

Privacy Regulations HIPAA-Administrative Simplification Internal Assessment

Blue font indicates what was initially on document and what Linda added

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
Use and Disclosure					
<p>§ 164.502 Uses and disclosures of protected health information: general rules.</p> <p>(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.</p> <p>1. Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:</p> <ul style="list-style-type: none"> i. To the individual; ii. Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations; iii. 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), and (g). <p>2. Required disclosures. A covered entity is required to disclose protected health information:</p> <p>(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and</p> <p>(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</p>	<p>Is (COMPANY NAME) able to identify health information as "protected" health information?</p> <p>Is the covered entity able to identify health information as "protected" health information?</p> <p>Does the CE have P&P concerning compliance with use and disclosure standards?</p> <p>How does the CE provide for the consent or authorization of disclosure of</p>				

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
entity's compliance with this subpart.	PHI?				
<p>164.502 (b) Standard: minimum necessary.</p> <ol style="list-style-type: none"> 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 efforts 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: <ol style="list-style-type: none"> 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) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f); iii. Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter; iv. Uses or disclosures that are required by law, as described by § 164.512(a); and v. Uses or disclosures that are required for compliance with applicable requirements of this subchapter. 	<p>Does covered entity have policies and procedures (reasonable efforts) for using and disclosing the minimum amount of protected information necessary to accomplish the purpose of the use or disclosure?</p>	<p>Implementation specification: To comply with this standard a covered entity must:</p> <ol style="list-style-type: none"> (i) Identify appropriate persons within the entity to determine what information should be used or disclosed consistent the minimum necessary standard (ii) Ensure that the persons identified under paragraph b (2) (I) of this section make the minimum necessary determinations when required (iii) Within the limits of the entity's technological capabilities, provide for the making of such determinations individually. (3) When making disclosures to public officials that are permitted under §164.510 but not required by law, a covered entity may rely on the representations of such officials that the info requested is the minimum necessary for the state purpose. 			
<p>§164.502 (c) Standard: uses and disclosures of protected health information subject to an agreed upon restriction.</p> <p>A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>§164.502 (d) Standard: uses and disclosures of de-identified protected health information.</p> <ol style="list-style-type: none"> 1. Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity. 2. Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that: <ul style="list-style-type: none"> (i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and (ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart. 	<p style="color: blue;">Has (COMPANY NAME) determined if and how it will create de-identified health information?</p>	<p>A covered entity may use protected health info to create de-identified info by removing, coding, encrypting, or otherwise eliminating or concealing the info that makes such info individual identifiable.</p> <p>(ii) Info is presumed to be de-identified if:</p> <p>(A)The following identifiers need to be removed:</p> <ol style="list-style-type: none"> 1. Name 2. Address, including street address, city county zip and geocodes 3. Names of relatives 4. Name of employers 5. Birth Date 6. Phone Number 7. Fax Number 8. Email address 9. SS number 10. Medical record number 11. Health plan beneficiary number 12. Account number 13. Certificate/license number 14. Vehicle or other device serial number 15. Web Universal Resource Locator (URL) 16. IP address 17. Finger or voice prints 18. Photographic images 19. Any other unique identifying number, characteristic, or code that may be available to an anticipated recipient of the info and <p>(B)The covered entity has no reason to believe that any anticipated recipient could use the info alone or in combinations with other info to identify the individual.</p> <p style="color: blue;">(iii) Notwithstanding paragraph (d)(2)(ii) of this section, entities with appropriate statistical experience and expertise may treat the info as deidentified if they include info listed in paragraph (d)(2)(ii) of this section and they determine that the probability of identifying individuals with such identifying info retained is very low, or may remove additional info, if they have a basis to believe such additional info could be used to identify an individual</p> <p style="color: blue;">(iv)</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
§164.502 APPLICATIONS TO BUSINESS ASSOCIATES					
<p>(e) standard: disclosures to business associates.</p> <p>i. A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.</p> <p>ii. This standard does not apply:</p> <p>A. With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;</p> <p>B. With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or</p> <p>C. With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information</p> <p>D. used to determine enrollment or eligibility in the health plan is</p>	<p>Has (COMPANY NAME) included HIPAA provisions in its contracts with business partners?</p> <p>Has the CE provided for "reasonable steps" to cure or end violations of BAs where applicable?</p>	<p>Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).</p> <p>Satisfactory assurance means a contract between the covered entity and the BA to which such info is to be disclosed. The contract must include that</p> <p>(A) The BA not use or further disclose the information other than as permitted or required by the contract</p> <p>(B) (B) Not use or further disclose the info in a manner that would violate the requirements of this subpart</p> <p>(C) Use appropriate safeguards to prevent use of disclosure of the info other than provided by its contract of which it becomes aware</p> <p>(D) Report to the covered entity any use or disclosure of the info not provided for by its contract of which it becomes aware</p> <p>(E) Ensure that any subcontractors or agents to whom it provides protected health info to agree to the same restrictions and conditions that apply to the BA.</p> <p>(F) Make available protected Health info in accordance with §164.514(a)</p> <p>(G) Make its internal practiced, books and records relating to the use and disclosure available to the Secretary for purposes of determining the covered entity's compliance with this subpart</p> <p>(H) At termination of the contract return or destroy all protected health info and retain no copies of the info</p> <p>(I) Incorporate any amendments for corrections when notified pursuant to 164.516</p> <p>(ii)Authorize the covered entity to terminate the contract if the covered entity determines that the BA has violated the contract</p> <p>(iii) A material breach by a BA under the contract will be considered noncompliance, if the covered entity knows of the breach and did not take reasonable steps to cure the breach or terminate the contract or report to HHS.</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.</p> <p>iii. A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).</p> <p>§164.502 (f) Standard: deceased individuals A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.</p> <p>§164.502 (g): (1) Standard: personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a</p>	<p>Do we have procedure in place to ensure the protection of health info for deceased persons for the time period required by law following the death?</p>	<p>(2) Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>personal representative as the individual for purposes of this subchapter.</p>		<p>under this subchapter, with respect to protected health information relevant to such personal representation.</p> <p>(3) Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:</p> <p>(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;</p> <p>(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or</p> <p>(iii) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.</p> <p>(4) Implementation specification: deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.</p> <p>(5) Implementation specification: abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(h) Standard: confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.</p> <p>§164.502 (i): Standard: Uses and disclosures consistent with notice</p> <p>A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 64.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.</p> <p>§164.502 (j): Standard: disclosures by whistleblowers and workforce member crime victims.</p> <p>(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:</p> <p>(i) The workforce member or business associate</p>		<p>if:</p> <ul style="list-style-type: none"> (i) The covered entity has a reasonable belief that: <ul style="list-style-type: none"> (A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or (B) Treating such person as the personal representative could endanger the individual; and (ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative. 			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and</p> <p>(ii) The disclosure is to:</p> <p>(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or</p> <p>(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.</p> <p>(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:</p> <p>(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and</p> <p>(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).</p>					
