HIPAA PRIVACY & SECURITY
COMPLIANCE CHECKLIST BY SECTION

Regulation	Description	Done Yes or No
§164.308(a)(8)	Health care provider must have a certification process in place as part of its accreditation process.	
§164.308(a)(1)(ii)(A)	Health care providers must conduct a formal risk analysis that balances the cost of security against the expected value of losses.	
§164.308(a)(1)(ii)(B)	Health care providers must have a formal risk management process that reduces risk to an acceptable level.	
§164.308(a)(1)(ii)(C)	Health care providers must establish a formal sanctions policy for misuse or misappropriation of health information and communicate it to all employees and contractors.	
§164.308(a)(3)(ii)(C)	Health care providers must establish formal termination procedures with certain mandatory implementation features.	
§164.308(a)(5)(i)	Health care providers must maintain a formal security awareness training program with certain mandatory implementation features.	
§164.308(b)(1)	Health care providers must have “Business Associate Contract” in place in which business partners agree to protect the integrity and confidentiality of data exchanged.	
§164.308(a)(7)	Health care providers must implement an applications and data criticality analysis.	
§164.308(a)(7)	Health care providers must have a data backup plan.	
§164.308(a)(7)	Health care providers must have a disaster recovery plan.	
§164.308(a)(7)	Health care providers must have an emergency mode operation plan.	

§164.308(a)(7)	Health care providers must have testing and revision procedures for all contingency plans.	
§164.308(3) (e)	Health care providers must have a formal mechanism for processing records.	
§164.308(a)(4)	Health care providers must have formal access authorization policies and procedures.	
§164.308(a)(4)	Health care providers must have formal access establishment policies and procedures.	
§164.308(a)(4)	Health care providers must have formal access modification policies and procedures.	
§164.308(a)(1)(ii)(D)	Health care providers must perform regular internal audits	
§164.308(a)(3)(ii)(A)	Health care providers must assure supervision of maintenance personnel by an authorized, knowledgeable person. Health care providers must also assure that operating and maintenance personnel have proper access authorization.	
§164.308(a)(3)(i)	Health care providers must maintain a record of access authorizations.	
§164.308(a)(3)(ii)(B)	Health care providers must establish workforce clearance procedures.	
§164.308(a)(6)(i)	Health care providers must have a formal incident response plan.	
§164.308(a)(2)	Health care providers must assign security responsibility to one or more individuals.	
§ 164.310(d)(2)(iii	Health care providers must establish media controls with certain mandatory implementation features.	
§ 164.310(a)(1)	Health care providers must establish facility access controls with certain mandatory implementation features.	
§ 164.310(b)	Health care providers must establish a policy and guidelines on workstation use.	
§164.310(c)	Health care providers must position workstations to minimize unauthorized access.	
§164.312(a)(1)	Health care providers must employ access controls with certain mandatory and certain optional implementation features.	

§164.312(b)	Health care providers must employ audit controls.	
§164.312(c)(1)	Health care providers must employ authorization controls.	
§164.312(a)(2)(iii)	Health care providers must employ authentication controls with certain mandatory and certain optional implementation features.	
§164.312(e)(1)	Health care providers that transmit health data over a network must employ integrity controls and message authentication in addition to either encryption or network access controls.	
§160.310(a)	Health care providers are required to keep records and submit reports to demonstrate HIPAA compliance.	
§160.310(b)	Health care providers are required to cooperate with compliance reviews and investigations.	
§160.310(c)(1)	Health care providers must permit access to facilities, books and records and other information (including protected health information) that is pertinent to ascertaining whether or not the provider is in compliance with HIPAA regulations.	
§164.500(b)(1)	A health care clearinghouse that is a business associate of Health care providers must comply with the restrictions on use and disclosure of protected health information set out in §164.502 in addition to the restrictions imposed by the business associate agreement. The health care clearinghouse must also comply with §164.512 relating to uses and disclosures for which consent, authorization or an opportunity to agree or object is not required.	
§164.500(b)(2)	A health care clearinghouse that creates or receives protected health information other than as a business associate of another covered entity must comply with all HIPAA standards and requirements.	
§164.502(a)	Health care providers may not use or disclose protected health information except in certain specific instances (§164.512 lists the circumstances under which consent, authorization or the opportunity to agree or object is not required.). §164.514(b) specifies the distinction between individually identifiable information and “de-identified” information.	

