

[More Information](#)

Data protection in the United States: overview

by [Ieuan Jolly](#), Loeb & Loeb

Law stated as at 01 Jul 2017 • USA (National/Federal)

[Related Content](#)

A Q&A guide to data protection in the United States.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the data protection [Country Q&A tool](#).

This article is part of the global guide to data protection. For a full list of contents, please visit www.practicallaw.com/dataprotection-guide.

Regulation

Legislation

1. What national laws regulate the collection and use of personal data?

General laws

Not applicable.

Sectoral laws

In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. However, each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.

There are already a panoply of federal privacy-related laws that regulate the collection and use of personal data. Some apply to particular categories of information, such as financial or health information, or electronic communications. Others apply to activities that use personal information, such as

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioural Advertising.

- The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) regulates the collection, use and disclosure of financial information. It can apply broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products. GLB limits the disclosure of non-public personal information, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared. In addition, there are several Privacy Rules promulgated by national banking agencies and the Safeguards Rule, Disposal Rule, and Red Flags Rule issued by the FTC that relate to the protection and disposal of financial data.
- The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) regulates medical information. It can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information. The Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164) apply to the collection and use of protected health information (PHI). The Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) (45 C.F.R. 160 and 164) provides standards for protecting medical data. The Standards for Electronic Transactions (HIPAA Transactions Rule) (45 C.F.R. 160 and 162) applies to the electronic transmission of medical data. These HIPAA rules were revised in early 2013 under the HIPAA "Omnibus Rule".
- The HIPAA Omnibus Rule also revised the Security Breach Notification Rule (45 C.F.R. Part 164) which requires covered entities to provide notice of a breach of protected health information. Under the revised rule, a covered entity must provide notice of acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised.
- The Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer-reporting information (such as a credit card company). Consumer reports are any communication issued by a consumer reporting agency that relates to a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance.
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.) regulate the collection and use of e-mail addresses and telephone numbers, respectively.
- The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) regulate the interception of electronic communications and computer tampering, respectively. A class action complaint filed in late 2008 alleged that internet service providers (ISPs) and a targeted advertising company violated these statutes by intercepting data sent between individuals' computers and ISP servers (known as deep packet inspection). This is the same practice engaged in by Phorm in the UK and several UK telecommunications companies that resulted in an investigation by the European Commission.
- In 2016, Congress enacted the Judicial Redress Act, giving citizens of certain ally nations (notably, EU member states) the right to seek redress in US courts for privacy violations when their personal information is shared with law enforcement agencies.
- On 3 April 2017, President Donald Trump signed into law a bill that repealed a set of privacy and data security regulations for broadband internet service providers adopted by the Federal Communications Commission (FCC) in the last months of the Obama administration. The FCC adopted the Privacy Rule for broadband ISPs at the end of October 2016, after acknowledging that "the current federal privacy regime, including the important leadership of the Federal Trade Commission (FTC) and the Administration efforts to protect consumer privacy, does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks." The FCC Privacy Rule (which would have taken effect later in 2017) established a framework of customer consent required for ISPs to use and share their customers' personal information that was calibrated to the sensitivity of the information. The rules would have incorporated the controversial inclusion of browsing history and apps usage as sensitive information, requiring opt-in consent. They also would have included data security and breach notification requirements. The Federal Trade Commission (FTC), which oversees consumer privacy compliance for other

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

In addition to the above laws, there are also many guidelines issued by industry groups that are not legally enforceable but are generally considered "best practices" in those industries (such as the payment card, mobile marketing and online advertising industries). For example, the advertising industry continues to develop its self-regulatory programme for online behavioural advertising. This programme requires members of various advertising industry trade groups to comply with the groups' guidelines for online behavioural advertising, which largely mirror the FTC's guidelines. The programme includes an icon that members should place on their websites if tracking data is collected. The icon links to information about the website's data collection practices and how an individual can opt out of some online tracking. The self-regulatory programme was also expanded in 2015 to the mobile environment.

State privacy laws

There are many laws at the state level that regulate the collection and use of personal data, and the number grows each year. Some federal privacy laws pre-empt state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses pre-empts most state laws regulating the same activities. Conversely, there are many federal privacy laws that do not pre-empt state laws, which means that a company can find itself in the position of trying to comply with federal and state privacy laws that regulate the same types of data (for example, medical or health records) or types of activity.

Most states have enacted some form of privacy legislation, however California leads the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level.

California was the first state to enact a security breach notification law (California Civil Code §1798.82). The law requires any person or business that owns or licenses computerised data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorised person.

Most of the early state security breach notification laws mirrored California's law, and tended to be reactive, that is, they established requirements for responding to a security breach. More recently, a number of states laws have enacted more prescriptive and preventative laws, that is, these laws are more stringent and actually establish requirements to avoid a security breach. The best example of a preventative-type of law is the Massachusetts Regulation (201 CMR 17.00), which prescribes in considerable detail an extensive list of technical, physical and administrative security protocols aimed at protecting personal information that affected companies must implement into their security architecture, and describe in a comprehensive written information security programme.

As of April 2017, 48 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands all have enacted laws requiring notification of security breaches involving personal information. Alabama and South Dakota are the only states with no security breach law.