<p>Uses and disclosures: organizational requirements</p> <p>§164.504 (a)Definitions</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>§164.504 (b): Standard: Health care component If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.</p>		<p>(c)(1) Implementation specification: application of other provisions. In applying a provision of this subpart, other than this section, to a hybrid entity:</p> <p>(i) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;</p> <p>(ii) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, covered health care provider, or health care clearinghouse, as applicable; and</p> <p>(iii) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.</p> <p>(2) Implementation specifications: safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:</p> <p>(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;</p> <p>(ii) A component that is described by paragraph (2)(i) of the definition of health care component in this section does not use or disclose protected health information that is within paragraph (2)(ii) of such definition for purposes of its activities other than those described by paragraph (2)(i) of such definition in a way prohibited by this subpart; and</p> <p>(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member’s work for the health care component in a way prohibited by this subpart.</p> <p>(3) Implementation specifications: responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities:</p> <p>(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>§164.504 (d) Standard: Affiliated covered entities.</p> <p>Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.</p> <p>§164.504 (e): Standard: Business Associate Contracts.</p> <p>(e)(1) Standard: business associate contracts.</p> <p>(i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.</p> <p>(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a</p>		<p>with this subpart.</p> <p>(ii) The covered entity has the responsibility for complying with § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.</p> <p>(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j).</p> <p>(2) Implementation specifications: requirements for designation of an affiliated covered entity.</p> <p>(i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.</p> <p>(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).</p> <p>(3) Implementation specifications: safeguard requirements. An affiliated covered entity must ensure that:</p> <p>(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and</p> <p>(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.</p> <p>(2) Implementation specifications: business associate contracts. A contract between the covered entity and a business associate must:</p> <p>(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:</p> <p>(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:</p> <p>(A) Terminated the contract or arrangement, if feasible; or</p> <p>(B) If termination is not feasible, report the problem to the Secretary.</p>		<p>(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.</p> <p>(ii) Provide that the business associate will:</p> <p>(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;</p> <p>(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;</p> <p>(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;</p> <p>(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;</p> <p>(E) Make available protected health information in accordance with § 164.524;</p> <p>(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;</p> <p>(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;</p> <p>(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and</p> <p>(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.</p> <p>(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.</p> <p>(3) Implementation specifications: other arrangements.</p> <p>(i) If a covered entity and its business associate are both governmental</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>entities:</p> <p>(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.</p> <p>(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.</p> <p>(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.</p> <p>(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.</p> <p>(4) Implementation specifications: other requirements for contracts and other arrangements.</p> <p>(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:</p> <p>(A) For the proper management and administration of the business associate; or</p> <p>(B) To carry out the legal responsibilities of the business associate.</p> <p>(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:</p> <p>(A) The disclosure is required by law; or</p> <p>(B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>§164.504 (f): Standard: Requirements for group health plans.</p> <p>(i) Except as provided under paragraph (f)(1)(ii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.</p> <p>(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :</p> <p>(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or</p> <p>(B) Modifying, amending, or terminating the group health plan.</p>		<p>it was disclosed to the person; and</p> <p>(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.</p> <p>(2) Implementation specifications: requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to:</p> <p>(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.</p> <p>(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:</p> <p>(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;</p> <p>(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;</p> <p>(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;</p> <p>(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;</p> <p>(E) Make available protected health information in accordance with § 164.524;</p> <p>(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;</p> <p>(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;</p> <p>(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;</p> <p>(I) If feasible, return or destroy all protected health information received</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and</p> <p>(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.</p> <p>(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:</p> <p>(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;</p> <p>(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and</p> <p>(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.</p> <p>(3) Implementation specifications: uses and disclosures. A group health plan may:</p> <p>(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;</p> <p>(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;</p> <p>(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and</p> <p>(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.</p>			
With Multiple Covered Functions					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>§164.504 (g): Standard: Requirements for a covered entity with multiple covered functions. (1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed. (2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity’s health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.</p>					
<p>§164.506 Consent for uses or disclosures to carry out treatment, payment or health care operations</p>					
<p>(a) Standard: Consent requirement. (1) Except as provided in paragraph (a)(2) or (a)(3) of this section, a covered health care provider must obtain the individual’s consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. (2) A covered health care provider may, without consent, use or disclose protected health information to carry out treatment, payment, or health care operations, if: (i) The covered health care provider has an indirect treatment relationship with the individual; or (ii) The covered health care provider created or received the protected health information in the course of providing health care to an individual who is an inmate. (3)(i) A covered health care provider may, without prior consent, use or disclose protected health information created or received under paragraph(a)(3)(i)(A)–(C) of this section to carry out treatment, payment, or health care</p>	<p>Do we have a mechanism for obtaining and ensuring individual authorization before using or disclosing protected health information to a non-covered entity?</p>	<p>(b) Implementation specifications: <i>General requirements.</i> (1) A covered health care provider may condition treatment on the provision by the individual of a consent under this section. (2) A health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment. (3) A consent under this section may not be combined in a single document with the notice required by § 164.520. (4)(i) A consent for use or disclosure may be combined with other types of written legal permission from the individual (e.g., an informed consent for treatment or a consent to assignment of benefits), if the consent under this section: (A) Is visually and organizationally separate from such other written legal permission; and (B) Is separately signed by the individual and dated. (ii) A consent for use or disclosure may be combined with a research authorization under § 164.508(f). (5) An individual may revoke a consent under this section at any time, except to</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>operations:</p> <p>(A) In emergency treatment situations, if the covered health care provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;</p> <p>(B) If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts to obtain such consent but is unable to obtain such consent; or</p> <p>(C) If a covered health care provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.</p> <p>(ii) A covered health care provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.</p> <p>(4) If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to carry out treatment, payment, or health care operations, provided that such consent meets the requirements of this section.</p> <p>(5) Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information</p> <p>§ 164.506(e) Standard: Resolving conflicting consents and authorizations</p> <p>(1) If a covered entity has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity may disclose such protected health information only in</p>		<p>the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.</p> <p>(6) A covered entity must document and retain any signed consent under this section as required by § 164.530(j).</p> <p>(c) Implementation specifications: Content requirements. A consent under this section must be in plain language and:</p> <p>(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;</p> <p>(2) Refer the individual to the notice required by § 164.520 for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;</p> <p>(3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with § 164.520(b)(1)(v)(C), state that the terms of its notice may change and describe how the individual may obtain a revised notice;</p> <p>(4) State that:</p> <p>(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;</p> <p>(ii) The covered entity is not required to agree to requested restrictions; and</p> <p>(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;</p> <p>(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and</p> <p>(6) Be signed by the individual and dated.</p> <p>(d) Implementation specifications: Defective consents. There is no consent under this section, if the document submitted has any of the following defects:</p> <p>(1) The consent lacks an element required by paragraph (c) of this section, as applicable; or</p> <p>(2) The consent has been revoked in accordance with paragraph (b)(5) of this section.</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>disclose such protected health information only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.</p> <p>(2) A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual described in paragraph (e)(1) of this section by:</p> <p>(i) Obtaining a new consent from the individual under this section for the disclosure to carry out treatment, payment, or health care operations; or</p> <p>(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose protected health information in accordance with the individual's preference.</p> <p>§ 164.506 (f) (1) Standard: Joint consents. Covered entities that participate in an organized health care arrangement and that have a joint notice under § 164.520(d) may comply with this section by a joint consent.</p>		<p>(2) Implementation specifications: requirements for joint consents.</p> <p>(i) A joint consent must:</p> <p>(A) Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and</p> <p>(B) Meet the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the consent covers more than one covered entity.</p> <p>(ii) If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.</p>			
