VARONIS

U.S. Data Protection

Compliance and regulations

Table of contents

Introduction

U.S. privacy and data protection laws center on securing personally identifiable information (PII) against unauthorized access. In recent years, lawmakers have focused on safeguarding consumer financial and medical information. The evolving laws and regulations try to balance consumer privacy rights against the industry's need to freely communicate data within their organizations and share data with partners. With more data available online via social media, public databases, etc. — and because of the blurring of lines between PII and other personal data — regulators are looking to broaden the types of data that should be protected.

In recent years, federal lawmakers have focused on safeguarding consumer financial and medical information.

In this whitepaper, we survey key U.S. consumer data protection and privacy legislation, including the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and the Health Insurance Portability and Accountability Act (HIPAA). We also review recent guidelines from the Federal Trade Commission (FTC) that may suggest what new legal protections for digital identifiers will look like in the coming years. Finally, we consider the role that unstructured data plays in an organization's data-protection strategies.

The privacy landscape

Data privacy considerations in the U.S. can be traced to the nation's first communications "network" — the colonial mail delivery system[1]. While the technologies have advanced beyond what our founders might have imagined, these same concerns still shape our information laws. We expect that our transactions with service providers are private, and the personal data being transferred and maintained is secured against unauthorized access.

The rise of the internet in the 1990s, along with massive amounts of consumer data collected and shared by companies, has brought data privacy into sharper focus. At the core of the relevant laws and regulations is a view of what data types should be protected. These rules each try to answer the question, "What is personal data?" In many cases, the data protected against unauthorized access or disclosure is an identifier. In the U.S., this data is referred to as PII data (e.g., a name, address, social security number, or phone number). However, depending on the law — for example, HIPAA — this definition can be broadened to also include information that can be reasonably used to identify a person. In that case, the definition can include quasi-identifiers such as an email address or even IP address. And in some of the laws, for example, under the FCRA, the protected data can include anything concerning the credit history of consumers.

The European Union has taken a different approach to PII. In their groundbreaking Data Protection Directive (DPD), the EU commission defined "personal data" as any "information relating to an identified or identifiable natural person." This definition was explicit enough to include obvious identifiers and broad enough to cover new ones introduced by technology. It is similar in spirit to HIPAA's definition, but in EU nations the data privacy laws apply to all data, not just medical. In 2018, the EU replaced the DPD with the General Data Protection Regulation (GDPR), which expanded the protection of EU citizen data and regulated the collection of EU citizen data outside of the multination's borders.

Unlike the EU, the United States' approach to data protection and privacy is often focused on specific industries. The disadvantage of industry-specific laws is that there isn't necessarily a uniform definition of what constitutes personal data and how to protect it. However, many of the new state-level privacy laws provide guidance for all sectors of business. But by crafting laws at the national level to solve industry problems, the U.S. avoids a one-size-fits-all approach, and can take into account consumers' own experiences with their data and industry knowledge and practices.

The other issue U.S. laws and regulation address is how personal information is safeguarded. Generally, the laws call for protecting against "unauthorized" access, and for implementing systems and procedures for ensuring the security, confidentiality, and integrity of the data. In the U.S., there are exceptions for allowing affiliated companies and other third parties to access the data — as covered in the GLBA — but the third parties are required to implement the same protections as the original data collector. However, there are exceptions in which protections can be relaxed in certain situations.

Starting in the late '90s, security experts began to realize that along with personal data there was "quasi-personal data" that, if released, could also be used to identify an individual[2]. Identifying a person from this collection of data typically requires matching a collection of anonymous data points — birth dates (or years), ZIP codes, one's ethnicity, and even the type of car model driven — against publicly available databases.

In early 2012, the FTC released new data privacy guidelines that took into consideration the blurring of PII and non-PII data, and reimagined the existing framework for data privacy. In the FTC's vision, personal data should be collected on a business-needs basis and privacy controls should be designed into products and services from the beginning of inception, rather than as an afterthought. Considering the FTC's enforcement power and their influence on government policy, it is likely that this view of data privacy will find its way into new laws and be implemented into existing laws.

Key data protection legislation

Law	Year passed	Relevant agencies
Fair Credit Reporting Act	1970	FTC
Fair and Accurate Credit Transaction Act	2003	
Gramm-Leach-Bliley Act	1999	FTC and other agencies
HIPAA	1996	Health and Human Service (HHS)
HITECH	2009	HHS, FTC
Sarbanes-Oxley	2002	Securities and Exchange Commission

Important terms and concepts

Personally identifiable information (PII)

PII is any information that can directly identify an individual. In U.S. laws, this definition can also mean any information about an individual that's collected as part of a transaction. For HIPAA, the term "protected health information" or PHI is used instead in its rules for healthcare providers. PHI covers any information that can be related to an individual along with any information about "the individual's past, present, or future physical or mental health or condition."

Non-public personal information (NPI)

NPI is essentially PII, but with an exception for personal data that is already widely available. NPI is referenced in the Gramm-Leach-Bliley Act.

Authorized or permissible access

In data protection laws, there is always an allowance for authorized internal and external users to view and process PII. Typically, access rights are dependent on the specific industry's usage patterns. In some laws, for example the FCRA and HIPAA, authorization can also be based on permissible reasons, or functions, such as employment checks or insurance underwriting.