New laws and proposed amendments are constantly proliferating, as technological threats change and progress toward uniform federal legislation stalls. For example, California is seeing the implementation of a variety of data privacy laws and amendments it enacted in 2015 including:

- The California Electronic Communications Privacy Act (S.B. 178), which severely limits the ability of government authorities to seek electronic communication information for law enforcement purposes.
- Several amendments to security breach notification law. S.B. 570 amends the required content of security breach notices, requiring that notices clearly and conspicuously display certain prescribed headings. A.B. 964 now defines the term "encrypted" for purposes of California's breach notification law as "rendered unusable, unreadable, or indecipherable to an unauthorised person through a security technology or methodology generally accepted in the field of information security." Both amendments went into effect on 1 January 2016.
- A.B. 1541, which amends the definition of "personal information" in the state's data privacy statute to include:
 - a username or e-mail address combined with a password or security question and answer for access to an online account; and
 - health insurance information.

Scope of legislation

3. To whom do the laws apply?

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

The GLB Act. This applies to financial institutions, defined to include a range of institutions engaging in financial activities, such as banks, securities firms and insurance companies. According to the FTC, the primary enforcer of GLB, an institution must be significantly engaged in financial activities to be considered a financial institution. Whether a financial institution is significantly engaged in financial activities to come under GLB. Whether an institution is significantly engaged in financial activities is a flexible standard that takes into account all the facts and circumstances.

GLB also applies to third parties that are not financial institutions but that receive non-public personal information from non-affiliated financial institutions.

The HIPAA. This applies to covered entities and business associates. Covered entities include health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. These activities include:

- Claims processing or administration.
- Data analysis and processing.
- Quality assurance.
- Billing.
- Benefit management.
- Practice management.
- Re-pricing.

The California Security Breach Notification Law. This applies to any person or business that conducts business in California and that owns or licenses computerised data that includes personal information.

The California Online Privacy Protection Act. This applies to an operator of a commercial website, online service or mobile app, that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service.

3. What data is regulated?

The FTC Act does not regulate specific categories of data. Instead it prohibits unfair or deceptive acts or practices involving practices that fail to safeguard consumers' personal information. The FTC's Behavioural Advertising Principles apply to the tracking of a consumer's activities online over time, including the consumer's searches, web pages visits, and viewed content, to deliver advertising targeted to the individual consumer's interests.

The GLB Act applies to non-public personal information collected by a financial institution that is provided by, results from, or is otherwise obtained in connection with consumers and customers who obtain financial products or services primarily for personal, family or household purposes from a financial institution.

For the purposes of the GLB Act, a consumer is someone who has obtained a financial product or service but does not have an ongoing relationship with the financial institution (for example, someone who cashed a check with a check-cashing company or made a wire transfer or applied for a loan). A customer is a sub-set of consumers and refers to someone with an ongoing relationship with the institution. The non-public personal information that is the subject of GLB applies to information that is not publicly available and which is capable of personally identifying a consumer or customer.

The HIPAA regulates PHI, which is individually identifiable health and medical information that is maintained or transmitted by a covered entity or its business associate.

The California Security Breach Notification Law regulates personal information, which means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

- Medical information.
- Health insurance information.

Personal information also includes a user name or email address, in combination with a password or security question and answer that would permit access to an online account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

The California Online Privacy Protection Act defines personally identifiable information as individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

- A first and last name.
- A home or other physical address, including street name and name of a city or town.
- An e-mail address.
- A telephone number.
- A social security number.
- Any other identifier that allows the physical or online contacting of a specific individual.

Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described above.

4. What acts are regulated?

The FTC Act prohibits unfair or deceptive acts or practices. The FTC has used its authority to charge companies that:

- Fail to protect consumer personal data, leaving such data vulnerable to cyberattacks.
- Have changed their privacy policies without adequate notice.
- Fail to comply with a posted privacy policy.

The GLB Act regulates the collection, use, sharing and disclosure of non-public financial information. The requirements for written notice of privacy procedures and obtaining consent (and opportunities to opt-out of certain disclosures) vary depending on whether the data subject is a customer or a consumer and with whom the financial institution shares this information. One of the most onerous obligations financial institutions is to implement a security programme to protect the non-public personal information from unauthorised disclosures.

The HIPAA regulates the use and disclosure of PHI and the collection, use, maintenance or transmission of electronic PHI, and requires notice of privacy practices.

The California Security Breach Notification Law requires any person or business that conducts business in California and owns or licenses computerised data that includes personal information to disclose any security breach of this information following discovery or notification of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person. In addition, any person or business that maintains computerised data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, must be provided at no cost to the affected person for not less than 12 months.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes its

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

The Act also prohibits such operators from advertising and marketing products not legally available to minors (including alcohol, firearms, tobacco, tattoos and lottery tickets).

5. What is the jurisdictional scope of the rules?

The FTC Act and rules and guidelines promulgated under the FTC's authority apply to companies and individuals doing business in the US.

The GLB Act applies to financial institutions (which is defined very broadly, see [Question 2](#)) and to affiliated and non-affiliated third parties that receive non-public personal information from financial institutions. It also applies to persons who obtain or attempt to obtain, or cause or attempt to cause disclosure of, that non-public personal information from financial institutions through false or fraudulent means.

The HIPAA covers entities (defined in [Question 2](#)) over which the US Government has enforcement authority. However, certain business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of any US jurisdiction.

