BigID

A GUIDE TO

Types of Sensitive Information

Organizations of all sizes and verticals collect, process, store, and share all kinds of customer, vendor, and employee data — and that data often contains sensitive information that must be safeguarded from unauthorized access.

Broadly, sensitive information is considered information that can cause harm, embarrassment, inconvenience, or unfairness to an individual or business if it is exposed or gets into the wrong hands.

Table of contents

Types of Sensitive Information

To explore the different types of sensitive information that various regulations define and monitor, let's start with the basics of PII and PI, and then explore more specific iterations — particularly those relevant to certain verticals.

Then we will explore how these regulations overlap — and how to protect sensitive information across the enterprise — no matter what your industry or organization.

PII: Personally Identifiable Information

Personally Identifiable Information, or PII, is defined in the US as: "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

PII is the most commonly available and least regulated type of data, and may or may not be sensitive — or may be considered sensitive only under certain circumstances, or when combined with other data about an individual.

For example, PII like names, phone numbers, or other information that may be widely publicly available, is not usually considered sensitive (though could be in certain contexts), whereas PII like social security numbers, alien registration numbers, or driver's license numbers would always be sensitive.

Relevant regulations for Personally Identifiable Information include: GDPR, CCPA, CPRA, LGPD, & NY SHIELD.

> Personally Identifiable Information, or PII, is the most commonly available and least regulated type of data, and may or may not be sensitive.

PI: Personal Information

Personal Information, or PI, may include personally identifiable information (PII), but is a broader category. In other words, all PII is considered PI, but not all PI is PII.

This broader definition of PI is defined as: “Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

PI, therefore, can include data that is obviously associated with an identity — like a name or a date of birth, which is often also PII — or be interpreted in an extremely broad legal manner. PI can and often includes:

- IP addresses
- employee record information
- location information
- photographs
- racial or ethnic origin
- political affiliations or opinions
- religious or philosophical beliefs
- trade union membership
- sexual orientation
- criminal record
- health or genetic information
- some biometric information

Relevant regulations for Personal Information include: GDPR, CCPA CPRA, LGPD, NY SHIELD

> Personal Information, or PI, may include personally identifiable information (PII), but is a broader category.

SPI — Sensitive Personal Information

Sensitive Personal Information (SPI) under the upcoming California Privacy Rights Act (CPRA) is a new defined term covering data that is related to but does not directly identify an individual — and may causCompliance: What Insurance Companies Need to Know(Opens in a new browser tab)e harm if it's made public. SPI includes personal information that reveals:

- a consumer's social security, driver's license, state identification card, or passport number
- account log-in, financial account, debit card, or credit card numbers in combination with any required security or access code,
- password, or credentials allowing access to an account
- precise geolocation
- racial or ethnic origin, religious or philosophical beliefs, or union membership
- the contents of a consumer's mail, email, and text messages — unless the business is the intended recipient of the communication
- genetic data, including
    - » the processing of biometric information for the purpose of uniquely identifying a consumer;
    - » personal information collected and analyzed concerning a consumer's health; or
    - » personal information collected and analyzed concerning a consumer's sex life or sexual orientation

> Sensitive Personal Information (SPI) is a term covering data that is related to but does not directly identify an individual.

NPI — Nonpublic Personal Information

Nonpublic Personal Information, or NPI, is a type of sensitive information created and defined by the Gramm-Leach Bliley Act (GLBA), which specifically regulates financial services institutions.

NPI does not include publicly available information, and is defined as “personally identifiable financial information that is:

- provided by a consumer to a financial institution
- resulting from a transaction or service performed for the consumer, or
- otherwise obtained by the financial institution.”

NPI may include names, addresses, phone numbers, social security numbers, bank and credit card account numbers, credit or debit card purchases, court records from a consumer report, or any other consumer financial information that:

- a consumer provides to a financial institution
- results from a transaction or service performed for the consumer
- is otherwise obtained by the financial institutions
- NPI does not include information that has been made publicly available or widely distributed in the media or public government records

Relevant regulations for Nonpublic Personal Information include: GLBA, NYDSF / NYCRR 500

> **NPI does not include publicly available information, and is defined as “personally identifiable financial information.**

MNPI — Material Nonpublic Information

Material Nonpublic Information, or MNPI, is data relating to a company, its holdings, and its subsidiaries, that has not been publicly disseminated or made available to investors in general — and that could impact the company's share price.

