

Privacy Standards Assessment Tool

Entity / Department _____

Q#	Section/Regulation	Question	Response	Rule Comments
1	164.506(a). Consent for uses or disclosures to carry out treatment, payment, or health care operations.	Do you obtain an individual's consent prior to using or disclosing PHI to carry out treatment payment or health care operations? (See Attachment 2 for implementation specifications and definition of PHI)		Final rule requires consent for these purposes except in the following circumstances: provider has an indirect treatment relationship, individual is an inmate, in emergency treatment situations, law requires provider to treat individual, attempts are made to obtain consent but barriers to communication exist and consent to receive treatment is inferred from the circumstances.
2	164.506(a). Consent for uses or disclosures to carry out treatment, payment, or health care operations.	Does your consent form meet the requirements of the HIPAA regulation? (See Attachment 2 for the content requirements of the consent.)		The regulation lists the requirements for a valid consent. See attachment for the list of these requirements.
3	164.506(a). Consent for uses or disclosures to carry out treatment, payment, or health care operations.	Do you have a process in place to document failure to obtain a consent?		Failure to obtain a consent must be documented. The documentation must contain information about the attempt to obtain consent and the reason why consent was not obtained.
4	164.506(a). Consent for uses or disclosures to carry out treatment, payment, or health care operations.	Do you have a process in place to allow individuals to revoke a consent?		An individual may revoke a consent at anytime except to the extent that action has already been taken based on the existing consent. The revocation must be in writing.
5	164.506(a). Consent for uses or disclosures to carry out treatment, payment, or health care operations.	Do you have a record retention process in place that includes these consents?		Signed consents must be documented and retained in original or electronic copy for six years from the date of creation or the date that it was last in effect, whichever is later.
6	164.506(a). Consent for uses or disclosures to carry out treatment, payment, or health care operations.	Do you have a process in place to resolve conflicts between consents and any other authorization or written legal permission for use/disclosure of PHI for payment, treatment, or health care operations?		If a conflict exists, use and disclosure must follow the most restrictive document. The conflict may be resolved by obtaining a new consent or communicating (orally or in writing) with the individual to determine the individual's preference. This preference must be documented and followed.
7	164.508(a). Uses and disclosures for which an authorization is required.	Do you have a policy and procedure for obtaining authorization for use and disclosure of PHI for purposes other than payment, treatment, or health care operations?		The regulation requires authorization for uses and disclosure of PHI other than those obtained under the consent for payment, treatment, and health care operations or otherwise allowed under the rule.
8	164.508(b). Uses and disclosures for which an authorization is required.	If yes to the above, does your authorization form meet the regulation requirements? (See Attachment 4 for a list of the requirements).		The regulation spells out the core elements to an authorization as well as implementation specifications.
9	164.508(a). Uses and disclosures for which an authorization is required.	Do you generate psychotherapy notes? If yes, are these notes shared with or disclosed to anyone? (See Attachment 1 for definition of psychotherapy notes.)		Specific individual authorization is needed before this information could be disclosed with a few exceptions. These exceptions are listed in Attachment 3.
10	164.508(b)(3). Uses and disclosures for which an authorization is required.	Do you ever use "compound" or combined authorizations?		Authorizations for use and disclosure of PHI may not be combined with any other document to create a compound authorization except under specific conditions. These conditions are listed in Attachment 5.