The California Security Breach Notification Law applies to any person or business that conducts business in California, and that owns or licenses computerised data that includes personal information.

The California Online Privacy Protection Act applies to an operator of a commercial website or online service that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service.

6. What are the main exemptions (if any)?

The privacy rules and guidelines issued by the FTC provide exemptions from privacy requirements for law enforcement purposes.

Under the GLB Act, a financial institution can disclose a consumer's non-public personal information with an affiliated entity if it provides notice of this practice. The financial institution does not need to obtain consent for this disclosure. An affiliated entity is any company that controls, or is controlled by, or is under common control with another company, including financial and non-financial institutions.

A financial institution can disclose a consumer's non-public personal information with a non-affiliated entity without providing the consumer the right to opt out if all the following apply:

- The disclosure is to a third party that uses the information to perform services for the financial institution.
- The financial institution provides notice of this practice.
- The financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only as intended.

A financial institution can disclose a consumer's non-public personal information with a non-affiliated entity without providing the consumer the right to opt out if the information is necessary to effect, administer or enforce a transaction. In this case, the financial institution does not need to disclose this practice to the consumer.

A financial institution can disclose non-public personal information for compliance purposes (for example, to an insurance rating organisation) and for law enforcement purposes. A financial institution can disclose publicly available financial information (such as publicly available property tax records).

The HIPAA does not apply to health information that is not personally identifiable (for example, aggregate data), and it does not apply to health information used by individuals or entities that do not fall within the definitions of covered entities or business associates of covered entities. For example, some educational and employment records (such as a report about an individual's fitness for duty used to make an employment decision) does not fall under HIPAA. There are many exemptions from the restrictions on disclosure of PHI, for example, for law enforcement purposes and to avert a serious public health threat.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

Notification

7. Is notification or registration required before processing data?

The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising and disclose that consumers can opt out of these practices, providing an opt-out mechanism.

The GLB Act requires a financial institution to provide notice of its privacy practices, but does not have the same government regulator notification or registration requirements under Directive 95/46/EC on data protection (Data Protection Directive).

The HIPAA requires a covered entity to provide notice to data subjects of its privacy practices and of data subjects' rights under HIPAA, but does not have the same government regulator notification or registration requirements as under the Data Protection Directive.

The California Security Breach Notification Law does not have the same government regulator notification or registration requirements as under the Data Protection Directive. However, if a security breach occurs, notice should be provided in certain circumstances to all affected individuals in one of the following forms:

- Written notice.
- Electronic notice, if the notice provided is consistent with national laws concerning electronic signatures (*15 U.S.C. §7001*).
- Substitute notice, if the company demonstrates that the cost of providing notice would exceed US\$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the company does not have sufficient contact information.

Substitute notice must consist of all of the following:

- E-mail notice when the company has an e-mail address for the subject persons.
- Conspicuous posting of the notice on the agency's website page, if the agency maintains one.
- Notification to major state-wide media.

However, if a company maintains its own notification procedures through an information security policy for personal information and is otherwise consistent with legal timing requirements, the company complies with the notification requirements if it notifies subject persons in accordance with its policies if there is a breach of system security. Companies must submit to the California Attorney General a copy of the notification that was sent to affected consumers.

The California Online Privacy Protection Act requires commercial websites to disclose their privacy practices, but does not have the same government regulator notification or registration requirements under the Data Protection Directive.

Main data protection rules and principles

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The FTC has used section 5 of the FTC Act to charge companies that failed to comply with their own privacy policies or failed to safeguard data they have collected. The FTC Act does not expressly require a company to have or disclose a privacy policy, but the FTC's position is that if a company discloses a privacy policy, it must comply with it. In addition, the FTC has stated that it is a violation of the FTC Act for a company to retroactively change its privacy policy without providing data subjects an opportunity to opt out of the new privacy practice.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

- Won a notable appellate victory, with the Third Circuit affirming the Commission's authority to prosecute unreasonable data security practices under section 5 of the FTC Act. The defendant hotel chain ultimately settled with the FTC, but the appellate decision was significant in ruling that the FTC could use its general consumer protection authority to crack down on inadequate security measures as unfair and deceptive and practices.
- Released guidance to help companies take the appropriate actions in the wake of a data breach, in response to reports that data breaches at numerous companies put sensitive personal information belonging to hundreds of millions of consumers at risk.
- Ensured compliance with the (now-defunct) EU-U.S. Safe Harbour framework. For example, the FTC entered settlements with 13 companies over charges that they falsely represented compliance with their self-certification requirements under Safe Harbour rules.

