

HIPAA Cite	Topic	HIPAA Privacy Rule	CFR 42 Cite	42 CFR Part 2
<b>§164.501</b>	<b>Definitions</b>			
	Business associate	<p>A person who is not a member of the workforce and:</p> <ul style="list-style-type: none"> <li>• Performs or assists in the performance of an activity involving PHI on behalf of the covered entity or healthcare arrangement; or</li> <li>• Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services which involves use of PHI to the covered entity or healthcare arrangement</li> </ul> <p>Another covered entity can be a business associate.</p>	§2.11	<p>Qualified service organization: A person which provides services to a program (such as data processing, lab analyses, or legal, accounting, or medical services and has a written agreement:</p> <ul style="list-style-type: none"> <li>• Acknowledging it is bound by 42 CFR</li> <li>• Agreeing to resist efforts to obtain access to patient records not permitted under 42 CFR</li> </ul> <p>Another program cannot be a QSO.</p>
	Designated record set for providers	Any set of information that includes protected health information maintain, collected, used, or disseminated by or for a covered entity that constitutes the medical records and billing records about individuals or is used to make decisions about them.		
	Disclosure	Release, transfer, provision of access to, or divulging information in any other manner outside the entity.	§2.11	A communication of patient identifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the record of a patient who as been identified.
	Health oversight agency	A federal, state, or local agency or authority, or a person acting under a grant of authority from such an agency, that is authorized by law to oversee the healthcare system or related government programs		
	Individually identifiable health information	<p>Health information, including demographic information that:</p> <ul style="list-style-type: none"> <li>• Is created or received by the provider; and</li> <li>• Relates to past, present, or future physical or mental health condition, the provision of health care, or payment; and</li> <li>• Identifies or can be used to identify the individual</li> </ul>	<p>§2.11</p> <p>§2.12</p>	<p>Records: Any information, whether recorded or not, relating to a patient received or acquired by the program</p> <p>Applies to any information that identifies a patient as an alcohol or drug abuser (directly, by reference or publicly available information, or through verification) and is obtained by the program for diagnosis, referral, or treatment.</p>

			§2.13	Response to requests cannot acknowledge a patient's past or present status as a patient.
	Organized health care arrangement	<ul style="list-style-type: none"> <li>• A clinically integrated care setting in which individuals receive care from more than one provider</li> <li>• An organized system of care involving multiple entities that hold themselves out as participating in a joint arrangement and participate in joint utilization review, quality assessment and improvement, or payment activities</li> </ul>		
	Protected health information (PHI)	Individually identifiable information transmitted or maintained in any form.		
	Psychotherapy notes	<p>Counseling notes by a mental health professional documenting or analyzing content of conversation that are separated from the rest of the record. Excludes:</p> <ul style="list-style-type: none"> <li>• Medication prescription and monitoring</li> <li>• Session start and stop times</li> <li>• Modalities and frequencies of treatment</li> <li>• Results of clinical tests</li> <li>• Summary of any of the following: diagnosis, functional status, treatment plan, symptoms, prognosis, progress</li> </ul>		
	Required by law	A legal mandate that is enforceable in a court of law.		
	Research	Systematic investigation to develop or contribute to generalizable knowledge.		
<b>§164.502</b>	<b>Uses and disclosures: general rules</b>			
§164.502(a)	Standard	Entity may not use or disclose PHI except as permitted or required under the regulations.	§2.13(a)	PHI may be used or disclosed only as permitted by the regulations and may not be used in any civil, criminal, administrative, or legislative proceedings.
§164.502(a)	To the individual	No authorization required to disclose information to the individual who is the subject of the information.	§2.23(a)	No authorization required to disclose information to the patient.
§164.502(a)	Treatment	<p>Entity may use or disclose PHI to carry out treatment (in compliance with §164.506 regarding notification), including:</p> <ul style="list-style-type: none"> <li>• Provision, coordination, or management of health care and related services,</li> <li>• Consultation between health care providers,</li> <li>• Referrals for health services.</li> </ul>		
§164.502(a)	Payment	PHI may be used or disclosed to provide or obtain reimbursement for health care services (in compliance with §164.506 regarding		

		notification), including: <ul style="list-style-type: none"> <li>• Eligibility or coverage determination</li> <li>• Billing, claims management, collections</li> <li>• Review of medical necessity, appropriateness, justification</li> <li>• Utilization review</li> </ul>		
§164.502(a)	Healthcare operations	Entity may use or disclose PHI to carry out health care operations (in compliance with §164.506 regarding notification). <ul style="list-style-type: none"> <li>• Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines; population-based activities relating to improving health or reducing health care costs, case management and care coordination, contacting patients with information about treatment alternatives</li> <li>• Reviewing competence or qualifications of professionals, evaluating practitioner and provider performance, training and internships, accreditation and licensing activities</li> <li>• Underwriting and related health insurance activities</li> <li>• Conducting or arranging for medical review, legal services, and auditing functions</li> <li>• Business planning and development</li> <li>• Business management and general administrative activities</li> </ul>	§2.12(b)	No authorization required for communication within a program or between a program and an entity having direct administrative control for purposes related to provision of services.  No authorization required to disclose PHI to Qualified Service Organizations with written agreement under which QSO: <ul style="list-style-type: none"> <li>• Acknowledges it is bound by 42 CFR</li> <li>• Agrees to resist efforts to obtain access to patient records not permitted under 42 CFR</li> </ul> Information limited to that necessary for QSO to perform services for the program.
	Incidental disclosures	No authorization required for uses and disclosures made incidental to another permitted use or disclosure.		
§164.502(b)	Minimum necessary	Entity must make reasonable effort to limit request and disclosure to minimum necessary to accomplish intended purpose. Exceptions: <ul style="list-style-type: none"> <li>• Disclosures to and requests by healthcare provider for treatment</li> <li>• Disclosures to the individual</li> <li>• Disclosures made pursuant to an authorization</li> <li>• Disclosures made to DHHS Secretary under part 160 (investigations and review, etc.)</li> <li>• Disclosures required by law and limited to requirements of the law [§164.512(a)]</li> <li>• Uses and disclosures required to comply with HIPAA</li> </ul>	§2.13(a)	Disclosure limited to information required to carry out purpose.
§164.502(c)	Information subject to agreed upon restriction	Entity may not disclose contrary to agreed upon restriction, except when needed to provide emergency treatment to the individual. [§164.522(a)]		
§164.502(d)	De-identified information	<ul style="list-style-type: none"> <li>• No authorization required to use PHI or disclose PHI to a</li> </ul>	§2.12(e)	Information that does not identify the patient