De-identify or anonymize

Generally, data has been de-identified if it has been stripped of PII so that it cannot link back to an individual. HIPAA is one of the few laws that directly address the issues of anonymizing data, though it is still an evolving concept. The Department of Health and Human Services, which enforces HIPAA, provides rules on how medical data can be de-identified — this may include removing ZIP codes and other location information.

Fair Credit Reporting Act (FCRA)

One of the first and most influential U.S. data privacy laws was the Fair Credit Reporting Act. Passed in 1970 and amended over the years (most significantly in 2003), the FCRA initially regulated Credit Reporting Agencies (CRAs) on their management of consumer credit profiles and their accuracy, accessibility to consumers, restrictions on who can see the data, and protections against identify theft. For example, you have the FCRA to thank when you see only the last four or five digits of a credit card number on a printed transaction.

At its heart, the FCRA protects credit information, and other personal credit data, which it refers to as a "credit report." The initial intention of the law was to regulate CRAs — these include the major national credit companies such as Experian, Equifax, Transunion, and others — who must take reasonable procedures "to protect the confidentiality, accuracy, and relevance of credit information"[3]. This includes limiting unauthorized access to the database of consumer records, deleting inaccurate or outdated information, and monitoring suspicious activity.

FCRA does allow third-party organizations who have "permissible" reasons to access credit data without consumer consent, like insurers, landlords, mortgage companies, banks, and other creditors. Generally, the FCRA controls how credit information can be distributed. The intent of this is to protect PII from third-party marketers or data brokers, who under FCRA are never considered to have permissible reasons for accessing credit data without consumer consent. One notable exception is the CRAs themselves: they can transfer the data within affiliated companies as long as the consumer has been alerted and has the chance to opt out.

One significant extension of the original law, based on the FCRA (2003), introduced the concept of "red flags" on consumer reports to indicate that a report that may be compromised by identity theft. In 2005, a disposal rule went into effect which requires companies to take reasonable measures to destroy or erase electronic files containing sensitive information pertaining to consumer credit.

Who is covered?

Financial companies involved with credit (CRAs, insurers, landlords, lenders, mortgage companies, attorneys)

Key privacy and data protection obligations

- CRAs must disclose all information in files and databases to consumers — no matter how or where they're stored.
- Companies with consumer reports must take reasonable measures to protect data.
- To prevent identity theft, strict authentication requirements should be put in place when consumer records are updated.

Regulatory agency

Federal Trade Commission, as well as other agencies, including FDIC

Liabilities

Civil penalties of up to $1,000 per violation, as well as separate court actions

Gramm-Leach-Bliley Act (GLBA)

Gramm-Leach-Bliley Act is an enormous piece of banking and financial legislation that covers more than just data privacy. Its protection of personal information is a major improvement over previous consumer financial data laws — including the FCRA. GLBA protects NPI, which is defined as any "information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available." As mentioned previously, NPI is essentially PII with an added exception for any widely available financial information — for example, property records or certain mortgage information.

Many of us have probably received privacy notifications from our banks, explaining the categories of NPI that are being collected along with special opt-out instructions if you don't want that information to be sent to a "non-affiliated" third party. That's a direct result of GLBA. While GLBA is similar in some ways to the FCRA, its scope is broader because it includes companies that are directly engaged or are significantly engaged in financial activities, and it is far more detailed about its data protection rules.

GLBA originally called for the relevant regulatory agencies — primarily the FTC — to establish standards for financial institutions relating to administrative, technical, and physical information safeguards" (501b). Out of this requirement came the Safeguards Rule (16 CFR 314): separate regulations written by the FTC. As in many U.S. federal regulations, the specific technical implementation details are left up to the companies.

The Safeguards Rule requires companies to develop a written security plan to: (1) designate the employee or employees to coordinate the safeguards, (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks, (3) design a safeguards program, and detail the plans to monitor it, (4) select appropriate service providers and require them (by contract) to implement the safeguards, and (5) evaluate the security program

Who is covered?

Any institution or business that is engaged in financial activities (banks, retailers that issue credit cards, brokerage firms, companies with layaway plans, insurers etc.)

Key privacy and data protection obligations

Establish standards for financial institutions relating to administrative, technical, and physical information safeguards.

Regulatory agency

FTC, the Security and Exchanges Commission, and federal banking agencies

Penalties

Civil penalties of up to $10,000 per violation; board members can also be fined separately, and criminal penalties can range up to five years in prison

and explain adjustments in light of changes to its business arrangements or the results of its security tests.[4]

Like the FCRA, the GLBA also allows for financial institutions to share NPI with their affiliated companies and service providers (which can include accountants, attorneys, and data processors), but requires financial institutions to abide by similar constraints — although, notably, opt-out permission from consumers is not required. GLBA is also more flexible than the FCRA in allowing NPI to be transferred to non-affiliated third parties that have entered into a marketing arrangement with the financial institution — without first requiring consumer opt-out. Generally, though, consumer opt-out is required for sharing NPI with non-affiliated companies. Also, these non-affiliated companies do not have to comply with the same data protection requirements as the financial institution. However, one inviolable rule is that a financial institution can never disclose an account number or a credit card number to another company, regardless of the relationship with the financial institution.

In evaluating risks for customer information, the Safeguards Rule asks financial companies to look specifically into "information systems, information processing, storage, transmission, and disposal" as well as "detecting, preventing, and responding to attacks, intrusions, or other systems failures." The latter part is significant in that the FTC recognizes hackers and other external agents as security threats, which in recent years is a significant risk factor for financial companies.