<p>§ 164.508 Uses and disclosures for which an authorization is required.</p>					
<p>(a) Standard: Authorizations for uses and disclosures. (1) Authorization required: General rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected</p>		<p>(b) Implementation specifications: General requirements. (1) Valid authorizations.</p> <p>(i) A valid authorization is a document that contains the elements listed in paragraph (c) and, as applicable, paragraph (d), (e), or (f) of this section.</p> <p>(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>health information, such use or disclosure must be consistent with such authorization.</p> <p><i>(2) Authorization required: psychotherapy notes.</i> Notwithstanding any other provision of this subpart, other than transition provisions provided for in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:</p> <p>(i) To carry out the following treatment, payment, or health care operations, consistent with consent requirements in § 164.506:</p> <p>(A) Use by originator of the psychotherapy notes for treatment;</p> <p>(B) Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or</p> <p>(C) Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and</p> <p>(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).</p>		<p><i>(2) Defective authorizations.</i> An authorization is not valid, if the document submitted has any of the following defects:</p> <p>(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;</p> <p>(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c), (d), (e), or (f) of this section, if applicable;</p> <p>(iii) The authorization is known by the covered entity to have been revoked;</p> <p>(iv) The authorization lacks an element required by paragraph (c), (d), (e), or (f) of this section, if applicable;</p> <p>(v) The authorization violates paragraph (b)(3) of this section, if applicable;</p> <p>(vi) Any material information in the authorization is known by the covered entity to be false.</p> <p><i>(3) Compound authorizations.</i> An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:</p> <p>(i) An authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined as permitted by § 164.506(b)(4)(ii) or paragraph (f) of this section;</p> <p>(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;</p> <p>(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.</p> <p><i>(4) Prohibition on conditioning of authorizations.</i> A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:</p> <p>(i) A covered health care provider may condition the provision of research-</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>related treatment on provision of an authorization under paragraph (f) of this section;</p> <p>(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:</p> <p>(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and</p> <p>(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section;</p> <p>(iii) A health plan may condition payment of a claim for specified benefits on provision of an authorization under paragraph (e) of this section, if:</p> <p>(A) The disclosure is necessary to determine payment of such claim; and</p> <p>(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and</p> <p>(iv) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.</p> <p>(5) <i>Revocation of authorizations.</i> An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:</p> <p>(i) The covered entity has taken action in reliance thereon; or</p> <p>(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.</p> <p>(6) <i>Documentation.</i> A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).</p> <p>(c) Implementation specifications: Core elements and requirements.</p> <p>(1 Core elements. A valid authorization under this section must contain at least the following elements:</p> <p>(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;</p> <p>(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;</p> <p>(iv) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;</p> <p>(v) A statement of the individual’s right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;</p> <p>(vi) A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;</p> <p>(vii) Signature of the individual and date; and</p> <p>(viii) If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual.</p> <p>(2) Plain language requirement. The authorization must be written in plain language.</p> <p>(d) Implementation specifications: authorizations requested by a covered entity for its own uses and disclosures. If an authorization is requested by a covered entity for its own use or disclosure of protected health information that it maintains, the covered entity must comply with the following requirements.</p> <p>(1) Required elements. The authorization for the uses or disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:</p> <p>(i) For any authorization to which the prohibition on conditioning in paragraph (b)(4) of this section applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;</p> <p>(ii) A description of each purpose of the requested use or disclosure;</p> <p>(iii) A statement that the individual may:</p> <p>(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.524; and</p> <p>(B) Refuse to sign the authorization; and</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>(iv) If use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.</p> <p>(2) Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.</p> <p>(e) Implementation specifications: authorizations requested by a covered entity for disclosures by others. If an authorization is requested by a covered entity for another covered entity to disclose protected health information to the covered entity requesting the authorization to carry out treatment, payment, or health care operations, the covered entity requesting the authorization must comply with the following requirements.</p> <p>(1) Required elements. The authorization for the disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:</p> <ul style="list-style-type: none"> (i) A description of each purpose of the requested disclosure; (ii) Except for an authorization on which payment may be conditioned under paragraph (b)(4)(iii) of this section, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and (iii) A statement that the individual may refuse to sign the authorization. <p>(2) Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.</p> <p>(f) Implementation specifications: authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual.</p> <p>(1) Required elements. Except as otherwise permitted by § 164.512(i), a covered entity that creates protected health information for the purpose, in whole or in part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must:</p> <ul style="list-style-type: none"> (i) For uses and disclosures not otherwise permitted or required under this subpart, meet the requirements of paragraphs (c) and (d) of this 			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>section; and</p> <p>(ii) Contain:</p> <p>(A) A description of the extent to which such protected health information will be used or disclosed to carry out treatment, payment, or health care operations;</p> <p>(B) A description of any protected health information that will not be used or disclosed for purposes permitted in accordance with §§ 164.510 and 564.512, provided that the covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i); and</p> <p>(C) If the covered entity has obtained or intends to obtain the individual's consent under § 164.506, or has provided or intends to provide the individual with a notice under § 164.520, the authorization must refer to consent or notice, as applicable, and state that the statements made pursuant to this section are binding.</p> <p>(2) Optional procedure. An authorization under this paragraph may be in the same document as:</p> <p>(i) A consent to participate in the research;</p> <p>(ii) A consent to use or disclose protected health information to carry out treatment, payment, or health care operations under § 164.506; or</p> <p>(iii) A notice of privacy practices under § 164.520.</p>			
<p>§164.510 Uses and disclosures requiring an opportunity for the individual to agree or object</p>					
