GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Protected Info	**Nonpublic personal information (§ 6809(4)):** Personally, identifiable financial information-- • Provided by a consumer to a financial institution; • Resulting from any transaction with the consumer or any service Performed for the consumer; or • Otherwise obtained by the financial institution. **Exclusions:** Nonpublic personal information (NPI) does not include information that the financial institution has a reasonable basis to believe is lawfully made "publicly available." Information is not NPI when the financial institution has taken steps to determine: • That the information is generally made lawfully available to the public; and • That the individual can direct that it not be made public and has not done so. For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, her phone number would not be "publicly available."	**Protected health information (§ 160.103):** Protected health information means individually identifiable health information that is: i. Transmitted by electronic media; ii. Maintained in electronic media; or iii. Transmitted or maintained in any other form or medium. **Health information**: Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: 1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and 2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. **Individual identifiable health information**: Individual identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and i. Identifies the individual; or ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Protected Info (cont.)		**Exclusions:** Protected health information excludes individually identifiable health information in: i. Education records covered by the Family Educational Rights and Privacy Act (FERPA) ii. Records on a student 18 years or older which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional iii. Employment records held by a covered entity in its role as employer. iv. Regarding a person deceased over 50 years
Covered Entities	**Financial institutions (§ 6809(3)):** Any institution the business of which is engaging in financial activities. Relevant financial institutions include: a. Banks, Member Banks b. Persons providing insurance, c. Investment companies, and d. Investment advisers.	**Covered entities (§160.102-103):** (1) A health plan; (2) A health care clearinghouse; (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA
Protected Individual	**Consumers (§ 6809(9)):** Any individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.	**Individual (§160.103):** Any individual who has their health information collected by a covered entity**.**
Individual Rights		**Right of an individual to request restriction of uses and disclosures**. **(§164.522):** (i) A covered entity must permit an individual to request that the covered entity restrict: A. Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and B. Disclosures permitted under § 164.510(b).

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Individual Rights (cont.)		**Right of access. (§164.524):** Except as otherwise provided, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set. **Right to amend. (§164.526):** An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set. **Right to an accounting of disclosures of protected health information. (§164.528):** An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures: i. To individuals of protected health information about them as provided in § 164.506; ii. Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502; iii. Pursuant to an authorization as provided in § 164.502; iv. For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510; v. For national security or intelligence purposes as provided in § 164.512(k)(2); vi. To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); vii. As part of a limited data set in accordance with § 164.514(e); or viii. That occurred prior to the compliance date for the covered entity.

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Prohibition Against Disclosure of Protected Information	**(§ 6802(a)):** A financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice. **Limitations on the sharing of account number information for marketing purposes (§6802(d)):** A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.	**Disclosure (§164.502(a)):** A covered entity may not use or disclose protected health information, except either: a. As HIPAA permits or requires; or b. As the individual who is the subject of the information (or the individual's personal representative) authorizes in writing. **Required Disclosures (§164.502(a)):** A covered entity must disclose protected health information in only two situations: a. To individuals (or their personal representatives) specifically, when they request access to, or an accounting of disclosures of, their protected health information; and b. To HHS when it is undertaking a compliance investigation or review or enforcement action.

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Prohibition Against Disclosure of Protected Information (cont.)	**General exceptions (§6802(e)):** Disclosure of nonpublic personal information is permitted: (1) As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with: A. Servicing or processing a financial product or service requested or authorized by the consumer; B. Maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or C. A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer; (2) With the consent or at the direction of the consumer; (3) A. To protect the confidentiality or security of the financial B. Institution's records pertaining to the consumer, the service or product, or the transaction therein; C. To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; For required institutional risk control, or for resolving customer disputes or inquiries; D. To persons holding a legal or beneficial interest relating to the consumer; or E. To persons acting in a fiduciary or representative capacity on behalf of the consumer;	**Permitted Uses and Disclosures (§164.502(a)(1));(https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html):** A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: 1. To the Individual; 2. Treatment, Payment, and Health Care Operations; 3. Opportunity to Agree or Object; 4. Incident to an otherwise permitted use and disclosure; 5. Public Interest and Benefit Activities; and 6. Limited Data Set for the purposes of research, public health or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make. *To the Individual*. **(https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html):** A covered entity may disclose protected health information to the individual who is the subject of the information. *Treatment, Payment, Health Care Operations*. **(https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html):** A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities. A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

	Gramm-Leach-Bliley Act 15 U.S.C. § 6801	**Health Insurance Portability and Accountability Act 45 CFR § 160, 164**
Prohibition Against Disclosure of Protected Information (cont.)	(4) To provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors; (5) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 *et seq.*], to law enforcement agencies (including the Bureau of Consumer Financial Protection, a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety; (6) (A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act [15 U.S.C. 1681 et *seq.*], or (B) from a consumer report reported by a consumer reporting agency; (7) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or (8) To comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.	*Uses and Disclosures with Opportunity to Agree or Object*. **(§164.501)**: Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual. *Incidental Use and Disclosure*. **(§164.502(a)(1)(iii)):** HIPAA does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by HIPAA, and the information being shared was limited to the "minimum necessary," as required by HIPAA. *Public Interest and Benefit Activities*. **(§164.512):** HIPAA permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information. *Limited Data Set*. **(§164.514(e)):** A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Authorization	**Opt-out (§ 6802(b)(1)):** A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless - A. Such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under [15 U.S.C. §6804] that such information may be disclosed to such third party; B. The consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and C. The consumer is given an explanation of how the consumer can exercise that nondisclosure option.	**Opt-in (§164.508):** A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by HIPAA. **(§508(b)(4)):** A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. **(§164.532):** An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.
Notice Requirement	**Timing (§ 6803(a)):** Disclosure must be given at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship A covered financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, of such financial institution's policies with respect to- (1) Disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 6802 of this title, including the categories of information that may be disclosed; (2) Disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and (3) Protecting the nonpublic personal information of consumers.	**Privacy Practices Notice (§ 164.520(a);(b)):** Each covered entity, with certain exceptions, must provide a notice of its privacy practices. HIPAA requires that the notice contain certain elements. The notice must: • Describe the ways in which the covered entity may use and disclose protected health information. • State the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. • Describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. • Include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices.