The regulation aims to monitor and prevent illegal types of insider trading by preventing those who hold MNPI from using it to their advantage in the trading of stock or other securities — or sharing it with others who may use it to their advantage. When trading involves the use of MNPI at all, it is considered illegal — regardless of whether or not the person who acts on it is an employee of the company.

The use or knowledge of MNPI determines in part the lawfulness of insider trading. So, while not all insider trading is illegal — as when employees buy or sell shares of their company and adhere to registration and filing requirements from regulating body, the Securities and Exchange Commission (SEC) — any trading that involves MPNI is illegal.

The "material" part of MNPI requires that the information be significant enough to influence the value of the company's stock. If the information would not reasonably affect the stock price, it is not considered MNPI.

Types of MNPI include — but are not limited to:

- corporate information that comes from either the company affected — or outside regulatory agencies, lawmakers, or financial institutions
- earning reports and other financial records
- upcoming corporate actions or plans, such as initial public offerings (IPO), acquisitions, or stock splits
- outcomes of legal proceedings
- rulings by agencies like the FDA

Relevant regulations for MNPI include the Securities and Exchange Commission's Securities Act and Exchange Act — Regulation FD (Fair Disclosure).

> Material Nonpublic Information, or MNPI, is data relating to a company, its holdings, and its subsidiaries, that has not been publicly disseminated or made available to investors.

Private Information

Private Information is the set of sensitive data regulated by the New York's Stop Hacks and Improve Electronic Data Security (NY SHIELD) Act.

NY SHIELD applies to "any person or business which owns or licenses computerized data which includes private information" of a resident of New York — also referred to as "covered businesses."

Private information expands upon "personal information," which was the type of data originally regulated by New York data breach law before SHIELD came on the scene. New York law defined personal information as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."

To define private information, the SHIELD Act broadened that definition to include "personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of information not encrypted — or is encrypted with an encryption key that has also been accessed or acquired."

> **"Any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."**

Those covered data elements are:

- social security number
- driver's license number or non-driver ID card number
- biometric information — or digital representation of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical measurement that could authenticate an individual's identity
- account number or credit/debit card number, either in combination with any required security code, access code, or password that would permit access — or without such additional identifying information

Private information does not include publicly available data that is legally available from government records at the federal, state, or local level.

The most important takeaway is that private information incorporates a **combination of different types of personal data**, like a username or email with a security question or passcode.

> **Private information does not include publicly available data that is legally available from government records at the federal, state, or local level.**

PHI / ePHI — Protected Health Information / Electronically Protected Health Information

Protected Health Information, or PHI, is a type of sensitive information regulated by the Health Insurance Portability and Accountability Act (HIPAA) — a US regulation for healthcare providers, health plans and insurers, healthcare clearinghouses, or businesses associated with health care organizations — also collectively called "HIPAA-covered entities" or just "covered entities."

PHI is any medical information that can identify an individual — or that is created, used, or disclosed in the process of providing health care services. This includes past, current, and future information about individuals' medical or physical/mental health-related conditions — as contained in physical records, electronic records, and even conversations that take place among patients and clinicians.

Health records, health histories, healthcare services rendered, lab or test results, prescriptions, appointments, patient forms, medical bills, and provider or patient communication records all fall under PHI. Any information at all is considered PHI if it can be related to an individual, even if it would be considered PI under a different regulation (e.g., names, social security numbers, birth dates).

> **Protected Health Information, or PHI, is any medical information that can identify an individual — or that is created, used, or disclosed in the process of providing health care services.**

PHI includes 18 identifiers — any one of which is considered PHI if handled by a covered entity:

- names
- dates
- phone numbers
- geographic data
- FAX numbers
- social security numbers
- email addresses
- medical record numbers
- account numbers
- health plan beneficiary numbers
- certificate/license numbers
- vehicle identifiers and serial numbers, including license plates
- web URLs
- device identifiers and serial numbers
- internet protocol addresses
- full-face photos and comparable images
- biometric identifiers
- any unique identifying number or code

PHI in digital files is called electronically Protected Health Information — or **ePHI**. The HIPAA Security Rule requires covered entities to ensure the sanctity and integrity of PHI with administrative, technical, and physical safeguards.

