine and recurring basis, standard protocols will be implemented by each department that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(C) *Non-routine requests:* For all other requests:

(1) Criteria will be developed by each department that are designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(2) Non-routine and non-recurring requests for disclosure will be reviewed on an individual basis in accordance with such criteria.

Entire medical record uses, disclosures and requests

When a use, disclosure, or request is subject to this policy, an entire medical record may not be used, disclosed or requested except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Required documentation

The following documentation will be obtained, maintained and retained as follows:

(1) Department specific protocols for routine and recurring uses, disclosures and requests

(2) Department specific criteria for review of non-routine and non-recurring uses, disclosures and requests.

REFERENCES:

Privacy Officer Policy

Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164), specifically §§ 164.502(b) and 164.514(d).