UNDERSTANDING AND COMPARING CERTAIN PRIVACY LAWS

GDPR, HIPAA, and CCPA (of California)

NETWORK INTELLIGENCE

The Digital Security Company

Photo Courtesy : Matthew Henry

CONTENTS

OVERVIEW OF GDPR, HIPAA, AND CCPA

1

1. Overview of GDPR, HIPAA, and CCPA

1.1 What are GDPR, HIPAA, and California Consumer Privacy Act (CCPA)?

Put together, GDPR, HIPAA, and CCPA constitute the most rigorous sets of laws, policies, and directives issued by various government authorities across the globe, designed to prioritize and protect consumer data.

The guidelines and directives issued under these acts & policies cover several jurisdictions and comprehensively cover data collection, storage, usage, trading, and access practices with an impetus of keeping the consumer in the loop before her data is accessed for profit-seeking purposes. Let's take a look at each of these briefly.

1.2.1 General Data Protection Regulation (GDPR)

The GDPR is a comprehensive set of rules, frameworks, and policies put out by the European Union that supersedes the previous data protection laws. GDPR comprehensively details the fundamental definition of personal data, who can access it, how it is utilized & transmitted, and the penalties for any breach of the policies.

GDPR's jurisdiction covers the entire European Union (EU). As long as you provide products or services to the citizens – and even residents – of the EU, the GDPR applies to you even if you are not physically present in the EU or its territories. The penalties for breach can be as high as EUR 20 million or 4% of global revenues, whichever is higher.

1.2.2 Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA was passed in 1996 to make insurance policies more consumer-friendly by making them more accessible and portable. The act is considered to be a benchmark in data privacy and protection. It aims to ensure that critical data required for improving or providing healthcare services are available only to 'covered entities.' HIPAA also warrants that robust data protection systems are in place to secure the data and prevent it from being utilized for criminal activities. The act puts the impetus on letting the patients and individuals have control of their data and lays down the liability on 'covered entities' to ensure that the data is available to patients in an accessible format. The covered entities include hospitals, clinics, pharmacies, individual practices, health insurance companies, corporate and

government insurance plans, and their employees and business associates. The act also serves as a guide for laying out 12 critical exceptions under which the information can be accessed outside the set framework's scope. These exceptions include situations where the data is vital for judiciary proceedings or is mandated by law, used for workers' compensation, utilized for determining the extent of domestic violence, neglect, or abuse, significant for organ donation, or necessary to conduct permitted research.

For example, all the Personal Health Information associated with you, available with your health insurance company is covered under this law. Your employer or the government can access it only under particular conditions such as definable use for judicial proceedings or for calculating your compensation.

The HIPAA Security Rule (also known as the HIPAA Privacy Rule) goes into details of putting the onus of ensuring that your data is safely stored, accessed, and transmitted even if it is in electronic form, on the covered entities.

1.2.3 California Consumer Privacy Act (CCPA)

The CCPA is a state-law that transfers the entire set of data ownership, including the ability to influence the point of collection, storage & transmission, use-case, and omission of information into the hands of the individual associated with the information.

CCPA emphasizes the individual's ability to ask the business about any information it possesses about him or her, inquire about the source & purpose of this information, and the individual's ability to opt-out of the information-sharing. Individuals have the right to ask the business to erase any information it possesses about themselves.

All businesses that have a revenue of over USD 25 million or collect information of more than 50,000 residents in California or get 50% of their revenues by selling information of California-residents are covered under the law.

The CCPA ensures that businesses cannot waive the rights granted to California residents under this law. Any contract provision between a business and an individual that says the individual waives these rights is unenforceable.

For example – Assume you are a naturalized resident of California. You visit a website that asks you to allow all the cookies, which will allow the website to collect information such as location history, IP address, your first & last name, and so on. The website also adds a clause in small letters that says you are foregoing your rights under CCPA. Under the CCPA, such an agreement would be null & void.