		<p>business associate to de-identify.</p> <ul style="list-style-type: none"> <li>De-identified information (§164.514) not subject to HIPAA privacy rule provided code is not disclosed.</li> </ul>		as a recipient of alcohol or drug abuse services is not subject to 42 CFR Part 2.
§164.502(e)	Disclosures to business associates	<p>No authorization required with contractual or other written assurance meeting specifications in §164.504(e) that business associate will appropriately safeguard info. This does not apply to:</p> <ul style="list-style-type: none"> <li>Disclosures to health care provider concerning individual's treatment</li> <li>Disclosures by health plan to sponsor with certain conditions met</li> <li>Disclosures by government benefit program with certain conditions met</li> </ul>	§2.12	<p>No authorization required to disclose PHI to Qualified Service Organizations with written agreement under which QSO:</p> <ul style="list-style-type: none"> <li>Acknowledges it is bound by 42 CFR</li> <li>Agrees to resist efforts to obtain access to patient records not permitted under 42 CFR</li> </ul> <p>Information limited to that necessary for QSO to carry perform services for the program.</p>
§164.502(f)	Deceased individuals	HIPAA applies to PHI relating to individuals who are deceased.	§2.15(b)	42 CFR Part 2 applies to PHI relating to individuals who are deceased.
§164.502(g)	Personal representatives	<p>Entity must treat personal representative as the individual. Personal representative includes:</p> <ul style="list-style-type: none"> <li>Person authorized to make healthcare decisions for an adult or emancipated minor</li> <li>Parent, guardian or other person authorized to make healthcare decisions for a minor, unless: <ul style="list-style-type: none"> <li>Minor is authorized to consent under state law, has consented, and has not requested the person to act as personal representative (even if consent of a parent or other person has also been obtained)</li> <li>Minor may obtain services without parental consent and the minor, court, or other person has given consent</li> <li>Person authorized to make healthcare decisions for the minor agrees to confidentiality agreement between minor and provider</li> </ul> </li> <li>When a parent has authority to act as personal representative, the minor does not have authority to exercise the rights of the individual and information may be disclosed to the parent without the minor's consent (unless otherwise provided by state law).</li> <li>In all cases involving minors, state law takes precedence.</li> <li>Person authorized to act on behalf of deceased person or estate</li> </ul>	<p>§2.14</p> <p>§2.15(a)</p>	<p>Persons authorized to give authorization on patient's behalf.</p> <p>Minor patients.</p> <ul style="list-style-type: none"> <li>If a minor acting alone can legally consent to treatment, written authorization may be given only by the minor. This includes disclosures to the parent(s).</li> <li>If state law requires parental consent to treatment, written authorization must be given by both the parent and the minor.</li> <li>If state law requires parental consent to treatment, minor's application for treatment may be disclosed to parent only if minor 1) has given written authorization or 2) lacks capacity to make rational choice and poses threat to self or others.</li> </ul> <p>Incompetent adults.</p> <ul style="list-style-type: none"> <li>If patient has been adjudicated as incompetent, written authorization may be given by guardian.</li> <li>If program director determines patient suffers from medical condition that</li> </ul>

		Provider may choose not to treat a person as the individual's personal representative if the individual may be subjected to domestic violence, abuse or neglect by the personal representative and disclosure could endanger the individual.	§2.15(b)	suffers from medical condition that prevents knowing or effective action, program director may exercise right of patient authorization only to obtain payment.  Deceased adults: Legal representative or, if none, family member.
§164.502(h)	Confidential communications	Entity must accommodate reasonable requests to provide confidential communications by alternative means or in alternative locations as provided in §164.522(b).		
§164.502(i)	Uses and disclosures consistent with notice	Provider may not use or disclose information inconsistent with published privacy notice.		
§164.502(j)	Disclosures by whistleblowers to health oversight agency or attorney	No authorization required to make good faith report to health oversight agency or accreditation agency, or to consult with attorney regarding legal options.		
§164.502(j)	Disclosures by workforce members who are victims of a crime to law enforcement	No authorization to disclose suspected perpetrator's name, address, date and place of birth, SSN, blood type, type of injury, date and time of treatment, date and time of death if applicable, description of distinguishing physical characteristics.	§2.12(c)	No authorization required to report crime (or threat) on premises or against program personnel to law enforcement. Information limited to circumstances, patient status, name and address, last known location.
<b>§164.504</b>	<b>Organizational Requirements</b>			
§164.504(b), (c)	Hybrid entities	In hybrid entity, the subpart applies only to the covered component, but safeguards must be implemented to protect PHI.	§2.11	42 CFR applies only to programs: <ul style="list-style-type: none"> <li>• Individual or entity that provides alcohol or drug abuse diagnosis, treatment, or referral</li> <li>• Identified drug or alcohol abuse unit within general medical facility</li> <li>• Staff in general medical facility whose primary function is provision of alcohol or drug abuse services</li> </ul>
§164.504(d)	Affiliated entities	Legally separate covered entities that are affiliated may designate themselves as a single covered entity if under common ownership or control (able to directly or indirectly substantially influence actions or decisions). Safeguards must be implemented.		
§164.504(e)	Business associate violations	Covered entity is not in compliance if it knows of business associate activity that constitutes material breach of contract, unless it took reasonable steps to address and, if unsuccessful,		

		terminated the contract or (if termination is not feasible) reported problem to HHS Secretary.		
§164.504(e)	Business associate contracts	<p>Contract or other written arrangement must establish permitted and required uses and disclosures consistent with HIPAA and require:</p> <ul style="list-style-type: none"> <li>• No other use or disclosure except as required by law</li> <li>• Appropriate safeguards to prevent use or disclosure</li> <li>• Reporting of non-compliant uses and disclosures</li> <li>• Ensuring agents subject to same conditions and restrictions</li> <li>• Making PHI available to individuals as required by §164.524</li> <li>• Compliance with amendment requirements of §164.526</li> <li>• Accounting of disclosures to comply with §164.528</li> <li>• Making practices and records relating to use and disclosure of PHI available to HHS secretary to determine compliance</li> <li>• Returning or destroying PHI At termination of contract, if feasible, or extending protections of contract</li> </ul>	§2.12	<p>Written agreement required with Qualified Service Organizations under which QSO:</p> <ul style="list-style-type: none"> <li>• Acknowledges it is bound by 42 CFR</li> <li>• Agrees to resist efforts to obtain access to patient records not permitted under 42 CFR</li> </ul>
§164.504(f)	Group health plans	Group health plan may disclose limited information to health plan sponsor under specified conditions.		
<b>§164.506</b>	<b>Treatment, payment, and healthcare operations (TPO)</b>			
§164.506(a)	Permitted uses and disclosures	Provider may use or disclose PHI without authorization for its own treatment, payment, or healthcare operations (except for marketing purposes), and, in most cases, for treatment, payment and healthcare operations of other covered entities.	§2.12(c)	No authorization required for internal communication within a program or between a program and an entity having direct administrative control for purposes related to provision of services.
<b>§164.508</b>	<b>Authorization Required</b>			
§164.508(a)	General rule	Except as otherwise permitted or required, authorization is required for use or disclosure of PHI.		
	Psychotherapy notes	<p>Authorization is required for use or disclosure of psychotherapy notes except:</p> <ul style="list-style-type: none"> <li>• By originator for treatment</li> <li>• By entity in student training or internship program</li> <li>• To defend a legal action brought by individual</li> <li>• To Secretary for investigation or compliance</li> <li>• To comply with legal mandates</li> <li>• For health oversight activities with respect to originator</li> </ul>		