Is the Safeguard Rule enforced?

The FTC monitors financial companies for violations of the GLBA. Complaints of GLBA violations that are filed with the FTC can be found on the FTC's website. It is not unusual for the FTC to audit companies right after they have reportedly suffered a security breach.

In two recent examples, hackers got into poorly secured file systems and obtained consumer data containing NPI. Inadequate security procedures cited by the FTC included not making "reasonable steps to maintain an effective system of monitoring access" or in another case, the inability to notice "unreasonable user activity" such as "spikes in the number of requests made on the account" of a specific user.

In both cases, the FTC ordered the companies to regularly prove their compliance to regulators for a period of five years.

Sarbanes-Oxley (SOX)

Passed in response to financial scandals involving Enron, WorldCom, and major accounting firms, the Sarbanes-Oxley Act of 2002 does not directly relate to personal data protection and privacy. The law is concerned exclusively with financial auditing controls for publicly traded companies. However, SOX section 404 does have implications for data protection controls: the act simply requests public companies to include an assessment of their internal controls for reliable financial reporting and an auditor's attestation in their annual reports. As the regulatory agency in charge of enforcement, the Security and Exchange Commission does not explicitly say what these controls should be.

In evaluating internal controls, the SEC recommends that companies review their risk areas as they relate to authorizing and recording transactions and their vulnerability to fraud. For IT, this has meant taking into account application-level controls designed to ensure that financial information can reasonably be relied upon.

While the data quantities for financial records are smaller compared to consumer records, the breadth and depth of financial information protected is larger than just personal identifiers. In any case, the same protection principles of restricting access and preventing unauthorized disclosures still apply.

To help companies assess protection risks with financial reporting, the SEC has called for suitable "frameworks." SOX doesn't make specific recommendations on IT control frameworks, though it does say that the Committee of Sponsoring Organizations (COSO), which is a private sector organization devoted to financial reporting, provides one such suitable framework.[5] Auditors are therefore free to select their own approach, which has historically has another framework known as Control Objectives for Information and Related Technology (COBIT).

Who is covered?

Any publicly traded company. However, small-cap companies have been given certain allowances in meeting requirements.

Key privacy and data protection obligations

- A report containing management's assertions on the effectiveness of their financial reporting controls is required.
- An independent auditor must attest to the company's financial reporting controls.

Regulatory agency

Securities and Exchange Commission

Penalties

Civil and criminal penalties: the SEC can use civil penalties to compensate defrauded investors. CEOs and CFOs can be fined up to $5 million and face prison terms of 20 years for "knowingly destroying, altering, concealing, or falsifying records."

There are parallels between the two frameworks, and both can be mapped into SOX section 404. In the case of COSO, the "control activity" is particularly relevant to improving the data integrity that needs to be in place to reduce or eliminate financial reporting risks. Also important for data integrity is COSO's requirement for continual monitoring of control activities. COBIT has equivalent objectives that can be found under its data security and monitor sections.

What is COBIT?

Unlike other data protection laws, SOX has little to say about the types of IT controls needed for compliance. Fortunately, auditors have been using Control Objectives for Information and Related Technology (COBIT) long before SOX as a way to review automated accounting systems.

COBIT maps nicely to regulations under SOX section 404. But it supplies a far broader framework that covers more than just financial reporting.

The following is a list of the most common COBIT control objectives, listed with the header number, used by IT auditors in meeting SOX requirements:

- Manage changes (AI 6)
- Manage third-party services (DS 4)
- Ensure system security (DS 5)
- Manage problems and incidents (DS 10)
- Manage data (DS 11)
- Monitor the processes (M1)

Health Insurance Portability and Accountability Act (HIPAA)

Passed in 1996, the Health Insurance Portability and Accountability Act was landmark legislation to regulate patient data in the healthcare industry and reform aspects of the health insurance industry. An important part of HIPAA — section 1173d — calls for the Department of Health and Human Services (HHS) "to adopt security standards that take into account the technical capabilities of record systems used to maintain health information, the costs of security measures, and the value of audit trails in computerized record systems".[6] The law also requires providers "to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information, and to protect against any reasonably anticipated threats."[7]

The HHS regulators responded by writing the Security Rule, which is at the heart of HIPAA's data protections (title 45, CFR section 160 and 164). The rule describes what "covered entities" — health plans, healthcare clearinghouses, and healthcare providers for example — must implement to secure electronic protected health information or e-PHI. E-PHI is any health information that can identify an individual or provides "a reasonable basis to believe the information can be used to identify the individual".

The Security Rule has multiple parts, but it can be broadly broken down into administrative and technical safeguards.

A key part of the administrative safeguards (164.308) section directs covered entities to develop policies and procedures to "detect, prevent, contain, and correct security violations". To be compliant, healthcare organizations are required to conduct a risk analysis to learn about security vulnerabilities and then implement a risk management plan. This must be followed with monitoring of IT systems using audit logs, access reports, and other incident data. There's an additional requirement to have policies and procedures in place to ensure that employees have appropriate access rights to e-PHI.

The technical safeguards (164.312) can be summarized as requiring any technology — the regulations are technology neutral — for access controls, audit controls, integrity, authentication, and transmission security.

Access means the right to read, write, modify, and perform other functions using "information systems, applications, programs, or files." The actual control scheme should follow the philosophy of restricting access to the minimum necessary information for an employee to perform a job.