1.3 What is Personal Data as Defined by GDPR, HIPAA, and CCPA?

	GDPR	HIPAA	CCPA
Definition of Personal Information.	Any data that can be used in isolation or in combination with other data to identify an individual.	Any Personal Health Information added by your doctor, nurse, or healthcare professional in your medical records or discussed during your conversations with the professional.	All information, knowledge, and intelligence are associated with, describe, or is related to a consumer or a household, whether it is subjective or objective or even inaccurate.
Scope of Coverage.	1. Data collected by automated means or even by filing systems. 2. Data on convictions and criminal records. 3. Data masked under pseudonyms.	1. Information about the person in the health-insurers' systems. 2. Billing information between the clinic and the individual. 3. Hospitals, clinics, nursing homes, health insurance companies, HMOs, corporate or government insurance plans, doctors/nurses/physicians, chiropractors/dentists, and pharmacies are covered under HIPAA.	1. The information also covers direct and indirect identifiers. 2. There is no limitation to the medium of transfer or on the format of the information.
What is Not Covered in the Scope?	1. Totally anonymized data. 2. Data on deceased persons. 3. Data on companies and government organizations, unless specifically associated with employees, directors, or partners.	1. Life insurers, employers, worker compensation carriers, schools & school districts, state & law enforcement agencies, and municipal offices are exempt from HIPAA.	1. Data that cannot be translated into material information. For example, the machine data shared between devices, which is not interpretable for humans.

(Note: The information in the table is only for informational purposes as some definitions and exceptions have been omitted from the table to make the context more accessible. The data aggregated for the table has been sourced from A, B, C, and D.)

1.4 GDPR – Overview of Key Terms

GDPR is comprehensive in its scope and can be a little tricky to understand in full. Hence, having a clear idea of what is personal data, who are the entities involved in the process, and what are the processes associated between these entities and the data, as defined by the EU, can help in understanding the policies in spirit:

1.4.1 Types & Scope of Data and Processing

All the information associated with an individual, like name, location, and ID numbers, is covered under GDPR. This also includes the genetic, biometric, and other forms of data associated with an individual's health.

Any set of actions such as collecting, organizing or structuring, storing, editing, retrieving, transmitting, releasing, or destroying are covered under the scope of processing and applicable to both present and future personal data. Even if the data is masked under a pseudonym, put under a distributed or centralized filing system, or processed across several member states, it is covered under the GDPR.

GDPR also lays out ground rules governing the profiling aspects of the data, which can be used to evaluate an individual's professional performance, economic stature, health status, personal choice, or location and movements.

1.4.2 Defining the Roles of Individuals, Organizations, and Entities Covered Under GDPR

There is a clear demarcation between the Controller, the Processor, and the Recipient. The individual, public authority, agency, or any other organization that determines the purpose of processing the data is termed as a Controller, while the entity which executes this processing is called the Processor. A Controller with a presence in more than one EU member state is termed as a Main Establishment. If the Controller or Processor sign over their representation to a separate entity, that entity is termed as a Representative.

A Supervisory Authority is a designated entity which is primarily overlooking the conduct of the Controller or the Processor or both. All the individuals who are living in the jurisdiction of this Supervisory Authority are called the Data Subjects Residing in the Member State.

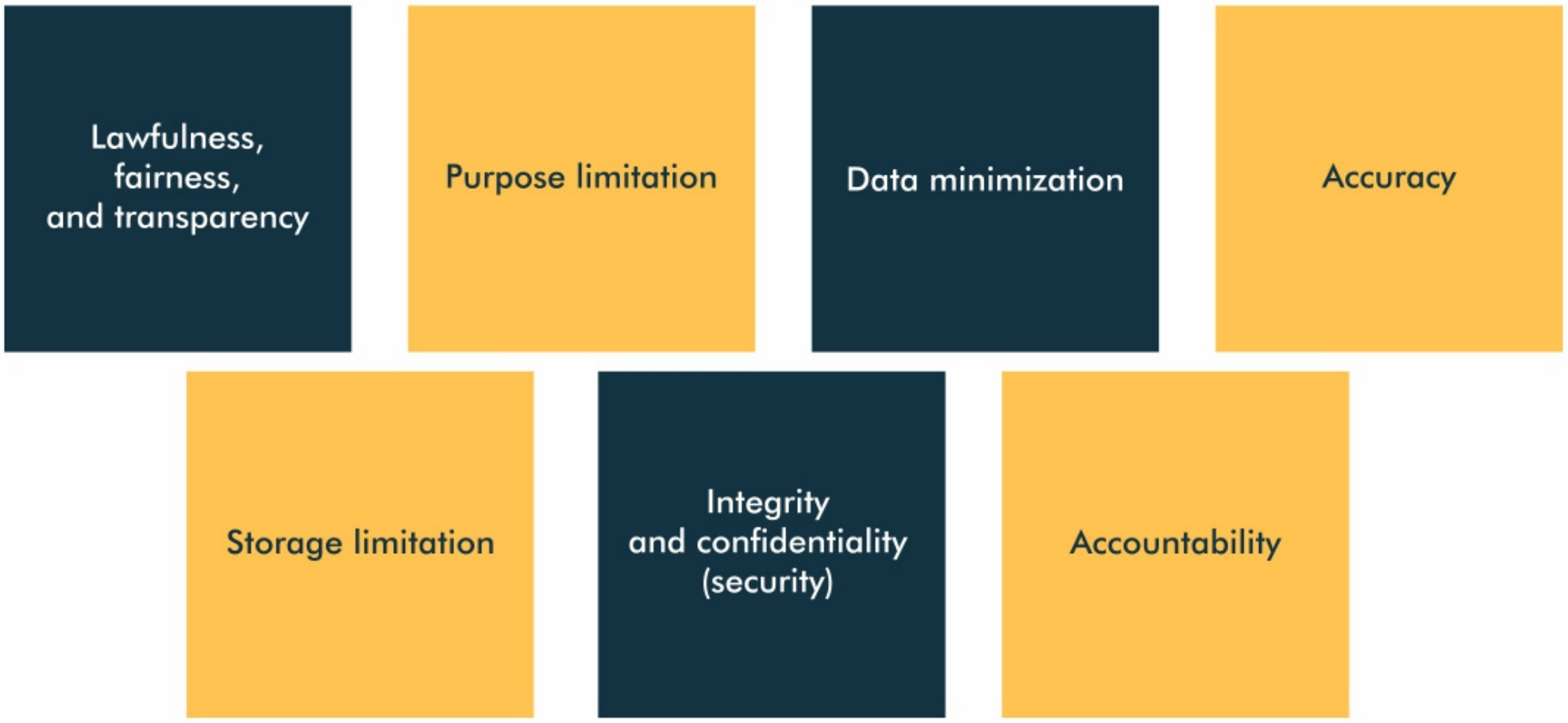
The entity on the receiving side of the personal data is called Recipient. Any entity in this entire ecosystem that is engaging in economic activity is termed as an Enterprise. All other individuals, organizations, and government bodies other than the subject with whom the data is associated, the Controller & the Processor and the people directly employed by them, are termed as the Third Parties.