		<ul style="list-style-type: none"> <li>To coroners or medical examiners as authorized by law</li> <li>To avert a serious threat to health or safety</li> </ul>		
	Marketing	<p>Marketing is defined as any communication about a product or service that encourages purchase or use of the product or service, unless the communication is made:</p> <ul style="list-style-type: none"> <li>To describe a health-related product or service that is provided by the entity;</li> <li>For treatment of the individual; or</li> <li>For case management or care coordination, or to direct or recommend alternative treatments</li> </ul> <p>Authorization required for all marketing uses and disclosures, except:</p> <ul style="list-style-type: none"> <li>Face-to-face communications</li> <li>Promotional gifts of nominal value</li> </ul>		
§164.508(b)	Defective authorizations	<p>Authorization is not valid if:</p> <ul style="list-style-type: none"> <li>Past expiration date or event</li> <li>Required element not present or completed</li> <li>Revoked</li> <li>Combined with other document (unless exception applies)</li> <li>Material information known to be false</li> </ul>	§2.31(c)	<p>Authorization is not valid if:</p> <ul style="list-style-type: none"> <li>Past expiration date or event</li> <li>Substantially fails to conform with content requirements</li> <li>Is known to have been revoked</li> <li>Is known, or through reasonable effort could be known, to be materially false</li> </ul>
	Prohibition on conditioning	<p>Authorization may not be required as condition of treatment, payment, enrollment, or eligibility, except:</p> <ul style="list-style-type: none"> <li>Research-related treatment</li> <li>Health plan eligibility or enrollment determinations</li> <li></li> <li>Providing healthcare solely for purpose of creating PHI for disclosure to third party</li> </ul>		
	Revocation	<p>Individual may revoke authorization at any time except to the extent entity has acted on the authorization, or if authorization obtained as condition of obtaining insurance.</p>	§2.31(a) §2.35	<p>Individual may revoke authorization at any time except to the extent entity has acted on the authorization, or if specified date or event not reached in cases of criminal justice referrals.</p>
	Documentation	<p>Entity must document and retain authorizations.</p>		
§164.508(c)	Content of authorization—core elements	<p>Must be written in plain language and include:</p> <ul style="list-style-type: none"> <li>Specific description of information to be used or disclosed</li> <li>Name or specific identification of person(s) or class of persons authorized to use or disclose</li> <li>Name or specific identification of person(s) or class of</li> </ul>	§2.31(a)	<p>All authorizations must include:</p> <ul style="list-style-type: none"> <li>Specific name or general designation of the program or person making the disclosure</li> <li>Name or title of the person or</li> </ul>

		<p>persons to whom info may be disclosed</p> <ul style="list-style-type: none"> <li>• Description of each purpose</li> <li>• Expiration date or event that relates to purpose</li> <li>• Statement of right to revoke in writing, exceptions, and description of how to revoke (or reference to notice where these are described)</li> <li>• Statement that info used or disclosed may be subject to redisclosure and not protected</li> <li>• Statement of ability or inability to condition treatment or payment on signature</li> <li>• Signature of individual and date</li> <li>• If signed by personal representative, description of authority</li> </ul>		<p>organization receiving the information</p> <ul style="list-style-type: none"> <li>• Name of patient</li> <li>• Purpose</li> <li>• How much and what kind of information is to be disclosed</li> <li>• Signature of patient (and parent if required)</li> <li>• Date of signature</li> <li>• State that authorization can be revoked at any time except to the extent action has been taken on it</li> <li>• Date or event of expiration</li> </ul>
	Copy to individual	If entity seeks the authorization, individual must receive copy of signed authorization.		
			§2.35	<p>Disclosures to CJ referral sources. If patient is participating in program as condition of probation, parole, or case disposition:</p> <ul style="list-style-type: none"> <li>• Disclosure can be made only to individuals within CJ system responsible for monitoring patient progress</li> <li>• Authorization must state period of effectiveness and that authorization can be revoked only after specific period or event</li> <li>• Information can only be used for purpose of disclosure</li> </ul>
			§2.32	<p>Prohibition on Redisclosure. Each disclosure made with authorization must be accompanied by written statement prohibiting redisclosure.</p>
<b>§164.510</b>	<b>Opportunity to agree or object required</b>			
§164.510(a)	Facility directory	<ul style="list-style-type: none"> <li>• Unless the individual objects, provider may use the following information for the facility directory 1) name, 2) location in facility, 3) condition in general terms, 4) religious affiliation</li> <li>• This info may be disclosed to clergy, and, except for religious affiliation, to other people who ask for client by name.</li> </ul>		



		<ul style="list-style-type: none"> <li>• Provider must give individual opportunity to restrict or prohibit some or all of these uses or disclosures.</li> <li>• In an emergency or in the case of incapacitation, use or disclosure is permitted if consistent with any prior expressed preference of the individual and deemed to be in the individual's best interest. Opportunity to object must be provided as soon as practicable.</li> </ul>		
§164.510(b)	Involvement in client's care and notification purposes	<ul style="list-style-type: none"> <li>• No authorization is required provided individual has opportunity to agree or object (if possible).</li> <li>• Information directly relevant to the person's involvement in treatment or payment may be disclosed to family, friends, and others identified by the client.</li> <li>• Information may be used or disclosed to notify family member, personal representative, or other person responsible for care of individual of the individual's location, general condition, or death.</li> <li>• If the individual is available, entity must: 1) obtain agreement, 2) provide opportunity to object and receive none; or 3) infer from circumstances that individual does not object.</li> <li>• If the individual is not available, provider may use professional judgment to make reasonable inferences of client's best interest (includes allowing person to act on client's behalf to pick up prescriptions, supplies, X-rays, etc.)</li> <li>• Info may be used or disclosed to public or private entity authorized by law or charter to 1) assist in disaster relief or 2) coordinate involvement and notification as described above.</li> </ul>		
§164.512	<b>No authorization, or opportunity to object required</b>			
§164.512(a)	Use or disclosure required by law	<p>No authorization required to use or disclose PHI when required by law if limited to relevant requirements. Must meet the requirements for:</p> <ul style="list-style-type: none"> <li>• abuse, neglect, or domestic violence;</li> <li>• judicial and administrative proceedings; or</li> <li>• law enforcement purposes.</li> </ul>		
§164.512(b)	Public health activities	<p>No authorization required to disclose PHI to:</p> <ul style="list-style-type: none"> <li>• Public health authority authorized by law to receive info to</li> </ul>	§2.15(b)	No authorization required to report cause of death under laws requiring collection of