Q#	Section/Regulation	Question	Response	Rule Comments
11	164.508(b)(4). Uses and disclosures for which an authorization is required.	Do you ever condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization from an individual?		Treatment, payment, enrollment in the health plan, or eligibility for benefits to an individual may not be conditioned on the provision of an authorization except under certain exceptions. See Attachment 6 for these exceptions.
12	164.508(b)(5). Uses and disclosures for which an authorization is required. Revocation of Authorization.	Do you have policies and procedures that allow for the revocation of an authorization?		An individual may revoke an authorization at anytime except to the extent that action has already been taken based on the existing consent, or if the authorization was obtained as a condition for obtaining insurance coverage, other law provides the insurer the right to contest a claim under the policy. The revocation must be in writing.
13	164.508(b)(6). Uses and disclosures for which an authorization is required. Documentation.	Do you have a documentation process in place that includes these authorizations?		Signed authorizations must be documented and retained in original or electronic copy for six years from the date of creation or the date that it was last in effect, whichever is later.
14	164.510(a). Uses and disclosure requiring an opportunity for the individual to agree or to object. Use and disclosure for facility directories.	Do you maintain a facility directory? If so does your directory containing only the allowable PHI?		The following PHI may be used in a facility directory: Individual's name, location within the facility, condition in general terms that does not communicate specific medical information, and religious affiliation.
15	164.510(a). Uses and disclosure requiring an opportunity for the individual to agree or to object. Use and disclosure for facility directories.	Does your policy regarding your facility directory allow for disclosure only to clergy and to persons asking for the individual by name?		Disclosure of directory information is allowed to members of the clergy or to persons who, except for religious affiliation, ask for the individual by name.
16	164.510(a). Uses and disclosure requiring an opportunity for the individual to agree or to object. Use and disclosure for facility directories.	Does your policy regarding your facility directory allow for the individual to restrict or prohibit some or all of the uses of directory information?		An individual must be informed of the PHI that may be included in a directory, to whom the information may be disclosed, and provide the individual with an opportunity to restrict or prohibit some or all of the uses of the PHI.
17	164.510(a). Uses and disclosure requiring an opportunity for the individual to agree or to object. Use and disclosure for facility directories.	Does your policy regarding your facility directory allow for use or disclosure of PHI in the facility directory in emergency circumstances?		If an opportunity to object is not able to be provided due to an individual's incapacity or an emergency treatment situation, PHI may be used in a facility directory under certain guidelines. See Attachment 7 for these restrictions.
18	164.510(b). Uses and disclosure requiring an opportunity for the individual to agree or to object. Uses and disclosures for involvement in the individual's care and notification purposes.	Do you ever disclose PHI to a family member, other relative, or close personal friend of the individual?		A covered entity may disclose to a family member, other relative, or close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the care if the disclosure is in accordance with certain requirements (See Attachment 8).
19	164.510(b). Uses and disclosure requiring an opportunity for the individual to agree or to object. Uses and disclosures for involvement in the individual's care and notification purposes.	If yes to the above, does your disclosure policy meet the requirements of the regulation? (See Attachment 8).		There are requirements to be met for disclosure depending upon whether or not the individual is present (See Attachment 8).

Q#	Section/Regulation	Question	Response	Rule Comments
20	164.510(b). Uses and disclosure requiring an opportunity for the individual to agree or to object. Uses and disclosures for involvement in the individual's care and notification purposes.	Do you ever disclose PHI to notify, or assist in the notification (including identifying or locating) a family member, personal representative, or another person responsible for the individual's care of the individual's location, general condition or death?		A covered entity may disclose PHI to notify, or assist in the notification (including identifying or locating) a family member, personal representative, or another person responsible for the individual's care of the individual's location, general condition, or death if the disclosure is in accordance with certain requirements (See Attachment 8).
21	164.510(b). Uses and disclosure requiring an opportunity for the individual to agree or to object. Uses and disclosures for involvement in the individual's care and notification purposes.	If yes to the above, does your disclosure policy meet the requirements of the regulation? (See Attachment 8).		There are requirements to be met for disclosure depending upon if the individual is present or not, or the disclosure is for disaster relief purposes (See Attachment 8).
22	164.510(b). Uses and disclosure requiring an opportunity for the individual to agree or to object. Uses and disclosures for involvement in the individual's care and notification purposes.	Do you ever allow persons to act on the behalf of individuals to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of PHI? If so does your disclosure policy meet the requirements of the regulation?		A covered entity may use professional judgment and 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 these items, if the individual is not present or able to agree or object to the disclosure.
23	164.512(b). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for public health activities.	Do you ever release PHI for public health activities (i.e., surveillance, communicable disease investigations, registries, birth or deaths, product defects or problems, adverse events, etc.)?		This type of PHI may be disclosed to a health authority that is authorized by law to collect or receive such information for the purpose of preventing, or controlling disease, injury, or disability. Must be sure policy & procedures match regulation (pp. 82813 & 82814).
24	164.512(b). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for public health activities.	Do you ever release PHI to an authority authorized by law to receive reports of child abuse or neglect?		This is not restricted, but do need to review process/policies to be sure match regulation (pp 82813 & 82814).
25	164.512(b). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for public health activities.	Do you ever release PHI to a person under the jurisdiction of the Food and Drug Administration?		Disclosure is not restricted for the purpose of reporting adverse events, product defects / problems, or biological product deviations, or for tracking products, enable recalls, repairs, or replacement, or for conducting post marketing surveillance.
26	164.512(b). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for public health activities.	Do you ever release PHI to persons who may have been exposed to a communicable disease or may otherwise be at risk for contracting or spreading a disease or condition?		Disclosure is not restricted if the covered entity is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.
27	164.512(b). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for public health activities.	Do you ever release PHI to employers about a member of the employers' workforce?		This is allowed, with some restriction, if you are a provider who is a member of the employer's workforce or who provides health care at the request of the employer for medical surveillance of the workplace, or to evaluate if the individual has a work related illness or injury. (See Attachment 9 for restrictions)