§164.502(a)(2)(i)	Health care providers must disclose protected health information to the patient when requested to do so.	
§164.502(a)(2)(ii)	Health care providers must disclose protected health information if required to do so as part of a compliance review or investigation.	
§164.502(b)	Health care providers are required to make reasonable efforts to limit the amount of protected health information used or disclosed to the minimum necessary to accomplish the purpose of the use or disclosure with certain exceptions including treatment, disclosures to the patient, required by law, or required for compliance.	
§164.502(c)	If Health care providers agree to a restriction on the use of protected health information, the provider is bound by that restriction. §164.522(a)(1) specifies the patient's right to request restrictions and the provider's responsibilities with respect to such requests.	
§164.502(e)(1)(i)	Health care providers must obtain satisfactory assurance from a potential business associate that the associate will appropriately safeguard protected health information before any such information may be shared with the associate with certain exceptions including treatment, to a plan sponsor, and government program providing public benefits.	
§164.502(e)(1)(iii)	If health care providers provide satisfactory assurances that it will protect information in its capacity as a business associate of another provider, it is bound by those assurances.	
§164.502(e)(2)	Health care providers must document the satisfactory assurances given by a business associate in the form of a contract, agreement or other arrangement. §164.504(e) specifies the mandatory content of these contracts.	
§164.502(f)	HIPAA privacy protections include protection of information that pertains to a deceased individual.	
§164.502(g)(1)	Health care providers must honor the patient's right to nominate one or more personal representatives to act on the patient's behalf with certain exceptions including if provider believes that the patient is the victim of abuse.	
§164.502(g)(2)	Health care providers must treat a person as a personal representative of a patient if that person has the authority to act on behalf of the patient in making health care decisions.	

§164.502(g)(3)	Health care providers must treat a parent, guardian or other person acting in loco parentis for an un-emancipated minor as a personal representative for the purposes of use or disclosure of protected health information with certain exceptions including when the minor may lawfully obtain the subject health care without parental consent.	
§164.502(g)(4)	Health care providers must treat a representative of a deceased person including executors, administrators, etc. as a personal representative for the purposes of health information protection.	
§164.502(h)	Health care providers must accommodate reasonable requests by the patient to use confidential communications channels such as being called at a work number rather than at home.	
§164.502(i)	Health care providers may not use or disclose protected health information in a manner that is inconsistent with its notice of information practices. Mandatory content is required.	
§164.504(c)(2)	A hybrid entity must ensure that the health care provider (component) does not disclose protected health information to the non-health care provider (component) of the organization.	
§164.504(c)(3)(iii)	A hybrid entity is responsible for designating the health care components of the organization.	
§164.504(d)(2)	If two health care providers (or other covered entities) are designated as affiliated (such as acting as a single covered entity) documentation of this designation must be maintained.	
§164.504(e)(1)(ii)	Health care providers that are aware of a breach of a business associate contract are out of compliance unless reasonable steps are taken to fix the breach. If these steps are unsuccessful the provider is required to either terminate the contract or notify the Secretary of DHHS.	
§164.506(b)(3)	Health care providers may not include the consent for use or disclosure of protected health information for treatment, payment or healthcare operations in the same document as the notice of information practices.	
§164.506(b)(6)	Health care providers must document and retain signed consent forms.	

§164.506(e)(1)	Health care providers that have multiple consents from a patient may use or disclose protected health information only in accordance with the more restrictive consent.	
§164.508(a)	Health care providers must obtain authorization to use or disclose protected health information for purposes other than treatment, payment or health care operations. §164.508(c-f) specifies mandatory content requirements for authorizations.	
§164.508(b)(6)	Health care providers must document and retain all signed authorizations.	
§164.510(a)(2)	Health care providers must advise a patient of protected health information that may be listed in a facility directory and provide the patient with the ability to object.	
§164.510(b)	Health care providers must provide the patient with an opportunity to object prior to revealing protected health information to family, friends, or others involved with the care of the patient.	
§164.512(c)(2)	Health care providers that discloses protected health information to a government authority concerning a victim of abuse must promptly notify the patient, with certain exceptions including when doing so would place the patient at risk.	
§164.512(i)(1):	Health care providers may not use or disclose protected health information for research without individual authorization unless a privacy board or an institutional review board has approved a waiver. The mandatory content of this waiver is set out in §164.512(i)(2). The provider must also obtain certain representations from the researcher.	
§164.512(j)(2)	Health care providers may not disclose protected health information to reduce the possibility of harm caused by a criminal act if the information is obtained as part of treatment to reduce the propensity to commit the criminal conduct.	
§164.512(j)(3)	Health care providers that discloses information to law enforcement about a patient who admits participation in a violent crime may reveal only the admission and the information specified in section §164.512(f)(2)(i) including name and address, social security number, date of birth, etc.	