		<p>prevent or control disease, injury, or disability, including reporting of disease, injury, vital events such as birth and death, and conduct of public health surveillance, public health investigations, and public health interventions</p> <ul style="list-style-type: none"> <li>• Public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect</li> <li>• A person subject to the FDA to 1) report adverse events, product defects, or biological product deviations; 2) track products; 3) enable recalls, repairs, or replacement; 4) conduct post marketing surveillance.</li> <li>• A person at risk of contracting or spreading a disease or condition, if entity authorized by law to notify such person</li> <li>• An employer, about workforce member of employer, if 1) the entity is health care provider working for the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury; 2) the information disclosed consists of findings concerning the surveillance or injury; 3) the employer needs the information to comply with its legal obligations; and 4) The covered provider gives the individual written notice of the disclosure.</li> </ul>	<p>§2.12(c)</p> <p>§2.51(b)</p>	<p>death or other vital statistics or permitting inquiry into cause of death.</p> <p>No authorization required to report suspected child abuse and neglect to appropriate authorities. Authorization required to disclose information for use in proceedings resulting from the report.</p> <ul style="list-style-type: none"> <li>• No authorization required to disclose information to medical personnel of FDA who assert reason to believe health of any individual may be threatened by error in manufacture, labeling, or sale of product, and that info will be used exclusively for notifying patients and physicians of potential dangers.</li> <li>• Disclosure must be immediately documented in patient record, including 1) name of medical personnel receiving info and affiliation with any health care facility, 2) name of individual making disclosure, 3) date and time of disclosure, and 4) nature of error.</li> </ul>
§164.512(c)	Disclosure about victims of abuse, neglect, or domestic violence	<p><i>Note: Does not include reports of child abuse or neglect covered above.</i> No authorization required to disclose information about an individual if the entity reasonably believes the person to be a victim of abuse, neglect, or domestic violence to a government agency authorized by law to receive such reports:</p> <ul style="list-style-type: none"> <li>• to the extent required by law</li> <li>• if the individual agrees; or</li> <li>• to the extent the disclosure is authorized by statute or regulation and the entity believes disclosure is necessary to prevent serious harm or, if the individual is incapacitated and cannot agree, the law enforcement or other public official authorized to receive the report represents that the information is not intended to be</li> </ul>		

		<p>used against the individual and immediate enforcement activity would be materially affected by delay.</p> <p>The entity must notify the individual of the disclosure unless the entity believes it would place the individual at risk of serious harm or the covered entity would be informing a personal representative and the entity believes the representative is responsible for the neglect, abuse, or domestic violence.</p>		
§164.512(d)	Health oversight activities	<p>No authorization required to disclose 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 for oversight of:</p> <ul style="list-style-type: none"> <li>• The health care system</li> <li>• Government benefit programs for which info is relevant to eligibility</li> <li>• Entities subject to government regulatory programs for which info is necessary for determining compliance</li> <li>• Entities subject to civil rights laws for which info is necessary for determining compliance</li> </ul> <p>Does not include investigations or other activities in which the individual is the subject and the investigation or activity does not arise out of and is not directly related to 1) receipt of health care, 2) claim for public health benefits, or 3) qualification or receipt of public benefits when patient's health is integral to claim.</p>	§2.53	<p>Audit and evaluation activities.</p> <ul style="list-style-type: none"> <li>• Information may be disclosed to 1) a governmental agency that provides financial assistance or has regulatory authority, or 2) a private entity that provides financial assistance, is a third party payer, or is a peer review organization.</li> <li>• If records are copied or removed written agreement must require security protections, destruction of information after completion of audit or evaluation, and compliance with limitations on disclosure and use.</li> </ul>
§164.512(e)	Judicial and administrative proceedings	<p>No authorization required to disclose information in the course of a judicial or administrative proceeding:</p> <ul style="list-style-type: none"> <li>• In response to an order of a court or administrative tribunal; or</li> <li>• In response to subpoena, discovery request, or other lawful process, if 1) entity receives assurance (written statement and supporting documentation meeting specified criteria) that reasonable efforts have been made to ensure that individual has been given notice and opportunity to object or that reasonable efforts have been made to secure a qualified protective order, or 2) the entity makes reasonable efforts to notify the individual or obtain a qualified protective order.</li> </ul> <p>A qualified court order is an order of a court of administrative tribunal or a stipulation by the parties that:</p>	<p>§2.61</p> <p>§2.63</p>	<p>Information may be disclosed only under a unique court order meeting requirements of 42 CFR Part 2. A subpoena is not sufficient. Both the court order and a subpoena must be issued to compel disclosure.</p> <p>The court order may authorize disclosure only if disclosure is:</p> <ul style="list-style-type: none"> <li>• Necessary to protect against existing threat to life or of serious bodily injury;</li> <li>• Necessary in connection with investigation or prosecution of an extremely serious crime, such as one threatening life or serious injury; or</li> <li>• In connection with proceeding in which</li> </ul>

		<ul style="list-style-type: none"> <li>Prohibits the parties from using or disclosing PHI for any other purpose; and</li> <li>Requires the return or destruction of PHI at the end of the litigation or proceeding.</li> </ul>	<p>§2.64</p> <p>patient offers testimony or other evidence pertaining to content</p> <p>Before order is issued, patient and program must be give notice and opportunity to respond.</p> <p>Court must find that:</p> <ul style="list-style-type: none"> <li>The information cannot be obtained in other ways; and</li> <li>Public interest and need for disclosure outweigh potential injury to patient and treatment.</li> </ul> <p>Court order must:</p> <ul style="list-style-type: none"> <li>Limit disclosure to essential elements</li> <li>Limit disclosure to persons with need of information; and</li> <li>Include measure necessary to limit disclosure to protect patient</li> </ul> <p>§2.65</p> <p>Special provisions apply to court orders for purpose of criminally investigating or prosecuting patients.</p> <p>§2.67</p> <p>Special provisions apply to court orders authorizing placement of undercover agents and informants.</p>
§164.512(f)	Law enforcement purposes: pursuant to or otherwise required by law	<p>No authorization required to disclose information to law enforcement official or in compliance with:</p> <ul style="list-style-type: none"> <li>A law requiring the disclosure, including laws that require reporting of wounds (other than abuse, neglect, domestic violence)</li> <li>A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer</li> <li>A grand jury subpoena</li> <li>An administrative request (including administrative subpoena or summons, civil or authorized investigative demand, or similar process authorized under law,</li> </ul>	<p>See above.</p>

		provided that 1) the info is relevant and material to a legitimate law enforcement inquiry; 2) request is specific and limited in scope to the extent practical; and 3) de-identified information could not reasonably be used.		
	Law enforcement purposes: identification and location purposes	No authorization necessary to disclose to law enforcement officer to identify or locate a suspect, fugitive, material witness, or missing person, provided the information is limited to: <ul style="list-style-type: none"> <li>• Name and address</li> <li>• Date and place of birth</li> <li>• Social security number</li> <li>• ABO blood type and rh factor</li> <li>• Type of injury</li> <li>• Date and time of treatment</li> <li>• Date and time of death, if applicable; and</li> <li>• Description of distinguishing physical characteristics.</li> </ul> Entity may not disclose PHI related to DNA, dental records, or typing, samples, or analysis of body fluids or tissue.		
	Law enforcement purposes: crime victims	No authorization required to disclose information about a suspected victim of crime to law enforcement official upon request (other than those for public health purposes or about victims of abuse, neglect, or domestic violence, covered above) if: <ul style="list-style-type: none"> <li>• the individual agrees; or</li> <li>• the entity cannot obtain agreement because of incapacity or emergency circumstance, provided the law enforcement official represents 1) the information is needed to determine if another person has committed a crime and the information is not intended to be used against the victim, 2) the law enforcement represents that immediate enforcement activity would be materially affected by delay, and 3) the entity determines the disclosure is in the best interests of the victim.</li> </ul>		
	Law enforcement purposes: deaths	No authorization required to disclose information to law enforcement about a person who has died if the entity suspects the death may have resulted from criminal conduct.	§2.15(b)	No authorization required to report cause of death under laws permitting inquiry into cause of death.
	Law enforcement purposes: crime on premises	No authorization required to disclose information to law enforcement official if the entity believes it constitutes evidence of criminal conduct on premises.	§2.12(c)	No authorization required to report crime (or threat of crime) on premises or against program personnel to law enforcement. Information limited to circumstances, patient status, name and address, last known