For access to e-PHI, the standard asks health providers to consider four technical points for "appropriate and reasonable" safeguards: unique user identifiers, emergency access procedures, automatic logoff, and encryption. IT administrators will likely consider access control lists as a possible implementation after reviewing job functions, along with other authorization and security mechanisms.

HIPAA's 19 PHIs

HIPAA doesn't explicitly define e-PHI other than to say it is information that can be "reasonably" linked back to an individual. To help healthcare organizations, regulators devised a safe harbor rule: as long as health organizations and other covered entities protect the following list, they would be in HIPAA compliance:

1. Name
2. Geographical identifiers smaller than a state — e.g., ZIP code, street address, city, county, geocode
3. Dates related to an individual — e.g., birth date, admission date, etc.
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers — e.g., license plate numbers
13. Device identifiers and serial numbers
14. Web universel resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifier or code

The audit controls are less technically specific but call for "mechanisms that record and examine activity in information systems that contain or use e-PHI." IT administrators will likely want to consider logging and alerting software to handle this aspect of the Security Rule. An important point is that the audit standard doesn't specify what data must be logged or how frequently. Instead, it is left up to the health organization to determine "reasonable and appropriate" audit controls for information that contains e-PHI.

The technical safeguards standard for authentication is straightforward and has no specific details: it calls for covered entities to ensure that those who access e-PHI are who they claim to be. Passwords, PINs, smart cards, or even biometrics are all viable solutions as far as HIPAA is concerned.

Transmission security has more detailed requirements. Essentially, the technical safeguards for this standard requires that data is encrypted over a network and that there are measures in place to ensure the integrity of the transmitted data — typically this can be taken care of by standard protocols, for example TLS.

Finally, there's an overall integrity standard for e-PHI. Effectively, it says that covered entities must protect against accidental destruction of data. As with the other standards for technical safeguards, there are many options available — for example, backup and recovery or file retention policies and procedures could be possible solutions.

In another key part of the Security Rule, health organizations are obligated to safeguard e-PHI accessed by third parties — for example, health records that were given to external data processors for billing. HIPAA calls for these "business associates" to sign contracts stating they would take appropriate measures to protect e-PHI that they "create, receive, maintain, or transmit on behalf of the health organization."

With the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, HIPAA's Security Rule for business associates was further strengthened. In proposed rules issued by HHS in 2010, business associates were held directly liable under the Security Rule.[8] In other words, regardless of whether there was a contract in place, they had just as much responsibility and legal liabilities — including civil and criminal penalties — as the originating health organization.

HITECH was also meant to spur adoption of advanced health technologies. With the rise of the internet as a means to acquire health information, HITECH acknowledges the potential that unauthorized access could occur externally — for example, via hackers and cybercriminals. In other rules that came out of HITECH, HHS required that after the discovery of a security breach involving "unprotected" e-PHI — the Breach Notification Rule — covered entities are obligated to alert each affected individual by written notice within 60 days. Business associates, in turn, are required to tell their healthcare partners of an e-PHI breach along with the individuals whose data was compromised.

Who is covered?

Health plans, healthcare clearing-houses, health exchanges, and any healthcare provider who transmits health information in electronic form, along with business associates who create, receive, maintain, or transmit protected health information on behalf of a covered entity.

Key privacy and data protection obligations

- Maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information.
- Notify individuals whose unprotected e-PHI has been compromised.

Regulatory agency

Department of Health and Human Services, Office of Civil Rights, FTC

Penalties

HHS seeks voluntary compliance or corrective remediation. However, it can ask for both civil and criminal penalties. Civil penalties can reach $50,000 per violation with an annual maximum of $1.5 million. Criminal penalties can include fines and prison terms of up to ten years.

Notifications are issued only in the case of unencrypted health data — unprotected means unencrypted in this context. Some exceptions are made for employees who accidentally, and in good faith, viewed e-PHI information that they were not authorized to view as part of their job role. In any case, when more than 500 unprotected e-PHIs have been compromised, the Breach Notification Rule requires HHS to publish on its website the names of the health organizations that had been hacked.

An interesting aspect of the Breach Notification Rule is that in some circumstances health data that has been de-identified — stripped of the name, address, social security number, and/or health account number — can still be considered unprotected PHI. The reasoning is that other markers in the data, including birth date and ZIP code, may be enough to re-identify the individuals when compared against other public data.[9]

After a period of public comment, in January 2013, HHS finalized the proposed HITECH rules[10]. The most significant aspect of these final regulations is that the Security Rule umbrella now covers sub-contractors used by business associates. These sub-contractors now have direct regulatory obligations to comply with the Security Rule, regardless of what was specified in their contractual agreements. Essentially, they are treated just like business associates, and this includes complying with Breach Notification requirements. Business associates, contractors, and health organizations had until September 23, 2013 to fully comply.

Bottom line: there's now a large sector of companies — service providers, data processors, etc. — who might not have considered themselves in the healthcare industry and now fall under the new business associate obligations of HIPAA.

Overall, compared with data protections for other industries, HIPAA is more technical in nature, and has greater awareness that health organizations are growing and complex; data can be accessed by different stakeholders, both internal and external.

Are you a healthcare subcontractor?

According to the new rules established by HITECH, a subcontractor doesn't necessarily need to have an actual contract in place to fall under HIPAA data protection obligations.

A subcontractor is defined as merely anyone who acts on behalf of a business associate — without being an employee — and "creates, receives, maintains, or transmits protected health information."