<p>A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described by §§ 164.506 and 164.508, respectively, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.</p> <p>§164.510 (a) Standard: use and disclosure for facility</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>directories.</p> <p>(1) Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:</p> <ul style="list-style-type: none"> (i) Use the following protected health information to maintain a directory of individuals in its facility: <ul style="list-style-type: none"> (A) The individual’s name; (B) The individual’s location in the covered health care provider’s facility; (C) The individual’s condition described in general terms that does not communicate specific medical information about the individual; and (D) The individual’s religious affiliation; and (ii) Disclose for directory purposes such information: <ul style="list-style-type: none"> (A) To members of the clergy; or (B) Except for religious affiliation, to other persons who ask for the individual by name. <p>(2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.</p> <p>(3) Emergency circumstances.</p> <ul style="list-style-type: none"> (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual’s incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility’s directory, if such disclosure is: <ul style="list-style-type: none"> (A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and 					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(B) In the individual’s best interest as determined by the covered health care provider, in the exercise of professional judgment.</p> <p>(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.</p> <p>(b) Standard: uses and disclosures for involvement in the individual’s care and notification purposes.</p> <p>(1) Permitted uses and disclosures.</p> <p>(i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person’s involvement with the individual’s care or payment related to the individual’s health care.</p> <p>(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual’s location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.</p> <p>(2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:</p> <p>(i) Obtains the individual’s agreement;</p> <p>(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or</p> <p>(iii) Reasonably infers from the circumstances, based</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>the exercise of professional judgment, that the individual does not object to the disclosure.</p> <p>(3) Limited uses and disclosures when the individual is not present. If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.</p> <p>(4) Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.</p> <p>§164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required</p> <p>A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described in §§ 164.506 and 164.508, respectively, or the opportunity for the individual to agree or object as described in § 164.510, in the situations</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.</p> <p>(a) Standard: uses and disclosures required by law.</p> <p>(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.</p> <p>(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.</p> <p>(b) Standard: uses and disclosures for public health activities.</p> <p>(1) Permitted disclosures. A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:</p> <p>(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;</p> <p>(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;</p> <p>(iii) A person subject to the jurisdiction of the Food and Drug Administration:</p> <p>(A) To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>disclosure is made to the person required or directed to report such information to the Food and Drug Administration;</p> <p>(B) To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;</p> <p>(C) To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or</p> <p>(D) To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration;</p> <p>(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or</p> <p>(v) An employer, about an individual who is a member of the workforce of the employer, if:</p> <p>(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides a health care to the individual at the request of the employer:</p> <p>(1) To conduct an evaluation relating to medical surveillance of the workplace; or</p> <p>(2) To evaluate whether the individual has a work-related illness or injury;</p> <p>(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;</p> <p>(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>surveillance;</p> <p>(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:</p> <p>(1) By giving a copy of the notice to the individual at the time the health care is provided; or</p> <p>(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.</p> <p>(2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.</p> <p>(c) Standard: disclosures about victims of abuse, neglect or domestic violence.</p> <p>(1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:</p> <p>(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;</p> <p>(ii) If the individual agrees to the disclosure; or</p> <p>(iii) To the extent the disclosure is expressly authorized by statute or regulation and:</p> <p>(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or</p> <p>(B) If the individual is unable to agree because of</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.</p> <p>(2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:</p> <p>(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or</p> <p>(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.</p> <p>(d) Standard: uses and disclosures for health oversight activities.</p> <p>(1) Permitted disclosures. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:</p> <p>(i) The health care system;</p> <p>(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;</p> <p>(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or</p> <p>(iv) Entities subject to civil rights laws for which health</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>information is necessary for determining compliance.</p> <p>(2) Exception to health oversight activities. For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:</p> <ul style="list-style-type: none"> (i) The receipt of health care; (ii) A claim for public benefits related to health; or (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services. <p>(3) Joint activities or investigations. Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.</p> <p>(4) Permitted uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.</p> <p>(e) Standard: disclosures for judicial and administrative proceedings.</p> <p>(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:</p> <ul style="list-style-type: none"> (i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or (ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if: <ul style="list-style-type: none"> (A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this 					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or</p> <p>(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.</p> <p>(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:</p> <p>(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);</p> <p>(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and</p> <p>(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:</p> <p>(1) No objections were filed; or</p> <p>(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.</p> <p>(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or</p> <p>(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.</p> <p>(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:</p> <p>(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and</p> <p>(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.</p> <p>(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.</p> <p>(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.</p> <p>(f) Standard: disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1)</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>through (f)(6) of this section are met, as applicable.</p> <p>(1) Permitted disclosures: pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:</p> <p>(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or</p> <p>(ii) In compliance with and as limited by the relevant requirements of:</p> <p>(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;</p> <p>(B) A grand jury subpoena; or</p> <p>(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:</p> <p>(1) The information sought is relevant and material to a legitimate law enforcement inquiry;</p> <p>(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and</p> <p>(3) De-identified information could not reasonably be used.</p> <p>(2) Permitted disclosures: limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:</p> <p>(i) The covered entity may disclose only the following information:</p> <p>(A) Name and address;</p> <p>(B) Date and place of birth;</p> <p>(C) Social security number;</p> <p>(D) ABO blood type and rh factor;</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(E) Type of injury; (F) Date and time of treatment; (G) Date and time of death, if applicable; and (H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.</p> <p>(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.</p> <p>(3) Permitted disclosure: victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:</p> <p>(ii) The individual agrees to the disclosure; or (iii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:</p> <p>(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim; (B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(4) Permitted disclosure: decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.</p> <p>(5) Permitted disclosure: crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.</p> <p>(6) Permitted disclosure: reporting crime in emergencies.</p> <p>(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:</p> <p>(A) The commission and nature of a crime;</p> <p>(B) The location of such crime or of the victim(s) of such crime; and</p> <p>(C) The identity, description, and location of the perpetrator of such crime.</p> <p>(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.</p> <p>(g) Standard: uses and disclosures about decedents.</p> <p><i>(1) Coroners and medical examiners.</i> A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.</p> <p>(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.</p> <p>(h) Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.</p> <p>(i) Standard: uses and disclosures for research purposes.</p> <p>(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:</p> <p>(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:</p> <p>(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or</p> <p>(B) A privacy board that:</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;</p> <p>(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and</p> <p>(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.</p> <p>(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:</p> <p>(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;</p> <p>(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and</p> <p>(C) The protected health information for which use or access is sought is necessary for the research purposes.</p> <p>(iii) Research on decedent's information. The covered entity obtains from the researcher:</p> <p>(A) Representation that the use or disclosure is sought is solely for research on the protected health information of decedents;</p> <p>(B) Documentation, at the request of the covered entity, of the death of such individuals; and</p> <p>(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.</p> <p>(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>documentation must include all of the following:</p> <ul style="list-style-type: none"> (i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved; (ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria: <ul style="list-style-type: none"> (A) The use or disclosure of protected health information involves no more than minimal risk to the individuals; (B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals; (C) The research could not practicably be conducted without the alteration or waiver; (D) The research could not practicably be conducted without access to and use of the protected health information; (E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research; (F) There is an adequate plan to protect the identifiers from improper use and disclosure; (G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and (H) There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart. 					