				location
	Law enforcement purposes: reporting crime in emergencies	When providing emergency health care in response to medical emergency off site, entity may disclose information to law enforcement official if it appears necessary to alert enforcement to: <ul style="list-style-type: none"> <li>• Commission and nature of a crime</li> <li>• Location and victim of such crime</li> <li>• Identify, description, and perpetrator of such crime</li> </ul> Note: Excludes medical emergency resulting from abuse, neglect, or domestic violence, covered above.		
§164.512(g)	Uses and disclosures relating to the deceased	No authorization required to disclose to: <ul style="list-style-type: none"> <li>• Coroners and medical directors for the purpose of identifying a deceased person, determining cause of death, or other duties authorized by law</li> <li>• Funeral directors to carry out their duties</li> </ul>	§2.15(b)	Deceased patients. <ul style="list-style-type: none"> <li>• PHI may be disclosed to report cause of death under laws requiring collection of death or other vital statistics or permitting inquiry into cause of death.</li> <li>• Other disclosure permitted only with authorization from legal representative or, if none, family member.</li> </ul>
§164.512(h)	Organ donation (of deceased individuals)	No authorization required to disclose information to entities involved in procurement, banking, or transplantation for those purposes.		
§164.512(i)	Research	No authorization required for research, providing: <ul style="list-style-type: none"> <li>• Alteration to or waiver of required authorization approved by IRB or similar review board using specified criteria; or</li> <li>• Reviews to prepare research: Entity obtains representations from researcher that 1) use is limited to information needed to prepare for research; 2) information will not be removed from the entity by researcher; and 3) information is necessary for the research; or</li> <li>• Research related to deceased: Entity obtains documentation of death (if requested by entity) and representations from researcher that 1) use is only for research on deceased and 2) information is necessary for the research</li> </ul>	§2.52	No authorization required to disclose information for scientific research if program director determines that recipient: <ul style="list-style-type: none"> <li>• Is qualified</li> <li>• Has research protocol with appropriate security safeguards for information and prohibition on redisclosure (except to program)</li> <li>• Has provided satisfactory statement of independent review by three individuals determining 1) patients rights and welfare will be protected, and 2) benefits outweigh risks of disclosure</li> </ul>
§164.512(j)	Uses and disclosures to avert serious threat to health or safety	No authorization required if use or disclosure is consistent with laws and ethical standards and the entity believes it necessary to: <ul style="list-style-type: none"> <li>• prevent or lessen a serious and imminent threat to health or safety of a person or the public and the disclosure is to a</li> </ul>		

		<p>person reasonably able to prevent or lessen the threat, including target; or</p> <ul style="list-style-type: none"> <li>is necessary for law enforcement to identify or apprehend an individual 1) because a statement by the individual admitted participation in a violent crime that entity believes may have caused serious harm to the victim; or 2) where it appears the individual has escaped from a correctional institution.</li> </ul> <p>Disclosure under (1) is not permitted if statement made in the course of treatment to affect the propensity to commit the criminal conduct, or counseling or therapy; or through a request by the individual to initiate such treatment, counseling, or therapy.</p>		
§164.512(k)	Military and veterans activities	<p>No authorization required for:</p> <ul style="list-style-type: none"> <li>Use of disclosure of information of Armed Forces personnel or foreign military personnel necessary to assure proper execution of military operation pending military notice in Federal Register</li> <li>Entity that is component of DOD or DOT may disclose information of armed forces personnel upon separation or discharge to VA for purposes of determining eligibility for benefits</li> <li>Entity that is component of VA may disclose veteran's information to components of the VA that determine eligibility or provide benefits</li> </ul>	§2.12(c)	<p>Regulations apply to the armed forces except:</p> <ul style="list-style-type: none"> <li>Exchange of information within the armed forces; and</li> <li>Exchange of information between armed forces and health care components of the VA</li> </ul>
	National security and intelligence activities	No authorization to disclose information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by National Security Act and implementing authority.		
	Protective services for the President and others	No authorization required to disclose information to authorized federal officials for provision of protective services to the President, foreign heads of state or other persons authorized under named statutes, or to conduct inspections authorized by those laws		
	Medical suitability determinations	If entity is component of State department no authorization required to make medical suitability determinations and to disclose determination to state department personnel for specified purposes.		
	Correctional Institutions and other law enforcement custodial	No authorization required to disclose to correctional institution or law enforcement with custody of individual, if representation is made that information is necessary for:		

	situations	<ul style="list-style-type: none"> <li>• Provision of health care to the individual</li> <li>• Health and safety of individual or other inmates</li> <li>• Health and safety of correctional officers, employees, and others at the correctional institution</li> <li>• Health and safety of people responsible for transporting or transferring inmates</li> <li>• Law enforcement on the premises of the correctional institution</li> <li>• Administration and maintenance of safety, security and good order of the correctional institution</li> </ul>		
	Entities that are government programs providing public benefits	<p>No authorization required for:</p> <ul style="list-style-type: none"> <li>• A health plan to disclose information related to eligibility or reenrollment to another agency administering the program if sharing or joint maintenance of information is required or authorized by statute or regulation</li> <li>• An agency administering a benefits program to disclose information to another government benefits program if they serve similar populations and disclosure is necessary to coordinate the programs or improve their administration and management</li> </ul>		
§164.512(l)	Workers' compensation	No authorization required to comply with workers' compensation or similar programs established by law.		
			§2.34	Disclosure to prevent multiple enrollments in narcotic treatment programs. Special provisions apply.
<b>§164.514</b>	<b>Other Requirements</b>			
§164.514(a,b)	Non-identifying information	<p>Information is not individually identifiable if:</p> <p>1) A qualified person uses generally accepted statistical and scientific principles and methods for rendering information not individually identifiable and determines risk of identification is very small that information could be used to identify an individual.</p> <p>OR</p> <p>2) The following identifiers of the individual or of relatives, employers, or household members of the individual are removed and the entity does not have knowledge that the information could be used alone or in combination with other information to identify the individual:</p> <ul style="list-style-type: none"> <li>• Names</li> <li>• Geographic subdivisions smaller than a state, except the</li> </ul>	§2.12	42 CFR Part 2 only applies to information that would identify an individual as alcohol or drug abuser, either directly or by reference to other publicly available information.



