VARONIS

WHITEPAPER

US Data Protection Compliance and Regulations

Contents

Introduction

US privacy and data protection laws have centered on securing personally identifiable information (PII) against unauthorized access. In recent years, lawmakers have focused their efforts on safeguarding consumer financial and medical information. The laws and regulations that have evolved try to balance consumer privacy rights against industry's need to freely communicate data within their organizations and to share data with partners. With more data available on-line—social media, public databases—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, lawmakers have focused their efforts on safeguarding consumer financial and medical information.

In this white paper, we survey key US consumer data protection and privacy legislation, including Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Sarbanes-Oxley, and the Health Insurance Portability and Accountability Act. We also review recent guidelines from the 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

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

Unlike the EU, the US approach to data protection and privacy is to focus on specific industries.

The rise of the Internet in the 1990s along with massive amounts of consumer data collected and shared by companies have brought a sharper focus to data privacy. At the core of the relevant laws and regulations is a view of what types of data should be protected. They each try to answer the question: "What is personal data?"

In many cases—although it varies—the data that is being protected against unauthorized access or disclosure is an identifier. In the US, these are referred to as personally identifiable information (PII), like 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 email address or even IP address. And in some of the laws, for example in the Fair Credit Reporting Act, the protected data can include anything concerning the credit history of consumers.

The European Union took a different approach to PII. In their 1996 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, as well take on new ones brought on 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.

While the EU DPD is important in its own right, it also impacts US companies through Safe Harbor rules that were negotiated by the government with the EU Commission: US companies that collect or process data from EU citizens are

required to recognize this definition of PII as well as apply the EU data protection framework, which is more extensive than what is mandated by US laws.

Unlike the EU, the US approach to data protection and privacy is to focus on specific industries. The disadvantage of industry-specific laws is that there isn't necessarily a uniform definition of what constitutes personal data and the ways to protect it. However, by crafting laws to solve industry problems, the US avoids a one-size-fit-all approach, and can take into account consumer's own experiences with their data and industry knowledge and practices.

The other question that US laws and regulation took up 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 US, there are exceptions for allowing affiliated companies and other third-parties—for example in Gramm-Leach-Bliley Act--to access the data, but then they are also required to implement the same protections as the original data collector. However, there are even exceptions here with protections relaxed in certain situations.

Starting in the late 1990s, security experts began to realize that along with personal data there was other data–let's call it quasi-personal–that if released could also be used to relate back to an individual[2]. The data magic to accomplish identification typically requires matching a collection of anonymous data points—birth dates (or years), zip codes, ethnicity, and perhaps car model driven–against publicly available databases.

In early 2012, the Federal Trade Commission released new data privacy guidelines that took into account not only this blurring of PII and non-PII data, but also a new framework for data privacy. In the FTC's vision, personal data will be collected on a business-needs basis and privacy controls will be designed into products and services from the beginning rather than as an afterthought. Considering the FTC's not inconsiderable enforcement power and its influence of the FTC on government policy, it is likely that this view of data privacy will find its way into new laws and be worked into existing ones.

Key Data Protection Legislation

Law	Year Passed	Relevant Agencies
Fair Credit Reporting Act	1970	Federal Trade Commission (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
EU Safe Harbor	2000	FTC and other agencies

Important **Terms** and **Concepts**

Personally Identifiable Information (PII)

Any information that can directly identify an individual. In US 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."

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.

Nonpublic Personal Information (NPI)

It is essentially PII, but with an exception for personal data that is already widely available. NPI is referenced in Gramm-Leach-Blilely 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 FCRA and HIPAA, authorization can be also 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 be used to 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 US data privacy law 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, their accuracy, accessibility to consumers, restrictions on who can see the data, and many protections against identify theft. You have the FCRA, for example, to thank when you see only last four or five digits of a credit card number on a printed transaction, or when you receive a notice that your credit card information may have been compromised.

At its heart, though, the FCRA protects PII data, at least as it relates to 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, bank and other creditors. Generally the FCRA controls how credit information can be distributed with the intention to protect PII from third-party marketers or data brokers, who are never considered to have permissible reasons. One notable exception is with the CRA's themselves: they can transfer the data within affiliated companies as long as the consumer has been alerted and has a chance to opt out.