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(D) of this section;</p> <p>(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:</p> <p>(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);</p> <p>(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;</p> <p>(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and</p> <p>(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.</p> <p>(j) Standard: uses and disclosures to avert a serious threat to health or safety.</p> <p>(1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:</p> <p>(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and</p> <p>(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or</p> <p>(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:</p> <p>(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or</p> <p>(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.</p> <p>(2) Use or disclosure not permitted.. A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:</p> <p>(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>counseling or therapy; or</p> <p>(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.</p> <p>(3) Limit on information that may be disclosed. A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.</p> <p>(4) Presumption of good faith belief. A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.</p> <p>(k) Standard: uses and disclosures for specialized government functions.</p> <p>(1) Military and veterans activities.</p> <p>(i) Armed Forces personnel. A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:</p> <p>(A) Appropriate military command authorities; and</p> <p>(B) The purposes for which the protected health information may be used or disclosed.</p> <p>(ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.</p> <p>(iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.</p> <p>(iv) Foreign military personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section.</p> <p>(2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).</p> <p>(3) Protective services for the President and others. A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.</p> <p>(4) Medical suitability determinations. A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to</p>					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>such information for the following purposes:</p> <ul style="list-style-type: none"> (i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698; (ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or (iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act. <p>(5) Correctional institutions and other law enforcement custodial situations.</p> <ul style="list-style-type: none"> (i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for: <ul style="list-style-type: none"> (A) The provision of health care to such individuals; (B) The health and safety of such individual or other inmates; (C) The health and safety of the officers or employees of or others at the correctional institution; (D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another; (E) Law enforcement on the premises of the correctional institution; and (F) The administration and maintenance of the safety, security, and good order of the correctional institution. (ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed. 					

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.</p> <p>(6) Covered entities that are government programs providing public benefits.</p> <p>(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.</p> <p>(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.</p> <p>(I) Standard: disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.</p> <p>§ 164.514 OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION</p> <p>§ 164.514 (A) Standard: de-identification of protected health information. Health information that does not</p>		<p>(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.</p>		<p>health information. A covered entity may determine that health information is not Individually identifiable health information only if:</p> <p>(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:</p> <p>(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and</p> <p>(ii) Documents the methods and results of the analysis that justify such determination; or</p> <p>(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:</p> <p>(A) Names;</p> <p>(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:</p> <p>(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and</p> <p>(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.</p> <p>(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;</p> <p>(D) Telephone numbers;</p> <p>(E) Fax numbers;</p> <p>(F) Electronic mail addresses;</p> <p>(G) Social security numbers;</p> <p>(H) Medical record numbers;</p> <p>(I) Health plan beneficiary numbers;</p> <p>(J) Account numbers;</p> <p>(K) Certificate/license numbers;</p> <p>(L) Vehicle identifiers and serial numbers, including license plate numbers;</p> <p>(M) Device identifiers and serial numbers;</p> <p>(N) Web Universal Resource Locators (URLs);</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(d)(1) Standard: minimum necessary requirements. 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.</p>		<p>(O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code; and (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the Information. (c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that: (1) Derivation. The code or other means of record Identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and (2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-Identification. (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 needed and any conditions appropriate to such access. (ii) A covered entity must make reasonable efforts 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, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. (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</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>§ 164.514(e)(1) Standard: uses and disclosures of</p>		<p>(B) Review requests for disclosure on an individual basis in accordance with such criteria.</p> <p>(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:</p> <p>(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);</p> <p>(B) The information is requested by another covered entity;</p> <p>(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</p> <p>(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.</p> <p>(4) Implementation specifications: minimum necessary requests for protected health information.</p> <p>(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.</p> <p>(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 made.</p> <p>(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.</p> <p>(5) Implementation specification: other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose 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.</p> <p>(2) Implementation specifications: requirements relating to marketing. (i) A covered entity is not required to obtain an authorization under § 164.508 when it</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>protected health information for marketing. A covered entity may not use or disclose protected health information for marketing without an authorization that meets the applicable requirements of § 164.508, except as provided for by paragraph (e)(2) of this section.</p> <p>164.514(f)(1) Standard: uses and disclosures for fundraising. A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:</p>		<p>uses or discloses protected health information to make a marketing communication to an individual that:</p> <ul style="list-style-type: none"> (A) Occurs in a face-to-face encounter with the individual; (B) Concerns products or services of nominal value; or (C) Concerns the health-related products and services of the covered entity or of a third party and the communication meets the applicable conditions in paragraph (e)(3) of this section. <p>(ii) A covered entity may disclose protected health information for purposes of such communications only to a business associate that assists the covered entity with such communications.</p> <p>(3) Implementation specifications: requirements for certain marketing communications. For a marketing communication to qualify under paragraph (e)(2)(i) of this section, the following conditions must be met:</p> <ul style="list-style-type: none"> (i) The communication must: <ul style="list-style-type: none"> (A) Identify the covered entity as the party making the communication; (B) If the covered entity has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and (C) Except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications. (ii) If the covered entity uses or discloses protected health information to target the communication to individuals based on their health status or condition: <ul style="list-style-type: none"> (A) The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and (B) The communication must explain why the individual has been targeted and how the product or service relates to the health of the individual. (iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications, under paragraph (e)(3)(i)(C) of this section, are not sent such communications. <p>(2) Implementation specifications: fundraising requirements.</p> <ul style="list-style-type: none"> (i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice; (ii) The covered entity must include in any fundraising materials it sends to 			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(i) Demographic information relating to an individual; and (ii) Dates of health care provided to an individual.</p> <p>(g) Standard: uses and disclosures for underwriting and related purposes. If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.</p> <p>(h)(1) Standard: verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:</p> <p>(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and</p> <p>(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.</p>		<p>an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.</p> <p>(ii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.</p> <p>(2) Implementation specifications: verification.</p> <p>(i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.</p> <p>(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.</p> <p>(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).</p> <p>(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:</p> <p>(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;</p> <p>(B) If the request is in writing, the request is on the appropriate government letterhead; or</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.</p> <p>(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:</p> <p>(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;</p> <p>(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.</p> <p>(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).</p>			