The intent of the new subcontractor rule was to prevent lapses in security and privacy protections just because e-PHI was handled by someone other than a business associate. For example, if a business associate of a health organization hires a company — i.e., subcontractor — to handle the disposal of media containing e-PHI, the company would be directly required to comply with relevant parts of the Security Rule.

In the final rule issued in January 2013, there's effectively no difference in terms of compliance between a subcontractor and a business associate with a direct relationship to a health organization.

California Privacy Rights Act (CPRA)

In 2020, California residents voted to expand existing consumer privacy laws previously codified under the California Consumer Privacy Act of 2018 (CCPA). The amended, broader law was renamed the California Privacy Rights Act (CPRA) and is set to take effect January 1, 2023.[13] CPRA (and formerly CCPA) are unique in the United States in that they regulate all for-profit companies doing business in California — not just a single industry.

CCPA was the first state-level consumer data protection and privacy law in the U.S., and several other states have followed with similar laws of their own since 2018. CCPA was similar in philosophy and scope to the EU's own consumer privacy law, GDPR. CPRA, which was passed in 2020, adds additional consumer protections on top of CCPA and expands data privacy rights for California residents.

CPRA establishes several privacy principles that organizations doing business in California must follow and communicate to consumers: 1) collect data only for a specific purpose 2) tell consumers how long you intend to retain data, or if that's not possible, the criteria used to determine the retention period 3) only collect the minimum necessary data 4) establish a chain of custody for sharing or selling information with third parties and 5) protect consumer data with reasonable and appropriate security that is proportionate to its sensitivity.

A big change from CCPA to CPRA is the expanded definition of who constitutes a consumer: under the rights listed in CPRA, the definition now includes a business' employees and intendent contractors as well as consumers. Therefore, businesses with employees residing in California will need to be able to process employee data privacy requests, and provide disclosures of the use and retention period of the collected data, just as they would with their consumers.

Who is covered?

Businesses that collect and process data of California residents or that of California employees, referred to in CPRA as "consumers."

Key privacy and data protection obligations

- Delete consumer information or modify incorrect information upon the request of the consumer.
- Provide data collection and data sharing opt-out for consumers.
- Be aware of additional legal protections required for sensitive personal information.

Regulatory agency

California Privacy Protection Agency

Penalties

Businesses can be fined $2,000 to $7,500 per consumer depending on factors such as negligence. Violations for consumers under 16 are subject to tripled penalties.

California also creates a distinction between "personal information" (which is defined similarly to PII) and "sensitive personal information" (SPI). SPI has a very specific definition. It encompasses identifying information such as social security and state/national IDs, login information for financial institutions, and precise geolocations. But the definition has also been expanded to include categories that might result in discriminatory behavior against a consumer, such as their race, ethnicity, sexual orientation, religion, philosophical beliefs, the contents of their private communications, genetic data, or union status. Because the two definitions differ, it is important for businesses to be able to label both "personal information" and/or "sensitive personal information."

When comparing CPRA to other U.S. data privacy laws, a key difference stands out: CPRA aims to give consumers visibility into how their data is being used, and a measure of control over the collection, sharing, and retention of their data. Many other U.S. data privacy regulations require businesses to handle data responsibly, with minimal input by the consumer.

First, let's talk about how businesses can help consumers get visibility into how their data is being used. For all personal information and SPI that is collected, businesses will need to clearly state the reason for collection, the length of time the data will be retained (or the criteria used to determine how long the data will be retained), and which SPI must be collected for the service to function at a base level and which SPI is less essential to collect.

Businesses will also need to be able to take appropriate action for consumer requests — such as opting out of the collection of SPI that is non-essential to the functionality of the service, handing information correction requests, deleting consumer information upon request, providing consumers with a report of all of the data the business has collected on the consumer, and allowing customers to choose to not have their personal information and SPI shared or sold to third parties.

Because CPRA does not include guidance on technology that can be used to comply with the act, businesses have some flexibility in how they choose to implement CPRA compliance. However, some key capabilities are indicated by CPRA:

- Performing a gap analysis from CCPA to CPRA
- Creating an information inventory and mapping data flows
- Handling consumer requests for action or information
- Ensuring personal information and SPI is properly secured and enacting technology that can quickly alert on threats to this data
- Continuously monitoring for compliance

CPRA is a much broader regulation than most other privacy laws in the U.S. and affords the consumer a high level of control over their data. As a result, businesses with California consumers will need to be able to provide detailed reports on a consumer's data privacy and implement methods or technologies to process consumer data privacy requests.

What about CPRA sharing data with third parties?

CPRA requires businesses that sell or share information with third parties, service providers, or contractors to enter into an agreement to mutually protect the privacy and security of a California consumer's data.

This means that information can only be shared to other businesses for limited and specific purposes. It also grants the original data collector the right to ensure the recipient of shared consumer data takes appropriate steps to protect the privacy and security of consumer data.

Other state-specific data privacy laws

Colorado Privacy Act (CPA)[14]

Who is covered?

Applies to organizations that control data of more than 100,000 consumers annually. "Consumers" are defined under CPA as Colorado residents, excluding employees and others acting in a commercial context.

CPA also applies to organizations that can attribute 25 percent or more of their annual revenue to the sale of personal data of more than 25,000 consumers. Unlike most other state privacy laws, CPA applies to nonprofits as well as businesses. Organizations regulated by federal privacy regulations are not covered under CPA.