1.4.3 Establishing the Context of Processes as Defined by GDPR

Consent is a clearly defined statement given by an individual, which allows an entity to use her/his personal data in the manner as permitted in the statement. If the entity accidentally or deliberately destroys, alters, disclose, transmits, or processes the personal data without the individual's consent, it is termed as a Personal Data Breach. The policies hence applicable to the Controller/Processor are therefore termed "Binding Corporate Rules."

1.4.4 General Privacy Principles

The GDPR sets out seven fundamental principles:



1.4.5 Rights of the Data Subject

These are the rights of the data subject:

- Transparency and modalities
- Transparent information
- Communication and modes of communication to exercise the rights of the data subject
- Data and access to personal data
- Rectification and erasure
- Right to object and automated individual decision-making
- Restrictions

SCOPE AND APPLICABILITY

2

2. Scope and Applicability

2.1 Who needs to comply?

Controller, Processor, Recipient, Third Party, Main Establishment, Representative, Enterprise, and Supervisory Authority Concerned are the parties required to comply with GDPR.

Healthcare providers, health maintenance organizations (HMOs), Healthcare clearinghouses, Business associates are the parties required to comply with HIPAA. Only residents of California have rights under the CCPA.

2.2 GDPR applicability within and outside of the EU

- Any organization that processes personal data within the European Union and non-EU data controllers and processors must comply with GDPR when they process data from individuals in the EU.
- Any organization that is present in other countries other than the EU offering goods or services to individuals in the EU must comply with GDPR even though the organization may offer free or paid services.
- Any organization that provides social networking services or similar services that monitor the behavior of individuals inside the EU has to adhere to GDPR.

2.3 HIPAA for Individuals

HIPAA's structure has two aspects – one focuses on ensuring that healthcare institutions are safeguarding personal data, and the other aspect ensures that data is accessible to the individuals associated with it. This personal data can take the form of X-Ray Reports, Vaccine Records, Lab Test Reports, and all the historical as well as ongoing treatment records. The institutions having the liability to safeguard this data include but are not limited to healthcare providers, including the doctors, hospitals, pharmacies, laboratories, and even the health insurance plans that store your personal data.

2.4 Professional Responsibilities as Mandated Under HIPAA

HIPAA is designed with the awareness that some personal data is critical for providing effective healthcare. Hence, it puts emphasis on ensuring that all the personal data available with healthcare providers is secured with great due diligence. The HIPAA has laid out a framework called the Administrative Simplification Rules. These are essential standards established by the government to ensure uniformity across all healthcare transactions. Transaction Standards include instances where the exchange of PHI is vital for carrying out a mandatory or value-adding transaction. The scope of such standards includes – payment & remittance advice, claims and encounter information, coordination benefits, enrollment status, referrals, and premium payments.