Some bills advanced or introduced in the 115th Congressional term (Jan. 2017 – Jan. 2018) include:

- H.R. 387 (Email Privacy Act). This amends title 18, US Code to update the privacy protections for electronic communications information that is stored by third-party service providers to protect consumer privacy interests while meeting law enforcement needs and for other purposes (introduced on 9 January 2017, passed by House on 6 Feb 2017).
- H.R. 2454 (Department of Homeland Security Data Framework Act of 2017). This directs the Secretary of Homeland Security to establish a data framework to provide access for appropriate personnel to law enforcement and other information of the Department, and for other purposes (introduced on 16 May 2017).
- H.R. 2356 (Managing Your Data Against Telecom Abuses Act of 2017, or the MY DATA Act of 2017). This prohibits providers of internet broadband services or of internet content, applications, or devices from using unfair, or deceptive acts or practices relating to privacy or data security. The Federal Trade Commission (FTC), , can promulgate regulations to carry out such prohibition after consulting with the Federal Communications Commission (FCC). (Introduced on 4 May 2017 and a similar bill, S. 984, was introduced in the Senate on 27 April 2017).
- H.R. 2520 (Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, or the "BROWSER Act"). This requires providers of broadband internet access service and edge services to:
 - clearly notify users of their privacy policies; and
 - give users opt-in or opt-out approval rights with respect to the use of, disclosure of, and access to user information collected by the providers based on the level of sensitivity of the information, and for other purposes (introduced on 18 May 2017).

The GLB Act seeks to protect consumer financial privacy by limiting when a financial institution can disclose a consumer's non-public personal information to non-affiliated third parties. Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to opt out if they don't want their information shared with certain non-affiliated third parties. (See [Question 3](#) for definitions of customer and consumer.) Another part of GLB is the Safeguards Rule, which requires companies to develop a written information security plan that describes their programme to protect customer records and information. Federal and state agencies with jurisdiction under GLB over financial institutions must implement regulations requiring the financial institutions to establish safeguards under their security programme, including safeguards that:

- Protect against unauthorised access to, or use of, these records or information, which would result in substantial harm or inconvenience to any customer. Common standards that have been suggested to restrict unauthorised access include the use of:
 - data encryption;
 - authentication mechanisms;
 - background checks; and
 - frequent monitoring and testing of the information security protocols and systems.
- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of these records.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

In addition, any entity that receives consumer financial information from a financial institution can be restricted in its reuse and re-disclosure of that information.

The HIPAA requires (with some exceptions) covered entities to:

- Use, request and disclose the minimum amount of PHI necessary to complete a transaction (*HIPAA Privacy Rule*).
- Implement data security procedures, protocols and policies at administrative, technical, physical and organisational levels to protect data (*HIPAA Security Rule*).
- Comply with certain uniform standards established for certain electronic transactions (*HIPAA Transactions Rule*).

The California Security Breach Notification Law is triggered by unauthorised disclosure of unencrypted information, so it encourages companies to encrypt the personal information of Californians. An amendment enacted in 2015 defined encryption under the law, without specifying technological standards. Another California statute, Civil Code §1798.81.5, requires certain businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus social security number, driver's licence or state ID and financial account number) and to contractually require third parties to do the same. Civil Code §§1798.85-1798.86, 1785.11.1, and 1785.11.6 restrict businesses and state and local agencies from publicly posting, displaying selling or offering to sell social security numbers and prohibit embedding social security numbers on a card or document using a bar code, chip, magnetic strip or other technology, in place of removing the number as required by law. Civil Code §§1798.80 to 1798.81 and 1798.84 require businesses to shred, erase or otherwise modify the personal information in records under their control.

For California Online Privacy Protection Act requirements, see [Question 4](#). For the requirements for these privacy policies, see [Question 12](#).

9. Is the consent of data subjects required before processing personal data?

The FTC's Behavioural Advertising Principles suggest website operators should obtain affirmative express consent (which can be provided online) before using sensitive consumer data. Sensitive data includes:

- Financial data.
- Data about children.
- Health information.
- Precise geographic location information.
- Social security numbers.

In addition, website operators that revise their privacy policies should obtain affirmative express consent before using consumer data in ways that are materially different from the privacy policy that was in effect when the data was collected. The FTC also enforces the Children's Online Privacy Protection Act which requires websites that are directed to children, or that knowingly collect personal information from children, to obtain verifiable parental consent before sharing children's personal information.

The GLB Act requires a financial institution, at the time of establishing a customer relationship, and at least annually after that, to notify customers and consumers of the institution's privacy policy and practices and allow the individual to opt-out of certain disclosures of the individual's non-public personal information. A financial institution must provide the consumer or customer with reasonable means to opt-out of certain disclosures (such means can be written, oral or electronic).

The HIPAA generally requires covered entities to obtain consent in writing from a data subject before disclosing that data (with certain exceptions, for example, to provide medical treatment). Consent must generally be in writing and contain the signature of the data subject and the date. The HIPAA Privacy Rule provides specific statements that must be included in the consent.

The California Security Breach Notification Law requires disclosure of security breaches, but does not specifically address the requirement for

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

The FTC Act does not specifically address consent (see [Question 9](#)).

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The FTC's Behavioural Advertising Principles suggest website operators should obtain affirmative express consent before using sensitive consumer data (see [Question 9](#)).

The GLB Act does not specifically address individual categories of data, however, regulators have also implemented response programme regulations requiring the financial institutions to notify the regulator (and in some cases the customer) when there has been unauthorised access to sensitive customer information.

A law relating to GLB, the Fair Credit Reporting Act (15 U.S.C. §1681), limits how consumer reports and credit card account numbers can be used and disclosed. Financial institutions are prohibited from disclosing an account number to a non-affiliated entity (other than a consumer reporting agency) for telemarketing, e-mail marketing or direct marketing purposes.

Under the HIPAA, there are specific rules regulating the disclosure of psychotherapy notes. A covered entity must generally obtain written authorisation before disclosing psychotherapy notes, even for purposes of medical treatment, medical operations or payment.