When it goes into effect

July 1, 2023

Summary

Affected organizations will need to provide consumers the right to opt-out of data collection access, correct or delete their personal data, and receive a copy of their collected data. Organizations will need to receive explicit consent from consumers to collect sensitive personal data (defined in the same manner as CPRA), as well as collect data only for a specific purpose, protect consumer data using appropriate security measures, collect the minimum data necessary for the specific purpose, and communicate that purpose with the consumers.

Penalties

Up to $20,000 fine per consumer with a maximum of $500,000 for related violations.

Utah Consumer Privacy Act (UCPA)[15]

Who is covered?

Applies to for-profit businesses that control data of Utah consumers, have an annual revenue of at least $25 million, and either 1) collect personal data of 100,000 or more Utah residents or 2) derive over 50 percent of their gross revenue from the sale of personal data. Organizations regulated by federal privacy regulations are not covered under UCPA.

When it goes into effect

December 31, 2023

Summary

Covered businesses must grant consumers the ability to access, delete, and receive a copy of their personal data, as well as opt-out of the sale of their personal data or the processing of their data for targeted advertising.

Like other state privacy laws, Utah also defines both “sensitive data” and “personal data,” but unlike some states, UCPA does not require consumer consent for processing sensitive data. Instead, businesses must provide consumers with a written notice and the opportunity to opt-out before collecting sensitive data.

As in other states, controllers and processors of Utah resident data must provide customers with disclosures about how their personal data will be used, provide reasonable and appropriate technical security for customer data, and inform consumers about how their data will be used and shared with any third parties.

Penalties

Up to $7,500 per consumer for a violation.

Virginia Consumer Data Protection Act (CDPA)[16]

Who is covered?

CDPA applies to for-profit businesses that control data of more than 100,000 consumers annually, or collect data of more than 25,000 consumers annually and 50 percent of annual revenue is derived from the sale of consumer data. CDPA does not apply to businesses regulated by federal privacy laws.

"Consumers" are defined under CDPA as residents of Virginia who are not acting in a capacity as an employee or as a business associate of a covered business.

When it goes into effect

January 1, 2023

Summary

The Virginia law is broad in scope and incorporates many elements of the California privacy laws (CCPA, CPRA) and the EU's GDPR.

Similar to GDPR and other U.S. state privacy laws, Virginia distinguishes between "personal data" and "sensitive data." Virginia requires businesses to obtain explicit opt-in consent for processing sensitive data, and requires businesses to provide an opt-out for the collection of personal data.

Additionally, businesses covered under CDPA must protect consumer data with reasonable security, collect data only for a specific purpose (which must be disclosed to the consumer), enter into data processing agreements with any third parties the data is shared with, allow consumers to opt-out of the sale of their data, and comply with consumer requests, such as requests to access, update, or delete their personal data.

Penalties

Fines of up to $7,500 per consumer for a violation.

Connecticut Data Privacy Act (CTDPA)[17]

Who is covered?

Applies to for-profit businesses that control the personal data of Connecticut residents and have either collected data of more than 100,000 consumers, or have derived 25 percent of their revenue from the sale of consumer data.

Connecticut exempts businesses covered under GLBA and HIPAA from CTPDA regulations, as well as higher education, state and local governments, nonprofits, and businesses that collect personal data solely for the purposes of a financial transaction.

When it goes into effect

July 1, 2023

Summary

Connecticut defines “personal data” and “sensitive personal data” using similar phrasing as other U.S. state privacy laws. Businesses must receive the opt-in consent of the customer to collect sensitive personal data, and for personal data, businesses need to provide customers with an opt-out option.

Other obligations of businesses covered by the law include collecting only data which is relevant for a specific use, providing adequate and appropriate data security, and giving customers the opportunity to access their personal data, correct it, delete it, or receive a copy of it.

Penalties

Fines of up to $5,000 per consumer for a violation.

Other relevant regulatory ideas: the FTC's new data privacy guidelines

U.S. regulators at the FTC have recently recognized there's been a blurring of lines between personal identifiers and other data. EU regulators have also come to the same conclusion. Regulatory agencies both in the US and abroad have pointed to the same culprit: consumers are revealing information about themselves on social networks, which helps "re-identify" data once considered to be anonymous.

In early 2012, the FTC addressed the changing nature of PII and overall problems in ensuring consumer privacy in a report titled "Protecting Consumers in an Era of Rapid Change".[14] Here's what they had to say on PII:

"There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer, or device even if the individual pieces of data do not constitute PII. Moreover, not only is it possible to re-identify non-PII data through various means, businesses have strong incentives to actually do so."

In a significant shift for the FTC, their report recognizes that the current definition of PII is too narrow in scope to appropriately protect consumer privacy. Instead, their report proposes a framework to secure "consumer data that can be reasonably linked to a specific consumer, computer, or other device." With the new "reasonably linked" wording, the report places many new types of digital identifiers — email and IP addresses — as well as de-identified aggregated data under the same security protections given to social security numbers.

The report is essentially a list of best practices for companies to follow and is completely voluntary in nature. However, considering the FTC's power in privacy regulations and its ability to enforce "unfair and deceptive practices," the importance of these new guidelines should not be underestimated.

Who is affected?

While the FTC privacy guidelines are self-regulatory, the FTC has said it can take actions against companies that "fail to abide by self-regulatory programs they join."

Privacy by design

One of the cornerstone principles in the FTC's "Protecting Consumers in an Era of Rapid Change" is for organizations to treat privacy as a "default setting."