Other standards are Code Set Standards, Employer Identification Number Standards, and National Provider Identifier Standards. When used in aggregate, these standards ensure that the transaction is simple to understand for the patients and operationally uniform across all sets of healthcare institutions.

To ensure comprehensive data-security, the HIPAA has created a three-layer framework:

Administrative Safeguards:

Regular risk assessments to measure the vulnerability of the e-PHI system. Compliance-based staff training, limited access to health records, and contingency plans for restored data are mandated under this form of safeguards.

Physical Safeguards:

Mandated use of locks and sensors in the physical office space with even the monitors and workstations checked for privacy measures and data integrity.

Technical Safeguards:

Tested security measures that ensure Personal Health Information on the e-PHI is not accessed without authority, is not transmitted or transferred outside the permitted radius, and is guarded to maintain its integrity.

2.5 What is the 'Do Not Sell' Rule Under CCPA?

The Do Not Sell Rule can be exercised by a consumer under the Right to Opt-Out. This right gives the consumer the power to request a business to stop selling its data. Under the Right to Know, a consumer has the right to know about the degree, time, and purpose of the data collected by a business associated with her/him. If a business also engages in selling consumer-data, it will have to provide a 'Do Not Sell (DNS)' link in the notice at collection form. By using this option, a consumer can prohibit the business from selling her/his data. The business, except for certain exclusions, will have to stop selling that particular consumer's data unless that consumer explicitly permits again.

The term 'Selling' has been defined as a transaction where the data is transferred, transmitted, or made available to another organization, third-party, or individual using electronic or verbal means in exchange for money, gift, or other valuables.

PwC conducted a study on a sample of 700 businesses to understand how they were facilitating the Do Not Sell requests. Businesses from industries such as Consumer Markets and Technology, Media, and Telecom were found to be more active in facilitating such requests, with more than 20% of businesses in both the categories providing DNS links. For industries such as Healthcare, Industrial Products, and Financial Services, the percentage of businesses providing DNS links was in high to low single-digit percentages.

Moreover, data reported by Statista showed that over 33.33% of requests made by customers in 2020Q1 to businesses were DNS requests. This shows that CCPA has garnered significant traction from both the consumer and business frontiers.

While the rule has been designed for extensive applicability, there are some businesses that are not mandated to act under it. For instance – if a business is a service provider that is collecting and selling your data to another business that is responsible for providing you a product or service, you might not be able to ask the service-provider business to stop selling your data. The CCPA, in this case, would be applicable to the businesses whose products or services you are consuming. If there is an NDA between the data collecting and buying businesses, you will have to use third-party resources for understanding the exact title of the business on which you can exercise your CCPA.

Similar to this, collection agencies and businesses that are able to prove that they are storing your data for facilitating product returns or for optimizing their service will also get exempted from the CCPA.

Apart from the exempted businesses, the CCPA is applicable to any business with revenues of over USD 25 million, or one which buys, sells, or receives personal information of more than 50,000 California residents or devices, or one which derives more than 50% of its revenues by selling California residents' data, is liable to comply with the CCPA.

WHAT INFORMATION IS PROTECTED?

3

3. What Information is Protected?

GDPR puts out two broad categories, both of which constitute the 'personal information' category:

Identifiers: This includes all the data that can be used in isolation or can be triangulated with other datasets to identify a naturalized person. Such data would generally include name, identification number, location data, or an online identifier.

Sensitive Personal Data: This category includes any data which may hint at your physical, physiological, genetic, mental, cultural, social, political, religious, ideological traits, or even trade union memberships. It also includes an individual's health, genetic, and biometric data.

GDPR emphasizes using the term 'personal information' in a broad sense. Data-points such as a working-hours of a professional, or answers submitted by an examinee, or the IP address of an individual that can be used to identify the individual will be categorized as personal information.

3.1 Information Excluded from the Scope and Applicability of GDPR, HIPAA, and CCPA

The common thread between the three regulations is the instance where a business is able to prove that the personal data is of paramount importance for providing a certain service or product as requested by the consumer. On such grounds, the personal information is allowed to be collected, processed, and stored while still using the safeguarding measures as stated in the three regulations.