Q#	Section/Regulation	Question	Response	Rule Comments
28	164.512(c). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures about victims of abuse, neglect, or domestic violence.	Do you ever disclose PHI about individuals you reasonably believe to be a victim of abuse, neglect, or domestic violence?		This is allowed, with some restrictions, if the disclosure is to a government authority, including social services or protective services authorized by law to receive such reports. (See Attachment 10 for restrictions)
29	164.512(d). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for health oversight activities.	Do you ever release information for health oversight activities (i.e., audits, civil, administrative, or criminal investigations, licensure or disciplinary actions, etc.) for appropriate oversight of the health care system, Government benefit programs (where PHI is relevant to beneficiary eligibility), or entities subject to government regulatory programs or civil rights laws where PHI is needed to determine compliance?		Disclosure is allowed for these appropriate oversight activities. However, disclosure is not allowed if the individual is the subject of the investigation or activity AND the activity is not related to receipt of health care, a claim for public health benefits, or qualification for public benefits when the patient's health is integral to the claim for public benefits.
30	164.512(e). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for judicial and administrative proceedings.	Do you ever release PHI in the course of any judicial or administrative proceedings?		A covered entity may disclose PHI in the course of judicial or administrative proceedings if certain conditions are met. (See Attachment 11 for conditions)
31	164.512(f)(1). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for law enforcement purposes. Pursuant to process and as otherwise required by law.	Do you ever release PHI to a law enforcement official pursuant to process and as otherwise required by law?		Information may be disclosed to law enforcement pursuant to process and as otherwise required by law if certain conditions are met. (See Attachment 12 for conditions)
32	164.512(f)(2). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for law enforcement purposes. Limited information for identification and location purposes	Do you ever release PHI to a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person?		The following PHI may be disclosed: name & address; date & place of birth; social security number, ABO blood type & rh factor; type of injury; date & time of treatment; date and time of death; and description of distinguishing physical characteristics (including ht, wt., gender, race, hair/eye color, scars, tattoos, and facial hair). Except as permitted above, you may not disclose PHI related to DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue for purposes of location or identification.
33	164.512(f)(3). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for law enforcement purposes. Victims of a crime.	Do you ever release PHI to a law enforcement official about victims of a crime?		Information may be disclosed to law enforcement about victims of a crime if certain conditions are met. (See Attachment 13 for conditions)

Q#	Section/Regulation	Question	Response	Rule Comments
34	164.512(f)(4). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for law enforcement purposes. Decedents.	Do you ever release PHI to a law enforcement official about a person who has died for the purpose of alerting law enforcement of the death of the individual?		This type of disclosure is allowed if you have suspicion that the death may have resulted from criminal conduct.
35	164.512(f)(5). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for law enforcement purposes. Crime on premises.	Do you ever release PHI to a law enforcement official about a criminal conduct that may have occurred on your premises?		Disclosure of PHI to a law enforcement official is allowed if you believe in good faith constitutes evidence of criminal conduct that has occurred on your premises.
36	164.512(f)(6). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for law enforcement purposes. Reporting crime in emergencies.	Do you ever release PHI to a law enforcement official, in the course of responding to a medical emergency, that may be related to criminal conduct?		Disclosure of PHI in response to a medical emergency (except if the emergency is on your premises) is allowed if such disclosure appears necessary to alert law enforcement of the commission & nature of a crime; the location or such crime or victim; the identity, description, & location of perpetrator of such crime. If the medical emergency was the result of abuse, neglect, or domestic violence, you must follow the requirements related to that type of disclosure.
37	164.512(g)(1). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and Disclosures about decedents. Coroners and medical examiners.	Do you ever release PHI information about deceased persons to coroners or medical examiners?		Disclosure of PHI to coroners and medical examiners is allowed for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
38	164.512(g)(2). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and Disclosures about decedents. Funeral directors.	Do you ever release PHI information about deceased persons to funeral directors?		Disclosure of PHI to funeral directors is allowed to the extent the disclosure is consistent with applicable law, as necessary for the directors to carry out their duties with respect to the decedent. If necessary the disclosure may be made prior to and in reasonable anticipation of the individual's death.
39	164.512(h). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for cadvaric organ, eye, or tissue donation purposes.	Do you ever release PHI information to organ procurement organizations or organizations engaged in similar functions for the purpose of organ, eye, or tissue donation and transplantation?		Disclosure of PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue is allowed, for the purpose of facilitating such donation or transplantation.
40	164.512(i). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for research purposes.	Do you ever use or disclose PHI for research?		Use and disclosure of PHI for research, regardless of the funding of the research is allowed, provided certain conditions are met. (See Attachment 14).