§164.514(d)(2)	Health care providers must identify classes of persons who need access to protected health information to carry out their duties and must establish the levels of access needed by each person. The provider must make reasonable efforts to limit access to the minimum information required to perform an assigned job function.	
§164.514(d)(3)(i)	Health care providers must implement policies and procedures for routine disclosures to limit the information disclosed to that needed to accomplish the purpose of the disclosure.	
§164.514(d)(3)(ii)	Health care providers must develop criteria for their own non-routine disclosures to limit the information disclosed to the minimum necessary to accomplish the purpose of the disclosure. Providers must review requests for disclosure on an individual basis.	
§164.514(d)(4)(i)	Health care providers must limit requests for protected health information to the minimum necessary to accomplish the purpose for which the request is made.	
§164.514(d)(4)(ii)	Health care providers must establish policies and procedures to be used for their own routine requests for protected health information to ensure that it requests the minimum information needed to accomplish the intended purpose.	
§164.514(d)(4)(iii)	Health care providers must review each of their own non-routine request for protected health information to ensure that it requests the minimum information needed to accomplish the intended purpose.	
§164.514(d)(5)	Health care providers may not use, disclose or request an entire medical record unless they can justify needing the entire medical to accomplish the purpose of the use, disclosure or request.	
§164.514(e)(1)	Health care providers may not use protected health information for marketing except in certain specific circumstances such as face-to-face encounter, etc.).	
§164.514(e)(3)	If a health care provider uses protected health information for marketing purposes in a situation that does not require authorization, the marketing communication must contain certain specific content including a provision for the patient to opt-out.	

§164.514(f)(2)(i)	If a health care provider uses protected health information for fundraising without authorization its notice of information practices must state this fact. (§164.514(f)(1) specifies the types of information that may be used in these circumstances.	
§164.514(f)(2)(ii)	If a health care provider uses protected health information for fundraising without authorization the fundraising material must state how the patient may opt-out of future fundraising communication. (§164.514(f)(1) specifies the types of information that may be used in these circumstances.	
§164.514(f)(2)(iii)	Health care providers must make reasonable efforts to ensure that patients who opt-out of receiving fundraising communications are not sent such material.	
§164.514(h)(1)(i)	Health care providers must verify the identity of a person who requests protected health information.	
§164.514(h)(1)(ii)	Health care providers must obtain from the requestor any documents, statements or representations required before disclosing protected health information.	
§164.520(a)(1)	Health care providers, with certain exceptions including correctional institutions and group health plans must provide a notice of information practices. Mandatory content is specified.	
§164.520(c)(2)(i)	A health care provider that has a direct treatment relationship with a patient must provide notice of information practices no later than the date of the first service delivery following the compliance date for the provider.	
§164.520(c)(2)(ii)	A health care provider that maintains an office or site for delivery of service must have copies of the notice of information practices available for individuals to take with them. The provider must also post the notice in a public area where patients can read it.	
§164.520(c)(2)(iii)	A health care provider must make a revised notice of information practices available on request on or after the effective date of the revision.	
§164.520(c)(3)(i)	Health care providers that maintain a web site that provides information about the provider's services must post the notice of information practices on the web site.	
§164.520(c)(3)(ii)	Health care providers must provide a paper copy of the required notice of information practices if the provider knows that an attempt to deliver the notice electronically has failed.	

§164.520(c)(3)(iii)	If the first service to an individual is delivered electronically, the notice of information practices must be delivered contemporaneously in response to the request for service.	
§164.520(c)(3)(iv)	Health care providers must honor a request for a paper copy of the notice of information practices when the notice has previously been delivered electronically.	
§164.520(e)	Health care providers must maintain copies of all published notices of information practices as part of the required documentation.	
§164.522(a)(1)(i)	Health care providers must permit a patient to request restriction of uses and disclosures of protected health information for treatment, payment or health care operations. provider is not required to agree to the requested restriction.	
§164.522(a)(1)(iv)	If a health care provider discloses protected health information to another covered entity for emergency treatment, the provider must request that no further use of disclose the information be made.	
§164.522(b)(1)(i)	A health care provider must permit individuals to request and receive communications of protected health information by alternate means or at alternate locations.	
§164.522(b)(2)(iii)	A covered health care provider may not condition the provision of confidential communications on an explanation of the reason for the request.	
§164.522(a)(3)	Health care providers that agree to restrictions on the use or disclosure of protected health information for treatment, payment or health care operations must maintain written records of such agreements.	
§164.524(a)(1)	Health care providers must grant access to protected health information to the patient with certain exceptions including psychotherapy notes, and trial evidence.	
§164.524(a)(4)	If a health care provider has denied access to protected health information to the patient, the covered entity must allow review by a licensed health care professional (nominated by the covered entity) and must abide by the reviewer's decision.	
§164.524(b)(2)(i)	Health care providers must act on a request for access to protected health information by the	