<p>164.520 NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION</p>					
<p>(a) <u>Standard: notice of privacy practices.</u> (1) Right to Notice. Except for group health plans, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. (2)(i) An individual enrolled in a group health plan has a right to notice: (A) From the group health plan, if the individual does not receive health benefits under the plan through an insurance contract with an insurance issuer or HMO; or (B) From the health insurance issuer of the group health plan or from the HMO.</p>	<p>Have we organized a written notice of information practices for its patients?</p>	<p>(b) <u>Implementation Specification: Content of Notice.</u> (1) <u>Required elements.</u> The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph. (i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY." (ii) <u>Uses and disclosures.</u> The notice must contain: (A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted to make for each of the following purposes: treatment, payment, and health care operations. (B) A description of each of the other purposes which are permitted or required to use or disclose protected health information without the</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, that:</p> <ul style="list-style-type: none"> • Creates or • Receives protected health information in addition to summary health information (as defined in §164.504(a)) • Has information on whether the individual is participating in the group health plan • Has information on enrollment/ disenrollment from a health insurance issuer or HMO offered by the plan, must: <p>(A) Maintain a notice under this section; and (B) Provide such notice upon request to any person. (Provisions of (c)(1) of this section do not apply to such a group health plan)</p> <p>(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not:</p> <ul style="list-style-type: none"> • Create or • Receive protected health information other than summary health information (as defined in §164.504(a)) • Has information on whether the individual is participating in the group health plan • Has information on enrollment/ disenrollment from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section. <p>3. Exception for inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.</p>		<p>individuals written consent or authorization.</p> <p>(C) If a use or disclosure as described in (A) and (B) above is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.</p> <p>(D) For each purpose described in (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.</p> <p>(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).</p> <p>(iii) <u>Separate statements for certain uses or disclosures.</u> If the covered entity intends to engage in any of the following activities, the description required in (b)(1)(ii)(A) of this section must include a separate statement that:</p> <p>(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;</p> <p>(B) The covered entity may contact the individual to raise funds for the covered entity; or</p> <p>(C) A group health plan, or health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.</p> <p>(iv) <u>Individual rights.</u> The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:</p> <p>(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;</p> <p>(B) The right to receive confidential communications of protected health information as provided by § 164.522(b);</p> <p>(C) The right to inspect and copy protected health information as provided by § 164.524;</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>(D) The right to amend protected health information as provided by § 164.526;</p> <p>(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and</p> <p>(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.</p> <p>(v) <u>Covered entity's duties.</u> The notice must contain:</p> <p>(A) A statement that the covered entity is required by law to protect the privacy of its individual identifiable health info, provide a notice of its policies and procedures with respect to terms of the notice currently in effect;</p> <p>(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and</p> <p>(C) A statement that the entity reserves the right to change its policies and procedure relating to protected health info at any time with a description of how the entity will provide individuals with a revised notice.</p> <p>(vi) <u>Complaints.</u> The notice must contain a statement that individuals may complain to the covered entity and the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.</p> <p>(vii) <u>Contact.</u> The notice must contain the name, or title, and phone number of a contact person or office required by §164.530(a)(2)</p> <p>(viii) <u>Effective Date.</u> The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise, published.</p> <p>(2) <u>Optional elements.</u></p> <p>(i) If a covered entity elects to limit the uses or disclosures that it is permitted to make, the covered entity may describe its more limited uses or disclosures in its notice, provide that the entity may not include limitations affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(I).</p> <p>(ii) For the covered entity to apply a change in its more limited uses and</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include that statements required by paragraph (b)(1)(v)(C) of this section.</p> <p>(3) <u>Revisions to this notice.</u> The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual’s rights, the entity’s legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented before the effective date of the notice in which such material change is reflected.</p> <p>(c) Implementation specification: Provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in this section.</p> <p>(1) <u>Specific requirements for health plans.</u></p> <p>(i) Health Plans must provide a copy of the notice:</p> <p>(A) No later than the compliance date for the health plan, to individuals then covered by the plan;</p> <p>(B) Thereafter, at the time of enrollment, to individual who are new enrollees, and;</p> <p>(C) Within 60 days of a material revision to the content of the notice, to individuals then covered by the plan.</p> <p>(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.</p> <p>(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.</p> <p>(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.</p> <p>(2) <u>Specific requirements for certain covered health care providers.</u> A covered health care provider that has a direct treatment relationship with an individual must:</p> <p>(i) Provide the notice no later than the date of the first service delivery,</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>including service delivered electronically, to such individual after the compliance date for the covered health care provider;</p> <p>(ii) If the covered health care provider maintains a physical service delivery site:</p> <p>(A) Have the notice available at the service delivery site for individuals to request to take with them; and</p> <p>(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and</p> <p>(iii) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(ii) of this section, if applicable.</p> <p>(3) Specific requirements for electronic notice.</p> <p>(i) A covered entity that maintains a web site that provides information about the covered entity’s customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.</p> <p>(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.</p> <p>(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual’s first request for service.</p> <p>(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.</p> <p>(d) <u>Implementation specifications: joint notice by separate covered entities.</u> Covered entities that participate in organized health care arrangements may comply with this section by a joint</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>notice, provided that:</p> <p>(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;</p> <p>(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and</p> <p>(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;</p> <p>(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and</p> <p>(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.</p> <p>(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.</p> <p>(e) Implementation specifications: documentation. A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity as required by § 164.530(j).</p>			
§164.522 RIGHTS TO REQUEST PRIVACY PROTECTION FOR PROTECTED HEALTH INFORMATION					
(a)(1) Standard: Right of an individual to request restriction of uses and disclosures. (i) A covered entity must permit an individual to request that the covered entity restrict:	Does (COMPANY NAME) have procedures for	(2) Implementation specifications: Terminating a restriction. A covered entity may terminate its agreement to a restriction, if : (i) The individual agrees to or requests the termination in writing; (ii) The individual orally agrees to the termination and the oral agreement			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and</p> <p>(B) (B) Disclosures permitted under § 164.510(b).</p> <p>(ii) A covered entity is not required to agree to a restriction.</p> <p>(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(I) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.</p> <p>(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.</p> <p>(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(i), 164.510(a) or 164.512.</p> <p>(b)(1) Standard: Confidential communications requirements.</p> <p>(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.</p> <p>(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the</p>	<p>allowing patients to request that their health info not be used or disclosed for treatment, payment, or healthcare operations?</p>	<p>is documented; or</p> <p>(iii) (iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.</p> <p>(3) Implementation specification: <i>Documentation.</i> A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).</p> <p>(2) Implementation specifications Conditions on providing confidential communications.</p> <p>(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.</p> <p>(ii) A covered entity may condition the provision of a reasonable accommodation on:</p> <p>(A) When appropriate, information as to how payment, if any, will be handled; and</p> <p>(B) (B) Specification of an alternative address or other method of contact.</p> <p>(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.</p> <p>(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
individual.		individual			
§ 164.524 Access of individuals to protected health information.					