Under the concept of privacy by design, the FTC recommends organizations consider privacy and security at every stage of product and service development.

As a practical matter, the FTC suggests that organizations limit their collection of consumer data and implement a sensible retention policy for storing data only as long as it's necessary for business purposes.

Key privacy and data protection guidelines:

- Privacy by design — "companies should promote substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy."
- Companies should protect "data that can be reasonably linked to a specific consumer, computer, or other device."

Financial and medical use cases

GLBA

Let's say a mortgage lending company routinely collects personal data related to its current and potential customers as part of its business operations. This sensitive data includes credit histories, bank account numbers, social security numbers, and other personal identifiers.

In its credit-checking process, the mortgage lender obtains online credit histories from a credit-reporting agency (CRA). To log into the CRA's portal, a mortgage lender employee needs to enter a name, address, and social security number into an online form. The credit reports are stored in the mortgage lender's work area on the CRA portal. However, those reports can also be downloaded into the lender's file system.

As more data is collected, full credit reports and names, addresses, and social security numbers are stored in a folder with open access to all employees at the mortgage lender. The folder also contains a file with the login information to the CRA portal. In the course of doing business with a real estate developer, the lender gives the developer access to its VPN along with the login information to the CRA portal.

After consumer complaints of identity theft, an FTC investigation ultimately reveals that a hacker had gained access to the developer's network and then was able to enter the lender's network. In addition to transferring existing files containing customer credit histories and social security numbers of more than 200 customers, the hackers also used the CRA login information stored in a file with minimal protections to access the CRA portal. By generating random social security numbers, the hacker was able to download and transfer an additional 50 reports.

The FTC found that the lender had not made a reasonable security assessment of the risks in its file system and in its network access polices for third parties, had not taken reasonable steps to address these risks, and had not specifically reviewed the full scope of protected data in its folders. The FTC eventually found the lender had violated several parts of the Safeguard Rule of GLBA, including lack of security assessment, not designating an employee to coordinate a corporate security program, not implementing security safeguards for the file system with respect to NPI and continually monitoring its file controls, and finally not insuring that third parties had similar security measures for protecting NPI.

HIPAA

In this example, a small healthcare chain operates several clinics, labs, and outpatient facilities. Its back-end file system holds the records of more than 10,000 patients. The file system is accessed by doctors, nurses, medical technicians, and the chain's finance and billing departments. Access rights to files are roughly divided between medical and administrative staff.

It is the policy of this chain to allow only administrative users access to customer account records, which contain several different types of PHI, including insurance and social security numbers, along with home address and email information.

Based on patient complaints, HHS undertook an investigation involving the theft of health records. After auditing the healthcare's file system, it was discovered that several hundred patient records had been downloaded from the medical chain's IT system as unencrypted text files. These records corresponded to those patients who had originally filed complaints. The downloaded files were eventually traced to an employee in the billing department. On further investigation, the files were also found on the employee's laptop.

HHC investigators concluded that the chain had violated HIPAA's Security Rule. The healthcare company had not conducted a risk analysis of their file system and their portable device policies, had failed to protect e-PHI that it had "created, maintained, or transmitted," and that after the original complaints of identity theft had been reported to them, had not undertaken a thorough assessment of what was a potential breach.

By not exploring the breach, the investigators concluded that the chain had willfully neglected their obligations under HIPAA's Breach Notification Rule. As part of their agreement with HHS, they were required to take corrective measures, as well as pay enhanced penalties.

Conclusion: unstructured data and data protection compliance

The laws and regulations covered in this whitepaper place obligations on companies to protect data against unauthorized access and disclosure. In the case of personal medical and financial information, there's also a clear intent in U.S. laws to protect the confidentiality or privacy of the individual, or subject of the data. Holders of consumer financial data have additional requirements to make sure the data is accurate and can be corrected on demand by customers. In the case of Sarbanes-Oxley, which regulates internal financial data of public companies, there are strict controls on changes to reporting data to prevent financial fraud.

The trend in the consumer data laws has been to extend the types of data that should be treated as private and secured. This will have implications for companies that have viewed their supposedly de-identified data as anonymous (and therefore not subject to protections) and routinely embed this data in internal spreadsheets, presentations, and free-form text documents that may also be shared with third parties.

But even with traditional PII, there are issues with this data being freely used and distributed within organizations. While many of the laws — excluding HIPAA — are not as specific about who should have access to PII, the trend is moving toward more granular access rights. The new FTC guidelines call for limits on the types of data that should be initially collected with an eye toward restricting access by business functions.

Companies developing plans to comply with these laws will have to account for the vast amount of unstructured data residing outside of databases and other special-purpose applications. Based on analyst estimates, almost 80 percent of corporate data is in unstructured files. In light of recent regulatory rules and the FTC's own framework for privacy controls, which places more emphasis on "privacy by design," IT organizations will have to carefully review file access rights, assess PII and quasi-PII information that's currently in unstructured files, and implement strategies to monitor and control PII information from leaking into files, folders, and domains with less-restrictive authorizations.