Q#	Section/Regulation	Question	Response	Rule Comments
41	164.512(j). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures to avert a serious threat to health or safety.	Do you ever use or disclose PHI for the purpose of averting a serious threat to health or safety?		Disclosure of PHI to avert a serious threat to health or safety is allowed, provided certain conditions are met. (See Attachment 15).
42	164.512(k)(1)(i). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Military and veterans activities. Armed Forces personnel.	Do you ever use of disclose PHI of individual who are Armed Forces personnel?		Disclosure of PHI of Armed Forces personnel is allowed for the purpose of activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. The military authority has had to have published a notice in the Federal Register that states who the appropriate military command authorities are and the purposes for which the PHI may be used or disclosed.
43	164.512(k)(1)(ii). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Military and veterans activities. Separation or discharge from military services.	This is only applicable to covered entities who are components of the Departments of Defense or Transportation.		These covered entities may disclose PHI of an individual who is a member of the Armed Forces to the Department of Veterans Affairs for the determination of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.
44	164.512(k)(1)(iii). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Military and veterans activities. Veterans.	This is only applicable to covered entities who are a component of the Department of Veteran Affairs.		These covered entities may disclose PHI to components of the Department of Veterans Affairs that determine eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.
45	164.512(k)(1)(iv). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Military and veterans activities. Foreign military personnel.	Do you ever disclose PHI of individual who are foreign military personnel?		Covered entities may disclose PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes that are permitted for Armed Forces personnel and under the same conditions.
46	164.512(k)(2). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. National security and intelligence activities.	Do you ever disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities?		Such disclosure is allowed if the national security activities are authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

Q#	Section/Regulation	Question	Response	Rule Comments
47	164.512(k)(3). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Protective services for the President and others.	Do you ever disclose PHI to authorized federal officials for the provision of protective services to the President or other persons?		Such disclosure is allowed for the protective services of the President and 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 for the conduct of investigations authorized by 18 U.S.C. 871 and 879.
48	164.512(k)(4). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Medical suitability determinations.	This is only applicable to covered entities who are a component of the Department of State.		These covered entities may use PHI to make medical suitability determinations and may disclose whether or not the individual was found to be suitable to officials in the Dept. of State for specified purposes. (See the regulation for these purposes).
49	164.512(k)(5). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Correctional institutions and other law enforcement custodial situations.	Do you ever disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual, PHI about the inmate or individual?		This disclosure is allowed if the institution or official represents such PHI is necessary for the provision of health care to the individual; the health and safety of the individual, other inmates, officers or employees of the institution, or persons transporting the individual; law enforcement on the premises of the institution; and administration and maintenance of the safety, security, and good order of the institution.
50	164.512(k)(6). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Uses and disclosures for specialized government functions. Covered entities that are government programs providing public benefits.	This is only applicable to covered entities that are health plans that are government programs providing public benefits or government agencies that administer a government program providing public benefits.		Disclosure of PHI relating to eligibility for enrollment is allowed to another government agency if the sharing of such information is in a single or combined data system accessible to all such government agencies and is required or authorized by statute or regulation, or if the programs serve similar or same populations and the disclosure is necessary to coordinate the functions of such programs.
51	164.512(l). Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required. Disclosures for workers' compensation.	Do you ever disclose PHI to workers' compensation or other similar programs?		Such disclosure is allowed 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.
52	164.514(a). Other requirements relating to uses and disclosures of protected health information. De-identification of PHI.	Do you ever use or disclose health information that does not identify an individual and where there is no reasonable basis to believe the individual can be identified?		This type of information is not considered to be individually identifiable health information, and therefore is not subject to the requirements of this regulation. However, there are requirements to be met to ensure the PHI is de-identified. (See Attachment 16)