<p>(a) Standard: Access to protected health information.</p> <p>(b) (1) <i>Right of access.</i> 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:</p> <ul style="list-style-type: none"> (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: <ul style="list-style-type: none"> (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). <p>(2) <i>Unreviewable grounds for denial.</i> A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.</p> <ul style="list-style-type: none"> (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 health care provider acting under the 	<p>Do we have a mechanism to allow patients to access, inspect, and obtain a copy of their own health information?</p>	<p>(b) Implementation specifications: requests for access and timely action.</p> <p>(1) <i>Individual's request for access.</i> 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.</p> <p>(2) <i>Timely action by the covered entity.</i> (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.</p> <ul style="list-style-type: none"> (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. <p>(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.</p> <p>(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:</p> <ul style="list-style-type: none"> (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. 			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>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.</p> <p>(iii) An individual’s access to protected health information created or obtained by a covered health care 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.</p> <p>(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.</p> <p>(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.</p> <p>(3) <i>Reviewable grounds for denial.</i> 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:</p> <p>(i) A licensed health care professional</p>		<p>(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.</p> <p>(1) <i>Providing the access requested.</i> 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.</p> <p>(2) <i>Form of access requested.</i> (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.</p> <p>(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.</p> <p>(3) <i>Time and manner of access.</i> 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.</p> <p>(4) <i>Fees.</i> 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</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>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;</p> <p>(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</p> <p>(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.</p> <p>(4) <i>Review of a denial of access.</i> 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.</p>		<p>only the cost of:</p> <p>(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;</p> <p>(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.</p> <p>(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.</p> <p>(1) <i>Making other information accessible.</i> 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.</p> <p>(2) <i>Denial.</i> 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:</p> <p>(i) The basis for the denial;</p> <p>(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</p> <p>(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).</p> <p>(3) <i>Other responsibility.</i> 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.</p> <p>(4) <i>Review of denial requested.</i> 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</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>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.</p> <p>(e) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):</p> <ol style="list-style-type: none"> (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. 			
<p>§ 164.526Amendment of protected health information.</p>					
<p>(a) Standard: Right to amend.</p> <ol style="list-style-type: none"> (1) <i>Right to amend.</i> 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) <i>Denial of amendment.</i> 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: <ol style="list-style-type: none"> (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; (iii) Would not be available for inspection under 164.524 () ; or (iv) Is accurate and complete. 		<p>(b) Implementation of specifications: requests for amendment and timely action</p> <ol style="list-style-type: none"> (1) <i>Individual's request for amendment.</i> 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) <i>Timely action by the covered entity</i> <ol style="list-style-type: none"> (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: <ol style="list-style-type: none"> (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: <ol style="list-style-type: none"> (A) The covered entity within the time limit set by paragraph (b)(2)(I) of this 			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>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</p> <p>(B) The covered entity may have only one such extension of time for action on a request for an amendment.</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:</p> <p>(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and</p> <p>(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of amendment and that may have relied or could foreseeably rely on such information to the detriment of the individual.</p> <p>(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.</p> <p>(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:</p> <p>(i) <i>The basis for the denial in accordance with paragraph (a)(2) of this section;</i></p> <p>(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;</p> <p>(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>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</p> <p>(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in 164.530(d) (process for individuals to make complaints) the Secretary pursuant to the procedures established in 160.306 (Right and requirements for filing complaints). The description must include the name or title, and telephone number of the contact person or office designated in 164.530(a)(1)(ii) (Privacy officer to receive complaints & provide info).</p> <p>(2) <i>Statement of disagreement.</i> 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.</p> <p>(3) <i>Rebuttal statement.</i> 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.</p> <p>(4) <i>Recordkeeping.</i> 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.</p> <p>(5) <i>Future disclosures.</i></p> <p>(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.</p> <p>(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.</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>(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)(l) or (ii) of this section as applicable, to the recipient of the standard transaction.</p> <p>(e) Implementation specification Actions on notice 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.</p> <p>(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). (Requirements for retention of specified documentation.)</p>			
<p>§ 164.528 Accounting of disclosures of protected health information.</p>					
<p>(a) Standard: Right to an accounting of disclosures of protected health information.</p> <p>(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested except for disclosures:</p> <p>(i) To carry out treatment, payment & health care operations as provided in 164.502 (<i>Permitted uses and disclosure – to individual, w/consent for tx, w/o consent for tx if not req., etc.</i>)</p> <p>(ii) To individuals of protected health info about them as provided in 164.502 (<i>see Item i above</i>)</p> <p>(iii) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in 164.510 (<i>Uses requiring opportunity for subject to agree or object</i>)</p> <p>(iv) For national security or intelligence purposes</p>		<p>(b) Implementation specifications: Content of the accounting: The covered entity must provide the individual with a written accounting that meets the following requirements.</p> <p>(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a) (3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.</p> <p>(2) The accounting must include for each disclosure:</p> <p>(i) The date of the disclosure;</p> <p>(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;</p> <p>(iii) A brief description of the protected health information disclosed; and</p> <p>(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:</p> <p>(A) A copy of the individual's written authorization pursuant to 164.508 (<i>Uses & disclosures for which consent is required</i>); or</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>as provided in 164.512k(2) (<i>permitted disclosure to authorized federal officials</i>)</p> <p>(v) To correctional institutions or law enforcement officials as provided in 164.512(k)(5) (<i>disclosure to correctional institute if needed for hlth & safety of individuals, other inmates, officers or employees, etc.</i>) or</p> <p>(vi) That occurred prior to the compliance date for the covered entity.</p> <p>(2)(l) The covered entity must temporarily suspend an individuals right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in 164.512(d) (<i>Permission or exceptions for disclosures to health oversight activities</i>) or (f) (<i>Disclosure to law enforcement officers</i>) respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.</p> <p>(ii) If the agency or official statement in paragraph (a)(2)(i) (<i>suspension of individual's right to receive acct'ing of disclosures</i>) of this section is made orally, the covered entity must:</p> <p>(A) Document the statement, including the identity of the agency or official making the statement;</p> <p>(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and</p> <p>(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that</p>		<p>(B) A copy of a written request for a disclosure under 164.502(a)(2)(ii) (<i>General rules for disclosure</i>) or 164.512 (<i>Uses for which consent is not required</i>), if any.