There are several California laws that provide special rules in relation to the processing, collection, transmission and disclosure of certain types of data including, without limitation:

- Financial and medical data.
- Social security numbers.
- Credit card account numbers.
- Telecommunications records.
- Radio frequency identification (RFID).
- Library records.

Rights of individuals

12. What information should be provided to data subjects at the point of collection of the personal data?

For the FTC's Behavioural Advertising Principles' recommended practices, see [Question 7](#).

The GLB Act requires a financial institution to provide notice of its privacy practices, but the timing and content of this notice depends on whether the data subject is a consumer or a customer. A customer (someone with an established and ongoing relationship with the financial institution) is entitled to receive the financial institution's privacy notice when the relationship is established and annually after that. The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices. It should describe:

- The categories of information that it collects and discloses.
- The categories of affiliated and non-affiliated entities with whom it shares information.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

- The uses and disclosures of PHI the covered entity is entitled to make (such as to receive payment from an insurance company).
- How an individual can access his information.
- How to complain about an HIPAA violation.
- An effective date.

Covered entities are not required to register with a governmental agency, but covered entities must keep records of certain disclosures of PHI.

The California Security Breach Notification Law does not specifically address information that should be provided to data subjects at the point of collection, as it focuses on requirements of disclosure of security breaches.

The privacy policy required under the California Online Privacy Protection Act must:

- Identify the categories of personally identifiable information that the operator collects through the website or online service and the categories of third-party persons or entities with whom the operator can share that personally identifiable information.
- Explain how a consumer can review his personal information collected by the operator of the website or online service, and how the consumer can make changes to that information, if the website or online service operator allows this.
- Explain how the website or online service operator notifies consumers of changes to its privacy policy.
- State the effective date of the privacy policy.

13. What other specific rights are granted to data subjects?

The FTC Act and most US privacy laws (except the HIPAA and some California laws) do not generally provide data subjects with specific access rights to their data. However, the Children's Online Privacy Protection Act allows a parent to view the personal information collected by a website about a child, and to delete and correct that information.

The GLB Act allows consumers or customers to opt-out of certain disclosures but does not generally specifically provide access rights to these individuals. In some cases, financial institutions must notify the customer when there has been unauthorised access to his sensitive customer information.

Under the HIPAA, a data subject has the right to request access to and to make corrections to his own PHI, and can (with some exceptions) request an account of the manner in which his PHI has been used or disclosed.

The California Shine the Light Law, Civil Code §§1798.83 to 1798.84 allows consumers to learn how their personal information is shared by companies for marketing purposes and encourages businesses to let their customers opt out of this. In response to a customer request, a business must provide either:

- A list of the categories of personal information disclosed to other companies for their marketing purposes during the preceding calendar year, with the companies' names and addresses.
- A privacy statement giving the customer a cost-free opportunity to opt out of this information sharing.

Financial services companies subject to the California Financial Information Privacy Act are exempted from this law.

California's student privacy law, Cal. Bus. and Prof. Code §22584, prohibits an operator of an Internet website, online service, online application, or mobile application from knowingly engaging in targeted advertising to students or their parents or legal guardians, using covered information to amass a profile about a K–12 student, selling a student's information, or disclosing covered information.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

The California Online Privacy Protection Act requires operators of web sites, online services and mobile apps that are directed to minors, or that have actual knowledge that a minor is using their site or service, to permit a minor who is a registered user to remove or request the removal of certain online information that the user posted. The law does not require companies to remove data from their servers, as long as they delete it from their websites, and the law does not apply to content for which the minor 'received compensation or other consideration.'

Security requirements

15. What security requirements are imposed in relation to personal data?

The FTC's Behavioural Advertising Principles suggest that website operators that collect and/or store consumer data for behavioural advertising should provide reasonable security for that data and should retain data only as long as is necessary to fulfil a legitimate business or law enforcement need. Consumer data protection should be based on the:

- Sensitivity of the data.
- Nature of the company's business operations.
- Types of risk a company faces.
- Reasonable protections available to a company.

The GLB Safeguards Rule requires companies to develop a written information security plan that describes their customer information protection programme. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- Designate one or more employees to co-ordinate its information security programme.
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
- Design and implement a safeguards programme, and regularly monitor and test it.
- Select service providers that can maintain appropriate safeguards, ensure contracts require them to maintain safeguards, and oversee their handling of customer information.
- Evaluate and adjust the programme in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. According to the FTC, companies should implement safeguards appropriate to their own circumstances. The FTC's Disposal Rule regulates the destruction of consumer reports. The recently issued Red Flags Rules require financial institutions and creditors to develop a written programme that identifies and detects the relevant warning signs (red flags) of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The programme must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the programme.

The HIPAA requires covered entities to:

- Use and disclose the minimum amount of PHI necessary to complete a transaction.
- Implement data security procedures and policies to protect data.
- Comply with certain standards established for electronic transactions.

There is also Guidance for Remote Use of and Access to Electronic Protected Health Information that specifically addresses the risks associated with

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

For California Online Privacy Protection Act requirements, see [Question 4](#). For the requirements for these privacy policies, see [Question 12](#).