Overall, any financial institution or affiliate who has a credit report must protect the data, and therefore the scope of the FCRA extends beyond the CRAs.

One significant extension of the original law, based on Fair and Accurate Credit Reporting Act (2003), was to introduce the concept of "red flags" on consumer reports to indicate 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.

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 were 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 $1000 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 privacy. However, its protections of personal information are a major improvement over previous consumer financial data laws—including FCRA. Gramm-Leach-Bliley Act protects nonpublic personal information (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". It is essentially PII with an exception for any widely available financial information—for example property records or certain mortgage information.

Generally consumer opt-out is required for sharing NPI with non-affiliated companies.

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 do not wish that information to be sent to a "non-affiliated" third party. That's a direct result of GLB. While GLB is similar in some ways to the FCRA, its scope is broader, including companies that are directly engaged or are significantly engaged in financial activities, and it is far more detailed about its data protection rules.

GLB 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 so called Safeguards Rule (16 CFR 314), which were separate regulations written by the FTC. As in many US 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

Who is Covered

Any institution or business that is engaged in financial activities (banks, retailers that issue credit cards, brokerage firms, companies with "lay-away" plans, insurers)

Key Privacy and Data Protection Obligations:

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

Regulatory Agency

Federal Trade Commission. 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

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

Similar to the FCRA, 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 under similar kinds of protections—although, notably, opt-out permission from consumers is not required. GLB is also more flexible than 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 GLB. Some of these complaints filed by the FTC can be found on their website. It is not unusual for many of their actions to be triggered by a reported 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, to notice "unreasonable user activity" such as "spikes in the number of requests made on the account" of a specific user.

In both of these 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 the 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. SOX's Section 404 is usually the starting point for connecting these auditing controls with data protection: it simply asks public companies to include in their annual reports an assessment of their internal controls for reliable financial reporting, and an auditor's attestation. As the regulatory agency in charge of enforcement, the Security and Exchange Commission does not explicitly say what these controls should be.

While the data quantities for financial records are smaller compared to consumer records, the breadth of financial information protected is larger than just personal identifiers.

In evaluating internal controls, the SEC recommends that companies review their risk areas as they relate to authorizing and recoding 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 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". Sarbanes-Oxley doesn't make specific recommendations on IT control frameworks, though it does say that the

Who is Covered

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

Key Data Integrity Obligations

- A report containing management's assertions on the effective of their financial reporting controls
- Independent auditor attesting to the company's financial reporting controls

Regulatory Agency

Securities and Exchange Commission

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 for historical reasons, has been another framework known as COBIT.

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 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.

Penalties

Civil and criminal penalties. The SEC can use civil penalties as way 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".

What is COBIT?

Unlike other data protection laws, Sarbanes-Oxley has little to say about the types of IT controls that would be needed for compliance. Fortunately, auditors had been using Control Objectives for Information and Related Technology or COBIT long before SOX as a way to review automated accounting systems.

COBIT maps very nicely to Section 404 goals. 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—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 health insurance. 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 system".[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). It describes what "covered entities"—which includes health plans, health care clearinghouses, and health care providers—must implement to secure electronic "protected health information" or e-PHI. What is e-PHI? It is our old friend, personally identifiable information, which has been tightened up for a medical context. E-PHI is any health information that can identify an individual or where "there is 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, health care organizations are required to conduct a risk analysis to learn about security vulnerabilities and then implement a risk management plan. This has to be followed up with monitoring of IT systems by 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.

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 health care organizations, regulators devised a safe harbor rule: as long as health organization and other covered entities protect the following list, they would be in HIPAA compliance:

1. Name
2. Geographical identifiers small 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 Universal 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 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 take 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.

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 alert software to handle this aspect of the Security Rule. An important point is that the audit standard doesn't specify what data has to 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 SSL.

Finally, there's an overall integrity standard for e-PHI. Effectively, it says that covered entities have to 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 called 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".

Who is Covered

Health plans, health care clearinghouses, health exchanges, and any health care 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 five years.

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 communicate health information, HITECH acknowledges the potential that unauthorized access could occur externally—for example, hackers and cyber criminals. 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 individual by written notice within 60 days. Business associates, in turn, are required to tell their health care partners of an e-PHI breach along with the individuals whose data was compromised.