Q#	Section/Regulation	Question	Response	Rule Comments
53	164.514(c). Other requirements relating to uses and disclosures of protected health information. Re-identification of PHI.	If you use de-identified information, do you ever have a need to re-identify the information?		A covered entity may assign a code or other means of record identification to re-identify information provided that the code or record identification is not derived from information related to the individual or otherwise capable of being translated to identify the individual; and the covered entity does not use or disclose the code or other record identification for any other purpose, and does not disclose the mechanism for re-identification.
54	164.514(d). Other requirements relating to uses and disclosures of protected health information. Minimum necessary disclosures of PHI.	Do you have policies and procedures that allow for making reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose for which it is needed?		The regulation requires that when using or disclosing PHI, or requesting PHI from another covered entity, reasonable efforts are made to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Note: This minimum necessary standard does not apply to disclosures to a provider for treatment and other exceptions as noted in the regulation (164.502(b)(2)). (See Attachment 17 for the implementation specifications of minimum necessary uses of PHI).
55	164.514(d). Other requirements relating to uses and disclosures of protected health information. Minimum necessary disclosures of PHI.	Do you have policies and procedures that identify your workforce members who need access to protected health information to carry out their duties?		A covered entity must identify persons or classes of persons in the workforce who need access to PHI to carry out their duties. Also, for each person/class of person, the entity must identify and make reasonable efforts to limit that access to the category or categories of PHI to which access is needed and any conditions appropriate to such access.
56	164.514(e). Other requirements relating to uses and disclosures of protected health information. Uses and disclosures of protected health information for marketing.	Do you use PHI for marketing purposes?		A covered entity may use PHI for marketing purposes without an authorization if the marketing communication meets certain conditions. (See Attachment 18 for the list of conditions.)
57	164.514(f). Other requirements relating to uses and disclosures of protected health information. Uses and disclosures for fundraising.	Do you use PHI for fundraising purposes?		A covered entity may use PHI for fundraising purposes without an authorization if the use or disclosure meets certain conditions. (See Attachment 19 for the conditions.)
58	164.514(g). Other requirements relating to uses and disclosures of protected health information. Uses and disclosures for underwriting and related purposes.	Do you use PHI 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?		If a health plan receives PHI for the listed purposes, and if such health insurance or health benefits are not placed with the plan, such health plan may not use or disclose the PHI for any other purpose, except as may be required by law.
59	164.514(h). Other requirements relating to uses and disclosures of protected health information. Verification requirements.	Do you have policies and procedures in place to verify the identity and authority of persons requesting PHI and for obtaining any documentation, statements, or representation that is a condition of a disclosure?		The covered entity must verify the identity and authority of persons requesting PHI and obtain any required documents for the disclosure, except for disclosures requiring and opportunity for the individual to agree or object. (See Attachment 20 for the implementation specifications related to verification procedures.)
60	164.520(a). Notice of privacy practices for protected health information. Notice of privacy practices.	Do you have a process to provide adequate notice to individuals of the uses and disclosure of PHI that you may make, and of their rights and your legal duties with respect to PHI?		Other than certain exceptions for group health plans and inmates, individuals have rights to adequate notice of the use and disclosures of their PHI that may be made. (See the regulation for a description of these exceptions.)