References

- **HIPAA Security Technical Standards (HHS)**
- HIPPA Security Rule (HHS)
- Health IT Rule and Regulations (HHS)
- Protecting Consumers in an Era of Rapid Change (FTC)
- Credit Reporting and the FCRA (FTC)
- FACTA Disposal Rule Goes into Effect (FTC)
- Gramm-Leach-Bliley Act Privacy Information (FTC)
- FTC Safeguard Rule for Financial Data (FTC)
- California Privacy Rights Act (voter-approved)
- EU Data Protection Directive
- International Data Protection and Privacy Law, Donald Dowling, Jr. (White & Case)

[1] American Privacy: The 400-Year History of Our Most Contested Right (Lane, 2009)

[2] Broken Promises of Privacy: Responding to the Surprising Failures of Anonymization (Ohm, 2009)

[3] The Fair Credit Reporting Act (ftc.gov)

[4] Standards for Safeguarding Customer Information, 16 CFR 314 (ftc.gov)

[5] Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting (sec.gov)

[6] Statute for Health Information Privacy (hhs.gov)

[7] HIPAA Health Insurance Portability and Accountability Act (hhs.gov)

[8] Notice of Proposed Rulemaking to Implement HITECH Act Modifications (hhs.gov)

[9] Guidance Regarding Methods for De-identification of Protected Health Information (hhs.gov)

[10] New Rule Protects Patient Privacy, Secures Health Information (hhs.gov)

[11] Article 29 Data Protection Opinion on Cloud Computing (eu.gov)

[12] Protecting Consumer Privacy in an Era of Rapid Change (FTC, 2012)

[13] AB-1490 California Privacy Rights Act of 2020 (ca.gov)

[14] SENATE BILL 21-190, Colorado Privacy Act (leg.colorado.gov)

[15] S.B. 227 Utah Consumer Privacy Act (le.utah.gov)

[16] S.B. 1392 Virginia Consumer Data Protection Act (lis.virginia.gov)

[17] Substitute S.B. No. 6 Public Act No. 2215, Connecticut, An act concerning personal data privacy and online monitoring (cga.ct.gov)

Appendix 1

Varonis reports for compliance

Regulation: SOX

Report number	Report name	COBIT control objective
1.a.1	User access log	DS13.3 IT Infrastructure Monitoring
2.a.1	Access statistics	DS13.3 IT Infrastructure Monitoring
2.d.1	Activity by users other than the mailbox owner	DS13.3 IT Infrastructure Monitoring
3.d.1	Users and groups list	DS.5.4 User Account Management
4.m.1	Permissions for users and groups other than the mailbox owner	DS.5.3 Identity Management
10.a	Ownership	PO.4.9 - Data and System Ownership DS.5.3 Identity Management

Report number	SOX section	PCAOB control	COSO component
All reports	404	Access to programs and data	Control activities — Access security controls

Regulation: HIPAA

Report number	Report name/ Varonis product	Security standard (administrative and technical safeguards)	Implementation specifications
1.a.1	User access log	Security management process, audit controls	Information system activity review — access reports
2.a.1	Access statistics	1. Security management process 2. Workforce security	1. Information system activity review — audit logs 2. Authorization and/or supervision
2.d.1	Activity by users other than the mailbox owner	1. Security management process 2. Workforce security 3. Security incident procedures	1. Information system activity review — access reports 2. Workforce clearance procedure 3. Response and reporting — identify suspected security incidents
3.d.1	Users and groups list	Information access management	Access establishment and modification – documentation
3.e.1	Historical group membership	Security incident procedures	Response and reporting — help document security incidents and their outcomes
4.m.1	Permissions for users and groups other than the mailbox owner	1. Security management process 2. Workforce security 3. Information access management 4. Security incident procedures	1. Risk analysis — risk to EPI confidentiality 2. Authorization and/or supervision 3. Access establishment and modification — review permissions 4. Response and reporting — identify suspected security incidents
8.b.1	DatAdvantage operational log	Security management process	Information system activity review – audit logs
10.a	Ownership	Security management process	Risk analysis — risk to EPI confidentiality
7.a	Inactive users	1. Build and maintain a secure network 2. Workforce security	1. Response and reporting — Identify suspected security incidents 2. Termination
12.l.1	Open share and NTFS (Microsoft file system) permissions	1. Security management process 2. Workforce security 3. Security incident procedures	1. Risk analysis — risk to EPI confidentiality 2. Authorization and/or supervision 3. Response and reporting — identify suspected security incidents

Regulation: GLBA

Report number	Report name	Regulation	Requirement
10a	Ownership	Safeguards Rule (314.b)	Identify reasonable, foreseeable risks
7a	Inactive users	Safeguards Rule (314b)	Identify reasonable, foreseeable risk
1.a.1	User access log	Safeguards Rule (314.4c)	Test or monitor the effectiveness of key control systems
2.a.1	Access statistics	Safeguards Rule (314.4c)	Test or monitor the effectiveness of key control systems
2.d.1	Activity by users other than the mailbox owner	Safeguards Rule (314c)	Test or monitor the effectiveness of key control systems
8.b.1	DatAdvantage operational log	Safeguards Rule (314.c)	Test or monitor the effectiveness of key control systems
3.d.1	User and group lists	Safeguards Rule (314.d)	Evaluate and adjust information security program in light of any material changes to its business
12.l.1	Open share and NTFS permissions	Safeguards Rule (31.4d)	Evaluate and adjust information security program in light of any material changes to its business

Schedule a free Compliance Risk Assessment.

Get a detailed, true-to-life report based on your company data, that reveals the vulnerabilities hackers hunt for. Use the report to generate a prioritized remediation plan, get buy-in from leadership, and map out what you need to do next to meet regulations.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.