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

48 states and the District of Columbia, Puerto Rico and the US Virgin Islands have enacted security breach notification laws. There is no federal security breach notification law, although federal bills calling for such legislation have been proposed each year for several years. State security breach notification laws typically require any person or business that owns or licenses computerised data including personal information to disclose any breach of the system security to all residents whose unencrypted personal information was acquired by an unauthorised person. These laws may also require notification to state Attorneys General. Notification can be by e-mail, post, or in state-wide media, depending on the number of affected individuals. Most laws allow an entity to delay notification for law enforcement purposes.

The HIPAA also requires certain entities including health plans and health care providers to notify individuals when their unsecured personal health information has been breached (see *45 CFR Parts 160 and 164*).

National banking regulators issued guidance encouraging certain financial institutions to notify customers if an institution determines that misuse of customer information has occurred, and to notify the appropriate banking regulator as soon as possible (Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 CFR Part 30, 12 CFR Parts 208 and 225, 12 CFR Part 364, and 12 CFR Parts 568 and 570, issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision).

Processing by third parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The FTC has issued several rules, including the Safeguards Rule, the Affiliate Sharing Rule, and the Affiliate Marketing Rule, that limit the sharing and use of financial information and credit report information with affiliates.

Under GLB, a financial institution can disclose an individual's non-public personal information with a non-affiliated entity without providing the individual the right to opt out if:

- The disclosure is to a third party that uses the information to perform services for the financial institution.
- The financial institution provides notice of this practice to the individual before sharing the information.
- The financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only for the prescribed purpose.

The HIPAA Privacy Rule allows covered entities to disclose PHI to business associates if the parties enter into an agreement that requires the business associate to agree to use the information only for the purposes for which it was engaged by the covered entity, to safeguard the information from misuse, and to assist the covered entity comply with certain of the covered entity's duties under the Privacy Rule. When a covered entity knows of a material breach or violation by the business associate of the agreement, the covered entity must take reasonable steps to cure the breach or end the violation, and if these steps are unsuccessful, to terminate the arrangement. If termination of the agreement is not feasible, a covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights.

Under the California Security Breach Notification Law, a third party that maintains computerised data including personal information the third party does not own must notify the owner or licensee of the information of any breach of data security immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person. California law also provides that a business that discloses personal information about a Californian under a contract with a non-affiliated third party must contractually require the third party to

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The FTC's Behavioural Advertising Principles are voluntary in nature. These principles suggest that website operators:

- Disclose their data collection practices tied to online behavioural advertising which rely on the use of cookies.
- Obtain affirmative consent before collecting sensitive information.
- Disclose that consumers can opt out of these practices.
- Provide a mechanism for opting out.

The advertising industry has also created a self-regulatory programme that mirrors the FTC's suggestions. The Digital Advertising Alliance (DAA) issued self-regulatory principles and in 2013 announced compliance decisions. Several decisions involved companies that failed to provide both kinds of notice, on the webpage where data is collected and on the webpage where an advertisement is displayed based on the data that was collected. Other compliance actions have resulted from websites that offered an opt-out but did not honour that opt-out for a minimum of five years.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The CAN-SPAM Act is the federal anti-spam law that applies very broadly to commercial e-mail in the US (codified at 15 U.S.C. §§7701-7713 and at 18 U.S.C. §1037). FTC Rules implementing CAN-SPAM are collected at 16 CFR Part 316. Federal Communications Commission Rules regarding text messages that are subject to CAN-SPAM are in 47 CFR 64.3100.

CAN-SPAM addresses two types of e-mail:

- **Commercial e-mail.** This is defined as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an internet website operated for a commercial purpose).
- **A transactional or relationship message.** This is a message whose primary purpose is to:
 - facilitate, complete or confirm a commercial transaction that the recipient previously agreed to enter into with the sender;
 - provide product warranty, product recall or safety information concerning a product purchased by the recipient;
 - provide account information or employment or related benefit plan information;
 - to deliver goods or services, or updates or upgrades that the recipient is entitled to receive pursuant to a transaction previously entered into with the sender.

Commercial e-mail must include the following:

- Accurate and non-misleading routing and header information, that is, "From", "To", and "Reply To" fields.
- A "Subject" line that is not deceptive.
- A notice that the recipient has the right to opt out of receiving future e-mail messages from the sender. The law does not specify where the notice must appear, but it must be clear and conspicuous. The recipient should not have to search the message to find it.
- An internet-based opt-out mechanism capable of receiving opt-out requests for at least 30 days after transmission of the message. The sender must honour an opt-out request within ten business days.
- A clear and conspicuous identification that the e-mail is an advertisement or solicitation. This requirement does not apply if the sender has the

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

- The sender's physical postal address (PO boxes and commercial mail drops that meet certain US Postal Service requirements suffice as a sender's physical postal address).

All transactional or relationship messages must include accurate and non-misleading routing information. For example, the "From" and "To" lines must not be misleading.

CAN-SPAM imposes obligations on senders and initiators. A sender is the person or entity who initiates a commercial e-mail message and whose product, service or website is advertised or promoted by the message. Some e-mails, such as in a co-branded promotion, can have multiple senders, all of whom must comply with CAN-SPAM requirements. An initiator is the person or entity who originates or transmits a commercial e-mail message, but does not include the service that is responsible solely for the routine conveyance of the message. Multiple persons or entities can qualify as initiators and can therefore all be subject to CAN-SPAM requirements.