Q#	Section/Regulation	Question	Response	Rule Comments
61	164.520(b). Notice of privacy practices for protected health information. Content of notice.	Does your process provide a notice that contains the required elements?		The covered entity must provide a notice that is written in plain language and that contains specified elements. (See attached checklist for the required elements.)
62	164.520(b)(viii)(3). Notice of privacy practices for protected health information. Content of notice. Revisions to the notice.	Does your process provide for revisions of the notice and distribution of the changes?		When there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice, the covered entity must promptly revise and distribute its notice. (Except where required by law, such a change may not be implemented prior to the effective date of the notice in which the change is reflected.)
63	164.520(b)(1)&(2). Notice of privacy practices for protected health information. Provisions of notice. Requirements for health plans & Requirements for certain covered health care providers.	If applicable, do your processes meet the specific requirements for health plans or for health care providers that have a direct treatment relationship with an individual?		There are specific requirements for health plans and for certain covered health care providers related to the provision of the notice to individuals. (See attached checklist for the requirements.)
64	164.520(b)(3). Notice of privacy practices for protected health information. Provisions of notice. Requirements for electronic notice.	Do you maintain a web site that provides information about your customer services or benefits?		A covered entity that provides information about its customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site. (See attached checklist for further provisions of electronic notice).
65	164.520(d). Notice of privacy practices for protected health information. Joint notice by separate covered entities.	Do you participate in any organized health care arrangements?		Covered entities that participate in organized health care arrangements may comply with notice requirements by a joint notice if the joint notice meets certain conditions. (See attached checklist for these conditions)
66	164.520(e). Notice of privacy practices for protected health information. Documentation.	Do you have a process in place to document compliance with the notice?		A covered entity must document compliance with the notice requirements by retaining copies of the notices it issues for six years from the date of its creation or the date when it last was effective, whichever is later.
67	164.522(a)(1). Rights to request privacy protection for protected health information. Right of the individual to request restriction of uses and disclosures.	Do you have a process in place to allow individuals to request restrictions of PHI for treatment, payment, or health care operations, or for any disclosures permitted for involvement in care and notification purposes which require an opportunity to agree or object (164.510(b))?		A covered entity must permit an individual to request a restriction, however a covered entity is not required to agree to a restriction. If the restriction is agreed to, the entity may not violate the restriction except to provide emergency treatment. If this occurs, the entity must request that the provider not further disclose the information. Such a restriction is not effective to prevent use or disclosure permitted or required for treatment (164.502(a)(2)(i)), for facility directories (164.510(a)), or for which consent, authorization, or opportunity to agree/object is not required (164.512).
68	164.522(a)(2). Rights to request privacy protection for protected health information. Terminating a restriction.	Do you have a process in place to allow for the termination of a restriction?		A covered entity may terminate an agreement to restriction if the individual agrees to or requests termination in writing; orally agrees and agreement is documented; or the entity informs the individual of the termination (except such termination is only effective with respect to PHI created or received after it has so informed the individual).

Q#	Section/Regulation	Question	Response	Rule Comments
69	164.522(b)(1). Rights to request privacy protection for protected health information. Confidential communications requirements.	Do you have a process in place to allow for individuals to request to receive (and to accommodate such requests) communications of PHI by alternative means or at alternative locations?		Covered health care providers must permit individuals this request and must accommodate reasonable requests. Covered health plans must also permit and accommodate such requests, if the individual clearly states that the disclosure of all or part of the PHI could endanger the individual.
70	164.522(b)(2). Rights to request privacy protection for protected health information. Conditions on providing confidential communications.	Does your process to allow for individuals to request to receive (and to accommodate such requests) communications of PHI by alternative means or at alternative locations meet the implementation specifications of the regulation?		A covered entity may require the request in writing and may condition accommodation on information as to how payment, if any, will be handled (if appropriate) and specification of an alternative address or method of contact. A provider may not require an explanation as a basis for the request, but a health plan may require that a request contain a statement that the disclosure could endanger the individual.
71	164.524(a)(1). Access of individuals to protected health information. Right of access.	Do you have a policy in place to allow individuals to inspect and obtain a copy of PHI about themselves?		Individuals have the right of access to their own PHI with some exceptions. The entity may also deny access under certain circumstances. (See Attachment 21 for a description of the right of access and conditions for denial of access.)
72	164.524(b)(2). Access of individuals to protected health information. Requests for access and timely action. Timely action.	Do you have a policy in place to allow for timely responses to a request for access?		A covered entity must act on a request for access no later than 30 days after the receipt of the request, with certain conditions for the actions. (See Attachment 22 for conditions)
73	164.524(c). Access of individuals to protected health information. Provision of access.	When you grant a request for access, do your processes comply with the regulation's requirements?		A covered entity must comply with certain requirements when providing an individual with access, in whole or in part, to PHI. (See Attachment 23 for requirements)
74	164.524(d). Access of individuals to protected health information. Denial of Access.	When you deny a request for access, do your processes comply with the regulation's requirements?		A covered entity must comply with certain requirements when denying an individual access, in whole or in part, to PHI. (See Attachment 24 for requirements)
75	164.524(e). Access of individuals to protected health information. Documentation	Does your policy regarding provisions for access and denial of access include documentation and retention requirements?		A covered entity must document the designated record sets that are subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals. Such documentation must be retained for 6 years from time of creation or last effective date, whichever is later.
76	164.526(a). Amendment of protected health information. Right to amend.	Do you have a policy in place to allow individuals to amend PHI or a record about themselves?		Individuals have the right to amend their PHI or records. The entity may also deny the requested amendment under certain circumstances. (See Attachment 25 for a description of the right to amend and conditions for denial of the amendment.)
77	164.526(b)(2). Amendment of protected health information. Timely action.	Do you have a policy in place to allow for timely responses to a request for amendment?		A covered entity must act on a request for amendment no later than 60 days after the receipt of the request, with certain conditions for the actions. (See Attachment 26 for conditions.)
78	164.526(c)(1). Amendment of protected health information. Accepting the amendment. Making the amendment.	When you grant a request for amendment, do your processes comply with the regulation's requirements for making the amendment?		The appropriate amendment to the PHI or record must be made 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.