		<p>initial three digits of a zip code if the geographic unit containing all zip codes with those digits contains more than 20,000 people and the initial three digits of the zip codes for all such geographic units containing 20,000 or fewer people is changed to 000</p> <ul style="list-style-type: none"> <li>• All elements of dates (except year) for dates directly related to the individual, including dates of birth, death, admission, discharge; and all ages over 89 and all elements of dates (including year) indicating such ages, except that ages and date elements may be aggregated into a single category of age 90 or older</li> <li>• Telephone numbers</li> <li>• Fax numbers</li> <li>• Electronic mail addresses</li> <li>• Social security numbers</li> <li>• Medical record numbers</li> <li>• Health plan beneficiary numbers</li> <li>• Account numbers</li> <li>• Certificate/license numbers</li> <li>• Vehicle identifiers and serial numbers, including license plate numbers</li> <li>• Device identifiers and serial numbers</li> <li>• Web universal resource locators (URLs)</li> <li>• Internet protocol (IP) address numbers</li> <li>• Biometric identifiers, including finger and voice prints</li> <li>• Full face photographic images and any comparable images</li> <li>• Any other unique identifying number, characteristic, or code</li> </ul>		
§164.514(c)	Re-identification	<p>Entity may assign code to allow information to be re-identified if the code:</p> <ul style="list-style-type: none"> <li>• Is not derived from information about the individual and cannot be used to identify the individual; and</li> <li>• Is not used or disclosed for any other purpose</li> </ul>		
§164.514(d)	Minimum necessary standard for internal use of information	<p>The entity must:</p> <ul style="list-style-type: none"> <li>• Identify members of workforce who need access to information to carry out their duties and, for each person or class of person, the categories of information needed</li> </ul>	§2.16	The entity must have written procedures which regulate and control access to and use of written records.

		<p>and any conditions appropriate to such access.</p> <ul style="list-style-type: none"> <li>• Make reasonable efforts to limit access of workforce members to the minimum necessary to carry out duties.</li> </ul>	§2.12	Restrictions on disclosure do not apply to internal communications among staff with a need for information in connection with their job duties that arise from treatment services.
	Minimum necessary standard for disclosures	<p>The entity must:</p> <ul style="list-style-type: none"> <li>• For routine and recurring disclosures, implement policies and procedures that limit disclosed information to the amount reasonably necessary to achieve purpose.</li> <li>• For all other disclosures, 1) develop criteria to limit information to the amount reasonably necessary to achieve purpose and 2) review requests on an individual basis in accordance with criteria.</li> </ul> <p>The entity may, if reasonable, rely on a requested disclosure as the minimum necessary when:</p> <ul style="list-style-type: none"> <li>• Making permitted disclosures to public officials if officials represent requested information is the minimum necessary</li> <li>• The information is requested by another covered entity</li> <li>• The information is requested by a workforce member or business associate in order to provide professional services to the entity, if representation is made the information is the minimum necessary</li> <li>• Documentation or representations that comply with applicable requirements have been provided by a person requesting information for research</li> </ul>	§2.13	All disclosures are limited to information required to carry out the purpose
	Minimum necessary standard for requests	<ul style="list-style-type: none"> <li>• The entity must limit any request to information that is reasonably necessary to achieve purpose</li> <li>• For routine and recurring requests, entity must implement policies and procedures to limit requested information to minimum necessary</li> <li>• For other requests, entity must 1) develop criteria to limit information to the amount reasonably necessary to achieve purpose and 2) review requests on an individual basis in accordance with criteria</li> </ul>		
	Entire record	When the above standards for minimum necessary apply, the entity may not use, disclose, or request an entire medical record unless specifically justified as the amount reasonably necessary to achieve purpose		

§164.514(e)	Limited data set	Entity may use or disclose a limited data set for research, treatment, payment, or health care operations if the covered entity enters into a data use agreement with the limited data set recipient to limit use, protect data, and prevent redisclosure.		
§164.514(f)	Fundraising	No authorization required to disclose information to a business associate or related foundation for the entity's own fundraising purposes if information is limited to demographic information and dates of health care provided and specified conditions are met.		
§164.514(g)	Underwriting and related purposes	If a health plan receives information for activities relating to a current or potential contract for health benefits, and does not obtain the contract, it may not use or disclose the information for other purposes except as required by law.		
§164.514(h)	Disclosure verification requirements	Except for disclosures under §164.510 requiring an opportunity for the individual to agree or object (facility directory and involvement in patient care), entity must: <ul style="list-style-type: none"> <li>• Verify identity and authority of person requesting information, if not known to entity; and</li> <li>• Obtain any required documentation, statements, or representations (oral or written) required</li> </ul>		
<b>§164.520</b>	<b>Notice of Privacy Practices</b>			
§164.520(a)	Right to notice	Individuals have a right to notice of uses and disclosures of information and of their rights and the entity's legal duties related to protected information. Exceptions provided for group health plans (under certain conditions) and correctional institutions.	§2.22(a)	Program must inform patient of federal confidentiality protection and give written summary.
§164.520(b)	Content of notice: required elements	Must be in plain language and contain these elements. <ul style="list-style-type: none"> <li>• <u>Header</u>. "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."</li> <li>• <u>Uses and disclosures</u>. 1) A description and example of uses and disclosures for each of the following: treatment, payment, and health care operations. 2) Description of each other purpose permitted or required without authorization. 3) Statement that other uses and disclosures will be made only with written authorization that can be revoked.</li> <li>• <u>Separate statement for certain uses and disclosures</u>. If applicable, separate statement required for 1) appointment reminders, 2) marketing communications, 3) fundraising, or 4)</li> </ul>	§2.22(b)	Required content: <ul style="list-style-type: none"> <li>• General description of limited circumstances under which information may be disclosed</li> <li>• Statement that violation by program is a crime and suspected violations may be reported to authorities</li> <li>• Statement that commission of crime on premises or against staff is not protected</li> <li>• Statement that reports of child abuse and neglect are not protected</li> <li>• Citation to federal law and regulations</li> </ul>

		<p>disclosure by group health plan, insurance issuer, or HMO to plan sponsor.</p> <ul style="list-style-type: none"> <li>• <u>Individual rights</u>. Description of the following rights and how they may be exercised: 1) to request restrictions on certain uses and disclosures; 2) to receive confidential communications; 3) to amend information; 4) to receive an accounting of disclosures; and 5) to receive paper copy of notice.</li> <li>• <u>Entity's duties</u>. Statement that entity must: 1) maintain privacy of information and notify individuals of legal duties and privacy practices; 2) abide by terms of current notice; and 3) right to change terms of notice (if entity desires this flexibility) and how individuals will be notified of changes.</li> <li>• <u>Complaints</u>. Notice of right to complain to entity and to Secretary of HHS if privacy rights violated and how to do so, and statement of non-retaliation.</li> <li>• <u>Contact</u>. Name or title, telephone number of person to contact for further information.</li> </ul> <p><u>Effective date</u>. First effective date, not earlier than date printed or published.</p>		Sample notice provided.
	Content of notice: optional elements	If the entity intends to limit uses or disclosures that it is permitted to make, those limitations may be described provided they do not conflict with uses required by law or permitted to avoid imminent harm.	§2.22	May include information on state law or program policy if not inconsistent with regulations.
	Revisions to notice	Notice must be promptly revised and distributed when there is a material change in content.		
§164.520(c)	Provision of notice	<p>Notice must make notice available upon request and as specified below.</p> <ul style="list-style-type: none"> <li>• <u>Health plans</u>: Requirements specified.</li> <li>• <u>Provider that has direct treatment relationship with individual</u>: 1) No later than date of first service delivery after compliance date (or as soon as practicable in an emergency). 2) Except in emergencies, must make good faith effort to obtain written acknowledgment of receipt. 3) If provider has physical service site, notice must be posted at the site and copies available for individuals to take with them. 4) When revised, make notice available upon request.</li> <li>• <u>Electronic notice</u>. If the entity has a website with</li> </ul>	§2.22(a)	Must be provided at time of admission or as soon as patient is capable of rational communication.