Notifications are issued only in the case of unencrypted health data—that is the meaning of unprotected in this context. Some exceptions are made for employees accidentally, and in good faith, viewing e-PHI information that they were not authorized for 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 web site 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 name, address, social security number, and 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 have until September 23, 2013 to fully comply.

Bottom line: there's now a large sector of companies—service providers, data processors—who might not have considered themselves in the healthcare industry would 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 of health organizations as growing and complex organizations in which health data can be accessed by different stakeholders, both internal and external.

Are You a Health Care 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 final rules issues 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.

EU Safe Harbor Rules

The European Union's consumer privacy and data security regulations can be found in its 1995 Data Protection Directive (DPD). Unlike in the US, the EU took a centralized approach to regulating data privacy with a single law that applied to many organizations, instead of restricting single industries.

Not surprisingly, its definition of consumer data is more abstract and broader than can be found in US laws and regulations. The DPD defines "personal data" as "information relating to an identified or identifiable person." This can include obvious identifiers such as phone number, address, and account numbers, but the definition is flexible enough to encompass data not originally foreseen by the DPD's writers, including email and IP addresses, biometric information, and even images. In fact, some EU nations, who are free to craft their own data laws based on the DPD, have specifically included some of these cases in their own laws.

The EU regulators were also concerned about personal data of EU citizens being transferred to other countries, and this is where the DPD impacts US companies. Normally EU rules only allow data transfers to countries that have adequate data protection laws. The US actually fails this test, and instead a unique safe harbor relationship was negotiated with the EU commission.

US companies (particularly multi-nationals) or in the jargon of the DPD language, "data collectors", that accept EU personal data must follow seven overall principles, including public disclosures of privacy policy, opt-out choice, protect personal data from "loss, misuse, unauthorized access, disclosure", and provide adequate accessibility of personal data to EU users or "data subjects".[11] The US companies must also accept jurisdiction of the FTC. One important point for US companies is that they are allowed to self-certify their compliance with respect to these seven principles.

However, EU regulators recently decided that for cloud-based services provided to data collectors, self-certification is inadequate.[12] Essentially, this was an effort to plug a loop-hole in the law that would have allowed European data collectors to skirt data protection rules and liabilities by shipping the data to a third-party cloud-based hosting service for processing—the DPD calls these data processors.

Bottom line: US cloud companies providing processing services involving EU personal data must provide direct evidence "that the Safe Harbor self-certifications exists".

Who is Covered

US companies that collect personal data in the EU and transfer it to their internal operations within the US. US-based data processors that accept EU personal data. Some exceptions are made for US banks and financial companies.

Key Privacy and Data Protection Obligations

Protect personal data from "loss, misuse, unauthorized access, disclosure"

Regulatory Agency

- Federal Trade Commission. Department of Commerce
- Penalties: Organizations that fail to carry out their Safe Harbor obligation could be considered to be engaging in deceptive business practices. The FTC has the power to seek "administrative orders and civil penalties of up to $12,000 per day for violations".[13]

Other Relevant Regulatory Ideas: **The FTC's New Data Privacy Guidelines**

US regulators at the FTC have recently recognized that there's been a blurring of lines between personal identifiers and other data. EU regulators, by the way, have also come to the same conclusion. Regulatory agencies both in the IUS and abroad have pointed to the same culprit: consumers are revealing information about themselves in social networks that can help "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 entitled "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 the limited scope of PII in protecting consumer privacy, proposing instead 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. 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 that 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 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

GLBAA

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

The hackers used the CRA login information stored in a file with minimal protections to access the CRA portal.

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

Over a period of time, full credit reports and name, address, and social security numbers used to access the reports were stored in a folder that gave access to all employees at the mortgage lender. The folder also contained a file with the login information to the CRA portal. In the course of doing business with a real-estate developer, the lender gave 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 revealed 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 over 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 had 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 protection for protecting NPI.

HIPAA

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

The downloaded files were eventually traced to an employee in the billing department.

It was the policy of this chain to allow only administrative users access to customer account records, which contain several different types of PHIs, 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 their 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. It 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**

Based on analyst estimates, almost 80% of corporate data is in unstructured files.

The laws and regulations covered in this white paper 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 US 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, though, 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—HIPAA is an exception—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 towards restricting access by business functions.