Q#	Section/Regulation	Question	Response	Rule Comments
79	164.526(c)(2). Amendment of protected health information. Accepting the amendment. Informing the individual.	When you grant a request for amendment, do your processes comply with the regulation's requirements for informing the individual?		The individual must be informed timely that the amendment is accepted, and the entity must obtain the individual's identification of and agreement to have the entity notify the relevant persons with which the amendment needs to be shared.
80	164.526(c)(3). Amendment of protected health information. Accepting the amendment. Informing others.	When you grant a request for amendment, do your processes comply with the regulation's requirements for informing others?		A reasonable effort must be made to inform and provide the amendment, within a reasonable time, to persons identified by the individual as having received PHI and needing the amendment, and persons (including business associates) that the entity knows have the PHI that is subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.
81	164.526(d)(1). Amendment of protected health information. Denying the amendment. Denial.	When you deny a request for amendment, do your processes comply with the regulation's requirements for denial?		A covered entity must comply with certain requirements when denying a request for amendment, in whole or in part, to PHI. (See Attachment 27 for requirements)
82	164.526(d)(2). Amendment of protected health information. Denying the amendment. Statement of disagreement.	Does your policy regarding denial of a request for amendment allow for a statement of disagreement from the individual?		The entity must permit the individual to submit to the 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 the statement of disagreement.
83	164.526(d)(3). Amendment of protected health information. Denying the amendment. Rebuttal statement.	Does your policy regarding denial of a request for amendment allow for a rebuttal to a statement of disagreement from the individual?		The entity may prepare a written rebuttal to the individual's statement of disagreement. A copy of such a rebuttal must be provided to the individual who submitted the statement of disagreement.
84	164.526(d)(4). Amendment of protected health information. Denying the amendment. Recordkeeping.	Does your policy regarding denial of a request for amendment allow for the record keeping of the request for amendment, the denial of the request, the statement of disagreement, and the rebuttal?		The covered entity must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link all the documents listed to the left to the designated record set.
85	164.526(d)(5). Amendment of protected health information. Denying the amendment. Future disclosures.	Does your policy regarding denial of a request for amendment allow for future disclosures which include the information about the disagreement?		If a statement of disagreement has been submitted the entity must include, with the material appended in the recordkeeping requirement, an accurate summary of any such information with subsequent disclosures of the PHI involved. If there is not statement of disagreement, the entity must include the request for amendment and denial or summary thereof with subsequent disclosures of the PHI involved. If the disclosure is being made using a standard transaction that does not permit the additional material, the covered entity may separately transmit the additional material.
86	164.526(e). Amendment of protected health information. Actions on notices of amendment.	Do you have a process for amending an individual's PHI when you are informed by another covered entity of an approved amendment?		A covered entity that is informed by another covered entity of an amendment to an individual's PHI, must amend the PHI in designated record sets.
87	164.526(f). Amendment of protected health information. Documentation.	Do you document the titles of the persons or offices responsible for receiving and processing requests for amendments?		A covered entity must document the titles of the persons or offices responsible for receiving and processing requests from individuals for amendments and retain the documentation for 6 years from date of creation or last effective date, whichever is later.