		<p>information about services, the notice must be prominent posted on the website. An entity may provide notice electronically if the individual has agreed. If service is delivered electronically, notice must be provided with response to individual's first request for service. Acknowledgment requirements apply.</p> <ul style="list-style-type: none"> <li>• <u>Joint notice by separate entities</u>. Entities that participate in organized health care arrangements may comply with a joint notice, with certain modifications.</li> </ul>		
§164.520(e)	Documentation	<p>An entity must maintain:</p> <ul style="list-style-type: none"> <li>• copies of the notices it issues;</li> <li>• signed acknowledgments of receipt;</li> <li>• documentation of good faith efforts and reason if acknowledgment cannot be obtained.</li> </ul>		
<b>§164.522</b>	<b>Privacy Protection Requests</b>			
§164.522(a)	Requests for restriction of uses and disclosures	<ul style="list-style-type: none"> <li>• Individuals may request entity to restrict uses and disclosures for treatment, payment, healthcare operations, and disclosures under §164.510(b) for involvement in and notification of the individual's care.</li> <li>• Entity is not required to agree to request, but if it agrees, cannot violate terms of agreement except when needed to provide emergency treatment.</li> <li>• Entity may terminate restriction if 1) the individual agrees and agreement is documented; or 2) the entity informs the individual of the termination, but such termination is only applicable to information received or created after notification.</li> </ul>		
§164.522(b)	Confidential communications	Providers must permit and accommodate reasonable requests to receive communications by alternative means or at alternative locations.		
<b>§164.534</b>	<b>Access to information</b>			
§164.524(a)(1)	Right to access	<p>Individuals have a right to inspect and obtain copies of their information for as long as the information is maintained, except for</p> <ul style="list-style-type: none"> <li>• psychotherapy notes</li> <li>• information compiled for civil, criminal or administrative action or proceeding</li> <li>• information subject to Clinical Laboratory Improvements Act.</li> </ul>	§2.23(a)	<ul style="list-style-type: none"> <li>• Regulations do not prohibit patient access to records, including opportunity to inspect and copy any records maintained about patient.</li> <li>• Program is not required to obtain written authorization in order to provide access.</li> </ul>

§164.524(a)(2) )	Grounds for denial not subject to review	<p>Access may be denied:</p> <ul style="list-style-type: none"> <li>• To an inmate if access would jeopardize the health, safety, security, custody, or rehabilitation of the individual, other inmates, or others at the correctional institution</li> <li>• If the individual is currently participating in research and consented to restricted access</li> <li>• If the information is contained in records subject to Privacy Act and grounds for denial meet requirements of that law</li> <li>• If the information was obtained from someone other than a health care provider under promise of confidentiality and access is likely to reveal the source</li> </ul>		
§164.524(a)(3) )	Grounds for denial not subject to review	<p>Access may be denied in these circumstances if the individual is given right to have the denial reviewed by a licensed professional designated by entity as reviewing official and not involved in original decision:</p> <ul style="list-style-type: none"> <li>• Licensed professional determines access is likely to endanger life or safety of individual or other person</li> <li>• Information refers to another person (not health care provider) and licensed professional determines access likely to cause substantial harm to that person</li> <li>• Request made by personal representative and licensed professional determines access by representative is likely to cause harm to individual or other person</li> </ul>		
§164.524(b)	Timely response	<ul style="list-style-type: none"> <li>• Entity may require request to be in writing.</li> <li>• Access or denial must be provided within 30 days, except for information maintained off-site, which must be handled within 60 days.</li> <li>• Entity may extend the deadline by 30 days one time if it notifies individual of the reasons for the delay and the date action will be complete.</li> </ul>		
§164.524(c)	Provision of access	<ul style="list-style-type: none"> <li>• Information must be provided in format requested if it can be readily produced in that format</li> <li>• Entity may substitute summary or give explanation of information provided if individual agrees to the arrangement and any related fees</li> <li>• Entity shall arrange convenient time and place or mail a copy of the information at individual's request</li> <li>• Reasonable, cost-based fees may be imposed for copies, summaries, and explanations</li> </ul>		

§164.524(d)	Denial of access	<ul style="list-style-type: none"> <li>• If access is denied in whole or in part, the entity must, to the extent possible, give access to other requested information.</li> <li>• Entity must provide written notice of denial that includes 1) basis; 2) review rights if applicable; and 3) procedures for filing a complaint with the entity or the Secretary of HHS.</li> <li>• If the entity does not maintain the requested information, but knows where it is maintained, it must inform the client where to request access.</li> <li>• Entity must arrange for prompt review when requested, and provide written notice of outcome within a reasonable period of time.</li> </ul>		
§164.524(e)	Documentation	<p>Entity must maintain documentation of:</p> <ul style="list-style-type: none"> <li>• Designated record set subject to access</li> <li>• Titles of persons or offices responsible for receiving requests for access</li> </ul>		
<b>§164.526</b>	<b>Amendment</b>			
§164.526(a)	Right to amend	<p>An individual has the right to amend personal information in the designated record set as long as the information is maintained. An entity may deny the request if the information:</p> <ul style="list-style-type: none"> <li>• Was not created by the entity, unless originator is no longer available</li> <li>• Is not part of designated record set</li> <li>• Would not be available for inspection under §164.524</li> <li>• Is accurate and complete</li> </ul>		
§164.526(b)	Response	<ul style="list-style-type: none"> <li>• Entity may require written request, including reason.</li> <li>• Entity must amend or deny in writing within 60 days.</li> <li>• Entity may extend deadline for 30 days one time with written notice to individual including date to complete action.</li> </ul>		
§164.526(c)	Acceptance	<p>Entity must:</p> <ul style="list-style-type: none"> <li>• Identify affected records and include a link to the location of the amendment</li> <li>• Inform individual in writing and get information and agreement for notifying others</li> <li>• Make reasonable effort to notify and provide amendment to 1) persons identified by the individual as having received the information and 2) persons the entity knows possess the information that may have relied, or could foreseeably rely, on the information to the detriment of the individual</li> </ul>		
§164.526(d)	Denial	<ul style="list-style-type: none"> <li>• Entity must provide written notice that includes 1) basis for</li> </ul>		