Companies developing plans to comply with these laws will have to take into account the vast amount of unstructured data residing outside of databases and other special-purpose applications. Based on analyst estimates, almost 80% 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) http://www.fredericklane.com/index.php/fsl-books/american-privacy
- 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)
- EU Data Protection Directive
- EU Safe Harbor Framework (Department of Commerce)
- 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] EU-US Safe Harbor Overview (export.gov)

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

[13] US-EU Safe Harbor Overview (export.gov)

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

Appendix 1.
Varonis Reports for Compliance

Regulation: SOX

Report Number	Report Name	Cobit Control Objective	SOX Section	PCAOB Control	COSO Component
1.a.1	User Access Log	DS13.3 IT Infrastructure Monitoring	404	Access to programs and data	Control Activities - Access security controls
2.a.1	Access statistics	DS13.3 IT Infrastructure Monitoring	404	Access to programs and data	Control Activities - Access security controls
2.d.1	Activity By Users Other than the Mailbox Owner	DS13.3 IT Infrastructure Monitoring	404	Access to programs and data	Control Activities - Access security controls
3.d.1	Users and groups list	DS.5.4 User Account Management	404	Access to programs and data	Control Activities - Access security controls
4.m.1	Permissions for Users and Groups Other than the Mailbox Owner	DS.5.3 Identity Management Ensure that all users are uniquely identifiable. Confirm that user access rights to systems and data are in line with business needs	404	Access to programs and data	Control Activities - Access security controls
10.a	Ownership	PO.4.9 - Data and System Ownership DS.5.3 Identity Management	404	Access to programs and data	Control Activities - Access security controls
7.a	Inactive users	DS 5.4 User Account Management	404	Access to programs and data	Control Activities - Access security controls
12.l.1	Open Share and NTFS Permissions	DS.5.3 Identity Management Ensure that all users are uniquely identifiable (No global group access). Confirm that user access rights to systems and data are in line with business needs	404	Access to programs and data	Control Activities - Access security controls
1.a.2		DS13.3 IT Infrastructure Monitoring	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
	DataPrivilege	Access Control	Varonis DataPrivilege shifts accountability for access to the data business owners, who can best determine those authorized to access health data
2.a.1	Access statistics	1. Security Management Process 2. Workforce Security	1.(1)Information System Activity Review -Audit logs 2.(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.(1)Information System Activity Review - access reports 2.(2)Workforce Clearance Procedure 3.(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.(1)Risk Analysis - risk to EPI confidentiality 2.(2) Authorization and/or Supervision 3.(3) Access Establishment and Modification - review permissions 4.(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.(1)Response and Reporting - Identify suspected security incidents 2.(2) Termination
12.l.1	Open Share and NTFS Permissions	1. Security Management Process 2. Workforce Security 3. Security Incident Procedures	1.(1)Risk Analysis - risk to EPI confidentiality 2.(2) Authorization and/or Supervision 3.(3)Response and Reporting - Identify suspected security incidents
1.a.2		1.Security Management Process 2. Workforce Security .	1.(1)Information System Activity Review -Audit logs 2.(2) Authorization and/or Supervision

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

How **Varonis** Can Help

Varonis offers a framework to actualize data governance.

The Varonis Data Governance Suite helps organizations meet many of the implications of the laws covered in this white paper, providing a comprehensive, automated solution to address these compliance questions and challenges, providing a framework to identify and remediate excess access, monitor access activity, identify inappropriate data usage, enforce separation of duties (ethical walls), automate access authorization and entitlement review processes, and provide evidence that these processes are being followed.

The Varonis Metadata Framework non-intrusively collects critical metadata, generates metadata where existing metadata is lacking (e.g. its file system filters and content inspection technologies), pre-processes it, normalizes it, analyzes it, stores it, and presents it to IT administrators in an interactive, dynamic interface. Once data owners are identified, they are empowered to make informed authorization and permissions maintenance decisions through a configurable web-based interface—that are then executed—with no IT overhead or manual backend processes.

VARONIS

Free 30-day Assessment:

Within Hours of Installation

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

Within a Day of Installation

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

Within 3 Weeks of Installation

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

Try Varonis free.

Set up Varonis in your own environment. Fast and hassle free.

info.varonis.com/demo

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.