Q#	Section/Regulation	Question	Response	Rule Comments
88	164.528(a). Accounting of disclosures of protected health information. Right to an accounting of disclosures of protected health information.	Do you have processes in place to provide individuals with an accounting of disclosures of PHI made by you in the six years prior to the date on which the accounting is requested?		Individuals have the right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, with some disclosures excepted (See Attachment 28).
89	164.528(b). Accounting of disclosures of protected health information. Content of the accounting.	Do the accountings you provide in response to requests by individuals for accountings of disclosures meet all the requirements of the regulation?		There are specific requirements for the content of the accountings given in response to a request. (See Attachment 29 for these requirements.)
90	164.528(c). Accounting of disclosures of protected health information. Provision of the accounting	Do your provisions of requested accountings meet the timeliness requirements?		The covered entity must act on the individual's request no later than 60 days after receipt of such request, following certain conditions (See Attachment 30).
91	164.528(d). Accounting of disclosures of protected health information. Documentation.	Does your policy regarding provisions for accounting include documentation and retention requirements?		A covered entity must document the information required to be included in the accounting (content), the written accounting that is provided, and the titles of the persons or offices responsible for receiving and processing requests of an accounting. This documentation must be retained for 6 years from the date of creation or the last effective date, whichever is later.
92	164.530(a)(1). Administrative requirements. Personnel designations.	Does your entity have a designated privacy official?		Covered entities must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity, and a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered by the required notice.
93	164.530(b). Administrative requirements. Training	Does your entity have a program in place to provide training as required by the regulation?		A covered entity must train all members of its workforce on the policies and procedures relating to PHI, as necessary and appropriate for the workforce to carry out their function within the entity. Training must be given no later than the entity's compliance date, thereafter, to each new member of the workforce in a reasonable time frame, to each member whose functions are affected by a material change in the policies and procedures within a reasonable time frame, and the entity must document that the training has been provided.
94	164.530(c). Administrative requirements. Safeguards.	Does your entity have the appropriate safeguards in place to protect the privacy of PHI?		A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the PHI from any intentional or unintentional use or disclosure that is in violation of the regulation.
95	164.530(d). Administrative requirements. Complaints to the covered entity.	Do you have a process in place for individuals to make complaints concerning your policies and procedures that are required by the regulation or your compliance with such policies and procedures or any requirements of the regulation?		A covered entity must provide a process for individuals to make such complaints and must document all complaints received, and their disposition, if any. This documentation must be retained for 6 years from the date of creation or the last effective date, whichever is later.

Q#	Section/Regulation	Question	Response	Rule Comments
96	164.530(e). Administrative requirements. Sanctions.	Do you have a sanction policy in place to respond to members of your workforce who fail to comply with your privacy policies and procedures or the requirements of the regulation?		Covered entities are required to have such a sanction policy and must document the sanctions that are applied, if any. The sanction requirement does not apply to a member of the workforce who used or disclosed PHI that is permitted by the regulation (under 164.502) or meets the conditions for refraining from intimidating or retaliatory acts.
97	164.530(f). Administrative requirements. Mitigation.	Do you have a policy in place regarding mitigation of any harmful effect that may have occurred as a result of a use or disclosure of PHI in violation of your policies and procedures or the requirements of the regulation?		A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure in violation of its policies and procedures or the requirements of the regulation.
98	164.530(g). Administrative requirements. Refraining from intimidating or retaliatory acts.	Do you have a non-retaliation policy in place?		A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who exercised his/her rights as provided by the regulation, an individual or other person for filing a complaint with the Secretary, testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing, or for opposing any act or practice made unlawful by the regulation.
99	164.530(h). Administrative requirements. Waiver of rights.	Do any of your policies or procedures, intentionally or unintentionally require individuals to waive their rights to file a complaint of as condition to treatment, payment, enrollment in a health plan, or eligibility for benefits.		A covered entity may not require individuals to waive their rights to file a complaint (160.306) or as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
100	164.530(i). Administrative requirements. Policies and Procedures.	Do you have policies and procedures in place that are designed to comply with the requirements of the regulation and a process in place for making and implementing changes to these policies and procedures?		A covered entity must implement policies and procedures with respect to PHI that are designed to comply with the standard, implementation specifications, or other requirements of the regulation. A covered entity must change its policies and procedures as necessary and appropriate to comply with change in the law. (See Attachment 31 for the requirements related to policies and procedures and their changes).
101	164.530(j). Administrative requirements. Documentation.	Do your documentation procedures require you to maintain all required documentation, and to retain it for 6 years from the date of its creation or the date when it last was in effect, whichever is later?		A covered entity must maintain the required policies and procedures in written or electronic form, any required written communications in written or electronic form, and documentation of any required action, activity or designation in written or electronic form, for the required time period.
102	164.530(k). Administrative requirements. Group health plans	Is your entity a group health plan that may be exempt from many of the administrative requirements?		A group health plan is not subject to the standard or implementation specifications for personnel designations, training, safeguards, complaints, sanctions, mitigation, and policies and procedures if it meets certain requirements. See the regulation for these requirements.