Each separate e-mail in violation of the law is subject to penalties of up to US\$16,000, and more than one person can be held responsible for violations. For example, both the company whose product is promoted in the message and the company that originated the message can be legally responsible. E-mail that makes misleading claims about products or services can also be subject to laws outlawing deceptive advertising, such as section 5 of the FTC Act.

The CAN-SPAM Act has certain aggravated violations that can give rise to additional fines. The law provides for criminal penalties, including imprisonment, for:

- Accessing someone else's computer to send spam without permission.
- Using false information to register for multiple e-mail accounts or domain names.
- Relaying or retransmitting multiple spam messages through a computer to mislead others about the origin of the message.
- Harvesting e-mail addresses or generating them through a dictionary attack (sending e-mail to addresses made up of random letters and numbers in the hope of reaching valid ones).
- Taking advantage of open relays or open proxies without permission.

International transfer of data

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

There are few limits on the transfer of personal data outside the US. Several states have enacted laws that limit or discourage state agencies or state contractors from outsourcing data processing beyond US borders, but these laws are typically limited to state government agencies and private companies that contract to perform services for or provide goods to state agencies.

However, the position of the FTC and other regulators is that the applicable US laws and regulations still apply to the data after it leaves the US, and US regulated entities remain liable for:

- Data exported out of the US.
- The processing of data overseas by subcontractors.
- Subcontractors using the same protections (such as through the use of security safeguards, protocols, audits and contractual provisions) for the regulated data when it leaves the country.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

Data transfer agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

For years, many US companies engaging in cross-border transfers of personal data between Europe and the US had relied on the EU-US Safe Harbour programme, using European Commission (Commission) approved model contracts, or for multinationals, implementing binding corporate rules (BCRs). The Safe Harbour programme was developed by the US Department of Commerce and the Commission to address the Commission's determination that the US does not have in place a regulatory framework that provides adequate protection for personal data transferred from the European Economic Area (EEA).

In October 2015, Europe's highest court struck down the established Safe Harbour framework in its *Schrems v. Facebook* ruling. In light of the ruling, companies could no longer rely on self-certification to establish compliance with EU privacy laws. European and American regulators scrambled to find an alternative framework for trans-Atlantic data transfers and in February 2016, the US Department of Commerce and the European Commission released a new "Privacy Shield" framework, which was intended to create more robust, enforceable rights protecting data transfers. Although the EU Article 29 Working Party expressed concerns, the European Commission adopted the EU-US Privacy Shield on 12 July 2016. The Privacy Shield imposes strong obligations on companies handling data; clear safeguards and transparency obligations on US government access; effective protection of individual rights; and an annual joint review mechanism.

In addition, Congress passed the Judicial Redress Act in February 2016 to give additional civil remedies for citizens of EU member states. The Act allows citizens of ally countries (and organisations, such as the EU) to bring civil actions under the Privacy Act of 1974 for unlawful disclosure of their personal records by US government agencies.

Under GLB, before a financial institution transfers any non-public personal information, it must disclose its privacy notice and provide the individual with the opportunity to opt out of certain non-affiliated third party sharing (whether the transfer is within or outside of the US).

The HIPAA Transactions Rule covers trading partner agreements involving the exchange of information in electronic transactions. The Department of Health and Human Services has provided sample business associate agreements, but these are provided as guidance and covered entities are not required to use these sample agreements.

The California Security Breach Notification Law requires the disclosure of security breaches, but does not specifically address the use of data transfer agreements.

For California Online Privacy Protection Act requirements, see [Question 4](#), but these do not specifically address the use of data transfer agreements.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

For the FTC's Behavioural Advertising Principles' recommended practices, see [Question 7](#).

The GLB Act requires a financial institution to disclose to a customer its privacy practices and provide the customer an opportunity to opt-out of certain disclosures before transferring any non-public personal information. Because the mechanism required is an opt-out provision as opposed to an opt-in, an individual must take affirmative action to stop the transfer.

Under the HIPAA, if a business associate has signed a business associate agreement that is HIPAA compliant, and the disclosure of PHI is otherwise permitted without obtaining consent from the data subject, the agreement is generally sufficient to effect the transfer. Trading partner agreements are generally used to address the technology-relation obligations of the parties to a transaction and are generally insufficient to legitimise a transfer, where authorisation is otherwise required.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

The GLB Act does not require that a national regulator approve a data transfer agreement.

The HIPAA does not require that a national regulator approve a data transfer agreement, although a regulator may have audit powers to ensure compliance with HIPAA rules.

The California Security Breach Notification Law does not specifically address the use of data transfer agreements.

The California Online Privacy Protection Act does not specifically address the use of data transfer agreements.

Enforcement and sanctions

25. What are the enforcement powers of the national regulator?

The FTC is the primary US enforcer of national privacy laws. Although other national agencies (such as the banking agencies) are authorised to enforce various privacy laws, the FTC brings considerably more enforcement actions than the other agencies. The FTC can initiate an investigation, issue a cease and desist order, and file a complaint in court. The FTC also reports to Congress on privacy issues and recommends the enactment of required privacy legislation.

The GLB Act is enforced by the FTC, federal banking agencies, and state insurance agencies, although the FTC is more active as an enforcer than the other agencies.