		<p>denial, 2) notice of right to submit statement of disagreement and how to do so, 3) notice that if individual does not submit disagreement, individual may request entity to provide request and denial with future disclosures, and 4) how to submit complaint to entity and HHS Secretary.</p> <ul style="list-style-type: none"> <li>• Entity must permit individual to submit statement of disagreement.</li> <li>• Entity may prepare rebuttal and if so must provide copy to individual.</li> <li>• Entity must identify affected records and include link to request, denial, statement of disagreement, and rebuttal, as applicable.</li> <li>• Future disclosures must include any statement of disagreement, and if requested by individual must include request and denial.</li> </ul>		
§164.526(e)	Action on notice	A entity receiving notice of amendment must amend applicable records		
§164.526(f)	Documentation	Entity must document titles of person or offices responsible for handling requests		
<b>§164.528</b>	<b>Accounting of Disclosures</b>			
§164.528(a)	Right to accounting of disclosures	<p>An individual has the right to an accounting of disclosures made over the previous six (or fewer) years, except for disclosures:</p> <ul style="list-style-type: none"> <li>• For treatment, payment, and healthcare operations</li> <li>• To the individual</li> <li>• Incidental to another use or disclosure</li> <li>• Pursuant to a written authorization</li> <li>• For the facility directory or to persons (e.g., family) involved in the individual's care or related notification purposes</li> <li>• For national security or intelligence purposes</li> <li>• To correctional or law enforcement officials having custody of the individual</li> <li>• As part of a limited data set</li> </ul> <p>A health oversight agency or law enforcement official may suspend this right under certain circumstances</p>		
§164.528(b)	Content of accounting	<p>Written accounting must include:</p> <ul style="list-style-type: none"> <li>• Date of disclosure</li> <li>• Name of entity or person receiving information</li> <li>• Description of information disclosed</li> </ul>		



		<ul style="list-style-type: none"> <li>Brief statement of purpose (or copy of request), if any</li> </ul> <p>For multiple disclosures to same person for single purpose or under single authorization, entity may describe initial disclosure, frequency or number of disclosures, and date of last disclosure. Specific provisions also given for research disclosures.</p>		
§164.528(c)	Response	<ul style="list-style-type: none"> <li>Entity must provide accounting within 60 days, but may extend deadline up to 30 days one time with written notice to individual including reason for delay and date account will be provided.</li> <li>First accounting in a 12-month period must be free of charge. Entity may impose cost-based fee for subsequent accountings if individual receives advance notice of fee and opportunity to withdraw or modify request.</li> </ul>		
§164.528(d)	Documentation	<p>Entity must document and retain:</p> <ul style="list-style-type: none"> <li>Information required in an accounting</li> <li>Written accounting provided to individual</li> <li>Titles of persons or offices responsible for handling requests</li> </ul>		
<b>§164.530</b>	<b>Administrative Requirements</b>			
§164.530(a)	Personnel designations	<p>Entity must designate and document:</p> <ul style="list-style-type: none"> <li>Privacy officer responsible for developing and implementing privacy policies and procedures</li> <li>Contact person or office responsible for receiving privacy complaints</li> </ul>		
§150.530(b)	Training	<p>Entity must train all workforce members as appropriate and necessary to job duties:</p> <ul style="list-style-type: none"> <li>No later than compliance date</li> <li>To new members within reasonable period</li> <li>When functions are affected by material change in policies and procedures</li> </ul>		
§164.530(c)	Safeguards	<p>Entity must:</p> <ul style="list-style-type: none"> <li>Have appropriate administrative, technical, and physical safeguards to protect privacy of information</li> <li>Safeguard information from intentional or unintentional use or disclosure that violates HIPAA Privacy rule</li> <li>Safeguard information to limit incidental uses or disclosures</li> </ul>	§2.16	<ul style="list-style-type: none"> <li>Records must be in secure, locked storage when not in use.</li> <li>Program shall have written procedures regulating and controlling access to and use of records.</li> </ul>

§164.530(d)	Complaints	Entity must: <ul style="list-style-type: none"> <li>• Provide a process for making complaints</li> <li>• Document all complaints and their disposition</li> </ul>		
§164.530(e)	Sanctions	Entity must apply appropriate sanctions against workforce members for violations and document all sanctions applied.		
§164.530(f)	Mitigation	Entity must, to the extent practicable, mitigate known harm resulting from violations by entity or business associate.		
§164.530(g)	Retaliation and intimidation	Entity must refrain from retaliatory or intimidating acts against individuals or others who exercise rights, file complaints, participating in investigation or compliance activity, or oppose violations through reasonable means.		
§164.530(h)	Waiver of rights	Entity may not require individual to waive right to complain to HHS Secretary as condition of treatment, payment, enrollment, or eligibility for benefits.		
§164.530(i)	Policies and procedures	Entity must implement policies and procedures designed to achieve compliance which are reasonable given its size and operations. Entity must promptly update policies and procedures (including privacy notice) as necessary to comply with changes in law and regulations. Changes to privacy notice cannot be applied to information received or created prior to date of revision unless the notice includes this provision.		
§164.530(j)	Documentation	Entity must maintain in written or electronic form: <ul style="list-style-type: none"> <li>• Policies and procedures</li> <li>• Communications required under the regulation</li> <li>• Required documentation of activities</li> </ul>		
<b>§164.532</b>	<b>Transition</b>			
§164.532	Prior authorizations	<ul style="list-style-type: none"> <li>• Entity may act in accordance with authorizations obtained prior to date of compliance, with respect to information created or received prior to date of compliance.</li> <li>• If the authorization applies to a research project, the entity may also act in accordance with respect to information obtained or received after the date of compliance.</li> <li>• If an entity agrees to a restriction requested by an individual under §164.522(a), subsequent uses or disclosures must comply with restriction.</li> </ul>		
	Business associate contracts	Entities have up to an additional year from the compliance date to revise existing business associate contracts.		

<b>§164.534</b>	<b>Compliance Dates</b>			
§164.534(a)	Health care providers	Must comply by April 14, 2003		
§164.534(b)	Health plans	Small health plans must comply by April 14, 2004; all others by April 14, 2003.		
§164.534(c)	Health care clearinghouses	Must comply by April 14, 2003		
	<b>Items not in HIPAA</b>			
			§2.12(d)	Information obtained from a CD program cannot be used to initiate or substantiate criminal charges, conduct an investigation, or prosecute the patient.
			§2.12(d)	Restrictions on disclosures apply to: <ul style="list-style-type: none"> <li>• Third party payers</li> <li>• Entities with administrative control over a program</li> <li>• Those who receive information and notice of restrictions</li> </ul>
			§2.17	Program cannot knowingly employ an undercover agent or informant without special court order.
			§2.18	Program cannot require patients to carry ID cards off site.
			§2.19	If program closes or is taken over, PHI must be purged or destroyed unless patient gives written authorization or statute requires retention. If retention mandated, records must be sealed, held in secure location, and destroyed at end of retention period.