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Notice Requirement (cont.)	**Information to be included (§ 6803(c)):** (1) The policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 6802 of this title, and including: A. The categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to [the general exceptions in] section 6802(e) of this title; and B. The policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution; (2) The categories of nonpublic personal information that are collected by the financial institution; (3) The policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 6801 of this title; and (4) The disclosures required, if any, under section 1681a(d)(2)(A)(iii) of this title.	**Notice Distribution. (https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html):** A covered health care provider with a direct treatment relationship with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows: a. Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery); b. By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and c. In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates. **Acknowledgement of Notice Receipt. (§164.520(c)):** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice. HIPAA does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Permitted Use	**General Exception (§6802)**: Financial institutions shall not be prohibited from the disclosure of nonpublic personal information— (1) As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with— A. Servicing or processing a financial product or service requested or authorized by the consumer; B. Maintaining or servicing the consumer's account, C. A proposed or actual securitization, secondary market sale, or similar transaction related to a transaction of the consumer; (2) With the consent or at the direction of the consumer; (3) A. To protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; B. To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; C. For required institutional risk control, or for resolving customer disputes or inquiries; D. To persons holding a legal or beneficial interest relating to the consumer; or E. To persons acting in a fiduciary or representative capacity on behalf of the consumer; (4) To provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors; (5) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety; (6) A. To a consumer reporting agency in accordance with the Fair Credit Reporting Act, or B. From a consumer report reported by a consumer reporting agency;	**Limited Disclosure (§164.502(b), 164.514(d))**: A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. **(https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html):** A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. The minimum necessary requirement is not imposed in any of the following circumstances: a. Disclosure to or a request by a health care provider for treatment; b. Disclosure to an individual who is the subject of the information, or the individual's personal representative; c. Use or disclosure made pursuant to an authorization; d. Disclosure to HHS for complaint investigation, compliance review or enforcement; e. Use or disclosure that is required by law; or f. Use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. **Access and Uses. (https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html):** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of

	Gramm-Leach-Bliley Act 15 U.S.C. § 6801	**Health Insurance Portability and Accountability Act 45 CFR § 160, 164**
Permitted Use (cont.)	(7) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or (8) To comply with Federal, State, or local laws, rules, and other applicable legal requirements. A financial institution is not prevented from providing nonpublic personal information to a nonaffiliated third party to preform services for functions on behalf of the financial institution.	
Enforcement	**State and Federal enforcement (§ 6805):** In General. Subject to subtitle B of the Consumer Financial Protection Act of 2010, this subchapter and the regulations prescribed thereunder shall be enforced by the Bureau of Consumer Financial Protection, the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction under applicable law, as follows: (1) Under section 1818 of Title 12, by the appropriate Federal banking agency, as defined in section 1813(q) of Title 12, in the case of banks. (2) Under the Federal Credit Union Act [12 U.S.C.A. § 1751 et seq.], by the Board of the National Credit Union administration with respect to any federally insured credit union, and any subsidiaries of such an entity. (3) Under the Securities Exchange Act of 1934 [15 U.S.C.A. § 78a et seq.], by the Securities and Exchange Commission with respect to any broker or dealer. (4) Under the Investment Company Act of 1940 [15 U.S.C.A. § 80a-1 et seq.], by the Securities and Exchange Commission with respect to investment companies. (5) Under the Investment Advisers Act of 1940 [15 U.S.C.A. § 80b-1 et seq.], by the Securities and Exchange Commission with respect to investment advisers registered with the Commission under such Act. (6) Under State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 6701 of this title.	**Federal enforcement (§160.404):** Penalties imposed by HHS Secretary. (b) The amount of a civil money penalty that may be imposed is subject to the following limitations: (2) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty— (i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision, (A) In the amount of less than $100 or more than $50,000 for each violation; or (B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31); (ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, (A) In the amount of less than $1,000 or more than $50,000 for each violation; or (B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31); (iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30–day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, (A) In the amount of less than $10,000 or more than $50,000 for each violation; or

GLBA / HIPAA Privacy Comparison Chart

	Gramm-Leach-Bliley Act **15 U.S.C. § 6801**	**Health Insurance Portability and Accountability Act** **45 CFR § 160, 164**
Enforcement (cont.)	**Enforcement of Non-Public Personal Information Protection (§6801)** (1) Under the Federal Trade Commission Act [15 U.S.C.A. § 41 et seq.], by the Federal Trade Commission for any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under paragraphs (1) through (6) of this subsection. (2) Under subtitle E of the Consumer Financial Protection Act of 2010, by the Bureau of Consumer Financial Protection, in the case of any financial institution and other covered person or service provider that is subject to the jurisdiction of the Bureau and any person subject to this subchapter, but not with respect to the standards under section 6801 of this title. (b) Enforcement of section 6801. **Private right of action:** No.	(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31); (iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30–day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, (A) In the amount of less than $50,000 for each violation; or (B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31). (3) If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions. **Private right of action**: No. However, at least one state supreme court has held that the HIPAA can provide the standard of care for common law negligence claims against health care providers and does not preempt these claims. ***See Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433 (2014).**