The HIPAA is enforced by the Office of Civil Rights within the Department of Health and Human Services. This office can initiate an investigation into a covered entities information handling practises to determine whether it is complying with the HIPAA Privacy Rule, and allows individuals to file complaints about privacy violations.

The California Security Breach Notification Law and the California Online Privacy Protection Act are enforced by the California Attorney General and district attorneys.

26. What are the sanctions and remedies for non-compliance with data protection laws?

The FTC Act provides penalties of up to US\$16,000 for each offence. The FTC can also obtain an injunction, restitution to consumers, and repayment of investigation and prosecution costs. Criminal penalties include imprisonment for up to ten years. In 2006, a data broker agreed to pay US\$15 million to settle charges filed by the FTC for failing to adequately protect the data of millions of consumers. Settlements with government agencies can also include onerous reporting requirements, audits and monitoring by third-parties. A major retailer that settled charges of failing to adequately protect customer's credit card numbers agreed to allow comprehensive audits of its data security system for 20 years.

Penalties for violations of the GLB Act are determined by the authorising statute of the agency that brings the enforcement action. For example, an enforcement action brought by the FTC could include penalties of up to US\$16,000 per offence. Individuals who obtain, attempt to obtain, cause to be disclosed or attempt to cause to be disclosed customer information of a financial institution relating to another person through a false, fictitious or fraudulent means, can be subject to fines and/or imprisoned for up to five years. In addition, there are criminal penalties for the perpetrator of up to ten years in prison and fines of up to US\$500,000 (for an individual) and US\$1 million (for a company) if such acts are committed or attempted while violating another US law or as part of a pattern of illegal activity involving more than US\$100,000 in a year.

The HIPAA authorises civil penalties ranging from US\$100 to US\$1.5 million, depending on a number of factors, including whether the operator knew the act was a violation, whether the violation was quickly corrected and whether the operator was wilfully negligent. Criminal penalties can increase to US\$250,000 and/or up to ten years in jail if the offence was committed under false pretences or with intent to sell the data for commercial gain.

Some state and federal laws allow individuals to sue in court for privacy violations, including classes of individuals, and these can also result in

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

2017, Target agreed to pay US\$18.5 million to settle investigations by 47 states and the District of Columbia into the 2013 customer data breach. This is the largest multistate data breach settlement in history.

The Ponemon Institute calculated that in 2016 the average cost of a security breach to a company was US\$4 million up from US\$3.79 million in 2015. Breach prevention and notification is an increasingly costly proposition, with a 12% increase in per capita cost just since 2013. In addition to civil and criminal sanctions, security breaches can have far reaching consequences for companies in terms of loss of customer confidence and trust, customer churn, and loss of revenue, market share, brand and shareholder value.

Regulator details

Federal Trade Commission (FTC)

W www.ftc.gov

Main areas of responsibility. The FTC enforces the FTC Act, various rules and guidelines relating to commerce and privacy.

Department of Health and Human Services (HHS) Office of Civil Rights

W www.hhs.gov/ocr/privacy/index.html

Main areas of responsibility. The HHS Office of Civil Rights enforces HIPAA.

The California Attorney General

W <http://oag.ca.gov/>

Main areas of responsibility. The California Attorney General enforces all California laws including laws relating to commerce and privacy.

Online resources

The Federal Trade Commission Act

W www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I

Description. Unofficial website maintained by Cornell Law School with up-to-date text of Federal Trade Commission Act.

Title V of Gramm-Leach-Bliley (GLB) Act

W www.law.cornell.edu/uscode/text/15/6801

Description. Unofficial website maintained by Cornell Law School with up-to-date text of Title V of Gramm-Leach-Bliley (GLB) Act.

Health Information Privacy

W www.hhs.gov/ocr/privacy/index.html

Description. Official website containing the text of the Health Insurance Portability and Accountability Act (HIPAA) and various rules and guidelines, updated frequently.

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

Children's Online Privacy Protection Act

W www.ftc.gov/ogc/coppa1.htm

Description. Official up-to-date version of Children's Online Privacy Protection Act.

Electronic Code of Federal Regulations

W www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=fa34927e2ade43c1645fe450ea95d368&rgn=div5&view=text&node=16:1.0.1.3.36&idno=16

Description. Official version of FTC COPPA Rule, updated whenever the Rule is amended.

State of California Department of Justice

W <http://oag.ca.gov/privacy/privacy-laws>

Description. Official website of California Office of Privacy Protection which provides up-to-date text of all California and selected Federal privacy laws.

Contributor details

Ieuan Jolly, Partner

Loeb & Loeb LLP



T +1 212 407 4810

F +1 646 390 0403

E ijolly@loeb.com

W www.loeb.com

Areas of practice. Privacy; cybersecurity; data optimisation and technology-enabled transactions.

This document is free to view but most Practical Law documents require a subscription.

They can be accessed by signing in or requesting a free trial of Practical Law.

Request a Free Trial!

Request a free, no-obligation trial to Practical Law.

[Request](#)

Already a Subscriber?

Sign in to access this resource and thousands more.

[Sign In](#)

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)

Our policy towards the use of cookies

All Thomson Reuters websites use cookies to improve your online experience. They were placed on your computer when you launched this website. You can change your cookie settings through your browser.

[Read cookie policy](#) | [Close](#)