	patient within 30 days (10 days for California Health care providers).	
§164.524(c)(1)	Health care providers must provide access to protected health information to the patient in designated record sets.	
§164.524(c)(2)(i)	Health care providers must provide access to protected health information to the patient in the form requested by the patient, if it can be produced in the requested form.	
§164.524(c)(4)	In the granting of access to protected health information, health care providers may not charge fees exceeding the cost of copying, postage and preparation of summaries or explanations.	
§164.524(d)(1)	If a health care provider denies a patient's request to access certain protected health information, the provider must allow access to all information not applicable to the denial.	
§164.524(d)(2)	If a health care provider denies a patient's request to access certain protected health information, the denial must be in writing and must contain: the basis for the denial; a statement of the patient's rights; and a description of how the patient may appeal the decision.	
§164.524(d)(3)	If a health care provider does not maintain the protected health information requested by a patient, but knows the whereabouts of the information, the provider must inform the patient where to direct the request.	
§164.524(e)(1)	Health care providers must maintain documentation of the designated record sets for which a patient may submit a request for access.	
§164.524(e)(2)	Health care providers must maintain documentation on the titles and offices responsible for receiving requests to access protected health information.	
§164.526(a)(1)	Health care providers must honor a patient's request to amend incorrect or incomplete protected health information, with certain exceptions including that the information is accurate "as is". Section §164.526(a)(2) provides specifics under which the provider may deny the request.	
§164.526(b)(2)(i)	Health care providers must act on a patient's request for amendment of protected health information within 60 days of the submission of the request. (10 days for California health care providers) §164.526(b)(2)(ii) allows for one 30-day extension if the covered entity provides the patient with the reasons for the delay.	

§164.526(b)(2)(i)(B)	Health care providers that deny a request for amendment of protected health information must notify the requestor in writing. Section §164.526(d) specifies the mandatory content of the notification and the procedures.	
§164.526(c)(1)	If a health care provider accepts a request for amendment of protected health information it must make the appropriate amendment or provide a link to the amendment in the designated record set.	
§164.526(c)(2)	If a health care provider accepts a request for amendment of protected health information it must inform the patient and obtain a list of persons with whom the amendment is to be shared.	
§164.526(c)(3)	If a health care provider accepts a request for amendment of protected health information it must make reasonable efforts to provide the amendment to all persons identified by the patient. The covered entity must also inform business associates known to have a copy of the inaccurate or incomplete information.	
§164.526(e)	A health care provider that is informed by another provider (or covered entity) of an amendment to an individual's health information must make the same amendment to its own copies of the information.	
§164.526(f)	Health care providers must maintain documentation on the titles of persons or offices responsible for processing requests for amendment of protected health information.	
§164.528(a)(1)	Health care providers must provide a patient with an accounting of disclosures of protected health information on request, with certain exceptions such as treatment, payment or health care operations. Section §164.528(b) specifies the mandatory content of the accounting.	
§164.528(a)(2)(i)	Health care providers must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official.	

§164.528(d)(1)	Health care providers must retain documentation on each disclosure of protected health information that could be the subject for a request for an accounting of disclosures. The information maintained must include all items that are required to be part of a disclosure accounting.	
§164.528(d)(2)	Health care providers are required to maintain a record of written accountings of disclosures provided to patients.	
§164.528(d)(3)	Health care providers must retain records of the titles of persons or offices responsible for receiving and processing requests for an accounting of disclosures.	
§164.530(a)(1)(i)	Health care providers must designate a privacy official who is responsible for development and implementation of privacy policies and procedures.	
§164.530(a)(1)(ii)	Health care providers must designate a contact person responsible for receiving complaints.	
§164.530(b)(1)	Health care providers must train all workforce members on the policies and procedures regarding protected health information.	
§164.530(b)(2)(ii)	Health care providers must maintain records of training that has occurred.	
§164.530(c)(1)	Health care providers must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.	
§164.530(d)(1)	Health care providers must provide a process for individuals to make complaints concerning the provider's policies and procedures.	
§164.530(d)(2)	Health care providers must maintain records of all complaints received.	
§164.530(e)(1)	Health care providers must have a sanctions policy to deal with members of the workforce who fail to comply with privacy policies and procedures.	
§164.530(e)(2)	Health care providers must maintain records of sanctions that are applied.	
§164.530(f)	Health care providers must mitigate to the extent possible the harmful effects of a violation of its privacy policies and procedures.	

§164.530(g)	Health care providers may not engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations.	
§164.530(h)	Health care providers may not require an individual to waive the right to file a complaint as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.	
§164.530(i)(1)	Health care providers must implement policies and procedures with respect to protected health information to comply with all HIPAA standards.	
§164.530(i)(2)	Health care providers must change policies and procedures to comply with changes in the law.	
§164.530(j)(1)(i)	Health care providers are required to document all policies and procedures adopted to protect the privacy of protected health information.	
§164.530(j)(1)(ii)	Health care providers are required to keep copies of all communications that are required to be in writing.	
§164.530(j)(1)(iii)	Health care providers are required to keep records of all actions, activities and designations that are required to be documented.	
§164.530(j)(2)	Health care providers must maintain all required documentation for a period of six years following its creation date or last date in effect.	