</p> <p>(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under 164.502(a)(2)(ii) (<i>required disclosures to Secretary for complaint investigation or compliance reviews</i>) or 164.512 (<i>Uses & disclosures for which consent is not required</i>), or pursuant to a single authorization under 164.508 (<i>Uses and disclosures for which a consent is required</i>), the accounting may with respect to such multiple disclosures, provide:</p> <p>(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;</p> <p>(ii) The frequency, periodicity , or number of disclosures made during the accounting period; and</p> <p>(iii) The date of the last such disclosure during the accounting period.</p> <p>(c) Implementation Specifications: Provision of the accounting.</p> <p>(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.</p> <p>(i) The covered entity must provide the individual with the accounting requested; or</p> <p>(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:</p> <p>(A) The covered entity, within the time limit set by paragraph (c)(1) 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 provide the accounting; and</p> <p>(B) The covered entity may have only one such extension of time for action on a request for an accounting.</p> <p>(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>time.</p> <p>(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.</p>		<p>accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.</p> <p>(d) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by 164.530(j) (<i>Requirement to implement policies and procedures covering protected health information/standards</i>):</p> <p>(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section:</p> <p>(2) The written accounting that is provided to the individual under this section; and</p> <p>(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.</p>			
§ 164.530 ADMINISTRATIVE REQUIREMENTS					
<p>§ 164.530 (a)(1) Standard: personnel designations.</p> <p>(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.</p> <p>(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.</p> <p>(b)(1) Standard: training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.</p>	<p>Does (COMPANY NAME) have policies/procedures in place to comply with the various admin requirements of HIPAA?</p>	<p>(2) Implementation specification: personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.</p> <p>(2) Implementation specifications: training.</p> <p>(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:</p> <p>(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;</p> <p>(B) Thereafter, to each new member of the workforce within a reasonable</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(c)(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.</p> <p>(d)(1) Standard: complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.</p> <p>(e)(1) Standard: sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.</p> <p>(f) Standard: mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.</p> <p>(g) Standard: refraining from intimidating or retaliatory acts. A covered entity may not intimidate, threaten,</p>		<p>period of time after the person joins the covered entity's workforce; and</p> <p>(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.</p> <p>(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.</p> <p>(2) Implementation specification: safeguards. A covered entity must reasonably safeguard 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.</p> <p>(2) Implementation specification: documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.</p> <p>(2) Implementation specification: documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>coerce, discriminate against, or take other retaliatory action against:</p> <p>(1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;</p> <p>(2) Individuals and others. Any individual or other person for:</p> <p>(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;</p> <p>(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or</p> <p>(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.</p> <p>(h) Standard: waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.</p> <p>(i)(1) Standard: policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.</p>		<p>(3) Implementation specification: changes in law. Whenever there is a change</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(2) Standard: changes to policies or procedures.</p> <p>(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;</p> <p>(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or</p> <p>(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.</p>		<p>in law that necessitates a change to the covered entity’s policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.</p> <p>(4) Implementation specifications: changes to privacy practices stated in the notice.</p> <p>(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:</p> <p>(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity’s privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;</p> <p>(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and</p> <p>(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.</p> <p>(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:</p> <p>(A) Such change meets the implementation the requirements in paragraphs (i)(4)(i)(A)-(C) of this section; and</p> <p>(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.</p> <p>(5) Implementation specification: changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:</p> <p>(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and</p> <p>(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>(j)(1) Standard: documentation. A covered entity must:</p> <ul style="list-style-type: none"> (i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form; (ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and (iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation. <p>(k) Standard: group health plans.</p> <p>(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:</p> <ul style="list-style-type: none"> (i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and (ii) The group health plan does not create or receive protected health information, except for: <ul style="list-style-type: none"> (A) Summary health information as defined in § 164.504(a); or (B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan. <p>(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).</p>		<p>(2) Implementation specification: retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.</p>			
§ 164.532 Transition provisions.					
<p>(a) Standard: effect of prior consents and authorizations. Notwithstanding other sections of this subpart, a covered entity may continue to use or disclose protected health information pursuant to a consent,</p>		<p>(b) Implementation specification: requirements for retaining effectiveness of prior consents and authorizations. Notwithstanding other sections of this subpart, the following provisions apply to use or disclosure by a covered entity of protected health information pursuant to a</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
<p>authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information that does not comply with §§ 164.506 or 164.508 of this subpart consistent with paragraph (b) of this section.</p>		<p>consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, if the consent, Authorization, or other express legal permission was obtained from an individual before the applicable compliance date of this subpart and does not comply with §§ 164.506 or 164.508 of this subpart.</p> <p>(1) If the consent, authorization, or other express legal permission obtained from an individual permits a use or disclosure for purposes of carrying out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, use or disclose such information for purposes of carrying out treatment, payment, or health care operations, provided that:</p> <p>(i) The covered entity does may not make any use or disclosure that is expressly excluded from the a consent, authorization, or other express legal permission obtained from an individual; and</p> <p>(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.</p> <p>(2) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for a purpose other than to carry out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, make such use or disclosure, provided that:</p> <p>(i) The covered entity does not make any use or disclosure that is expressly excluded from the consent, authorization, or other express legal permission obtained from an individual; and</p> <p>(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.</p> <p>(3) In the case of a consent, authorization, or other express legal permission obtained from an individual that identifies a specific research project that includes treatment of individuals:</p> <p>(i) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to protected health information that it created or received either before or after the applicable compliance date of this subpart and to which the consent or authorization applies, make such use or</p>			

Regulation/Standard	Assessment Question	Implementation Specifications	Existing Yes/No	GapAnal Exist/vs. Stndrd)	Account ability
		<p>disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.</p> <p>(ii) If the consent, authorization, or other express legal permission obtained from an individual is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to protected health information that it created or received as part of the project before or after the applicable compliance date of this subpart, make a use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.</p> <p>(4) If, after the applicable compliance date of this subpart, a covered entity agrees to a restriction requested by an individual under § 164.522(a), a subsequent use or disclosure of protected health information that is subject to the restriction based on a consent, authorization, or other express legal permission obtained from an individual as given effect by paragraph (b) of this section, must comply with such restriction.</p>			