Regulated, Business, Confidential, and High-Risk Data

Taking a broader view of sensitive data that organizations might possess, companies must consider how they treat regulated data, business data, confidential data, and high-risk data – the crown jewels of an organization.

These categories may include information like intellectual property (IP) – including trade secrets, patents, copyrights, and trademarks. It can include financial or health data that is highly sensitive, personal information that must be kept confidential, and dark data that may lurk in silos, shadow servers, or data streams — and that pose heightened security risk if exposed.

It could be business-specific sensitive data that's critical to the business, but not traditionally labeled as sensitive or regulated. Or transactional data that's critical for Anti Money Laundering (AML), customer IDs, and more.

Such types of sensitive data will often overlap PI, PII, SPI, NPI, PHI, and other data definitions — but may need to be classified, mapped, and cataloged according to specific access permissions or reporting requirements, or custom tagged for specific business needs.

Businesses that are empowered with the ability to classify and correlate data not only by regulation — but according to risk categories, confidentiality principles, and other elements that are relevant to how the business runs — can better contextualize, understand, and take action on their data. This visibility allows companies to:

- enable risk scoring
- ensure proper access controls
- operationalize data minimization efforts and retention workflows
- establish data quality standards, and more.

From a business standpoint, enabling full visibility into your data will significantly reduce risk, strengthen safeguards from unauthorized access, lead to meaningful business insight, and ultimately help unleash the value of your data.

> “Taking a broader view of sensitive data that organizations might possess, companies must consider how they treat regulated data, business data, confidential data, and high-risk data – the crown jewels of an organization.”

Regulatory Exceptions by Vertical and Location

Depending on an organization's industry, it may be responsible for complying with multiple regulations — and tracking which of its sensitive data is regulated by which set of rules, and which is subject to multiples sets of rules. Establishing this "Venn diagram" for responsible regulatory practices requires sophisticated data classification functionality.

For example, a mortgage lending company that is subject to both GLBA and CCPA (or the upcoming CPRA) will always need to carefully track its NPI for GLBA compliance and reporting (as well as other regulations geared toward finance) — but will find that its NPI is exempt from CCPA's requirements. At the same time, data that the mortgage lending company collects, processes, and stores that is not considered NPI may still fall under the CCPA's requirements for sensitive PI.

On the other hand, a health services company that operates in France, Brazil, and multiple US states including New York and California, will need to determine and categorize which of their data is subject to PHI under HIPAA, PI under GDPR, LGPD, NY SHIELD, and CCPA — and soon, SPI under CPRA — and process it accordingly to meet the various reporting standards required by each. Complicating matters further, companies that operate internationally must also take cross-border transfer requirements into account.

The complications posed by multiple regulations can result in a virtual quagmire for data governance, security, and privacy programs — if the company's data is not properly mapped, tagged, cataloged, and cleaned up.

> “NPI does not include publicly available information, and is defined as “personally identifiable financial information.”

How BigID's Data Intelligence Platform Protects All Types of Sensitive Data

No matter where your business operates or what industry you're in, fulfilling a complex array of regulatory requirements starts with deep data discovery that maps, inventories, and categorizes all your sensitive information, all in one place.

BigID's discovery-in-depth goes beyond traditional discovery techniques, which only see one type of data, and targeted data discovery, which only finds data you already know about. Using advanced machine learning, you can protect all of your organization's PII, PI, SPI, NPI, PHI, and more; know what data is subject to which regulation; maintain accurate reporting standards; and achieve compliance across regulations.

Here are just some ways BigID's unmatched data intelligence platform can help:

- classify all your sensitive data — of all types — to know its purpose of use, quality, risk impacts, and more
- automatically catalog sensitive data and metadata in structured, unstructured, cloud, Big Data, NoSQL, data lake sources, and everywhere in between
- find, flag, and tag related data
- automatically identify duplicate, derivative, and similar data

Schedule a demo to learn more about what sensitive information your organization needs to protect — and how to get the most out of your data.

> BigID’s discovery-in-depth goes beyond traditional discovery techniques, and can protect all of your organization’s PII, PI, SPI, NPI, PHI, and more; know what data is subject to which regulation; maintain accurate reporting standards; and achieve compliance across regulations.