However, GDPR, HIPAA, and CCPA have explicitly mentioned what form of data is not governed under the purview of the three regulations:

a. Under GDPR, all data associated with companies and deceased people are outside the scope of 'personal data.' However, if the company data can be used to identify non-public information associated with its directors, partners, employees, or associates, it can be termed as personal information.

b. The CCPA states that all the information which is already publicly available under the federal, state, or local government records like professional licenses or real estate records, is not considered personal data. Moreover, data shared between two machines (uninterpretable by humans) is outside the scope of being called 'personal information' and hence is not governed by the CCPA.

c. As per the HIPAA, any data not linked with the individual's medical records which cannot be used in isolation to derive a person's identity is not covered by the HIPAA. Such data often includes heart rate and blood-sugar readings.

DATA TRANSFER

4

4. Data Transfer

In technical terms, data transfer is defined as the transmission of data from one system to another within or outside a network. This can be done between business associates, partners, suppliers, or third-party agents. Data Transfer and Data Portability are two different sub-clauses under each of the three regulations. Data Portability is defined as an on-demand service that a business has to provide to its consumer when the consumer wants to port the data to another service provider. Under this rule, the business has to ensure the data is transmitted without any risk to its integrity and is shared with the consumer or the other service-provider in a readily usable format.

All three regulations have different guidelines that cover Data Transfer. The common ground is in how GDPR, HIPAA, and CCPA define cross-border data transfer. All three regulations consider the process of transmission or exchange of data between servers from different countries as Cross-Border Transfer. While the definition states servers, it also includes data shared or transferred using electronic devices or in printed formats.

Ideally, if you are in a jurisdiction that is covered by any of the three regulations, you should deploy strict data encryption in order to transmit data across servers legally.

4.1 Restrictions to Data Transfer

1. The CCPA has not laid out explicit guidelines governing the data transfer for foreign locations. However, considering the opening remarks in the regulation that state the laws are applicable across all the data that belongs to naturalized citizens of the state of California, it would be safe to assume that as a business, you should try to keep the data in compliance with the security and integrity guidelines as mentioned in the CCPA, even if you are using a cloud storage system.

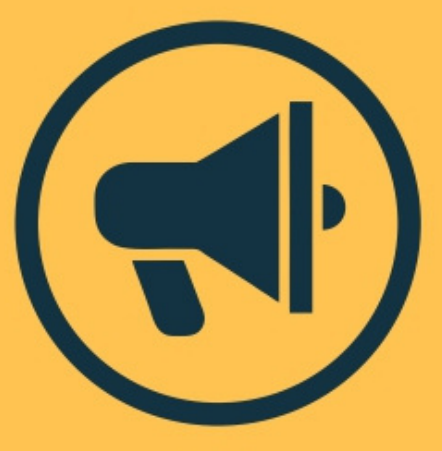
2. The GDPR guidelines have extensively laid out the basis for data transfer outside the European Economic Area (which includes the 28 members of EU along with Norway, Iceland, and Lichtenstein):

a. A business is not allowed to share personal information about an individual across jurisdictions where GDPR is not directly applicable.

b. Any means of transfer, including electronic, physical, email, or partial disclosure, are restricted under GDPR. Even the companies belonging to the same group or holding company but having operations across jurisdictions where GDPR is not uniformly applicable are not allowed to access the personal information covered under GDPR.

c. The business might be allowed to transfer data only, and only if one of the following conditions are satisfied: .

The business has taken explicit permission from the individual associated with the personal information being transmitted.



The transmission is being made in the public interest or using information already available in a public register.

European Union has recognized the location where the data is being transferred as one that is compliant with GDPR or explicitly stated that it is safe for transferring personal information

From the outset, it may seem that there is scope for transferring personal data even as a business stays compliant with GDPR guidelines. However, the exemptions come with several caveats that invite careful examination before a business decides to share, transfer, or exchange data with a designated foreign entity, location, or server.

HOW IS INFORMATION PROTECTED?

5

5. How is information protected?

5.1 How to deploy controls and maintain compliance with these regulations?

1. To deploy controls and comply with GDPR:
Provide information on the Rights of the data subject on your website.

2. To deploy controls and comply with HIPAA:
Provide information on HIPAA for individuals, HIPAA for professionals, the procedure to file a complaint, and HIPAA privacy rules on your website.

3. To deploy controls and comply with CCPA:
Add a "Do Not Sell" link on your website's homepage. This link should take the visitors to the policies page that should state:

a. The customer's right to opt-out.
b. Policies that are related to opt-in.
c. The process to submit an opt-out request.
d. Exceptions to submit an opt-out request.
e. The reasons for collecting more information.

5.2 What is the method of identification of required controls for PII Data protection?

These are the best practices with respect to the consumer authorization requirement:

Create and follow standard consumer authorization procedures that suit your work before you obtain access to consumers' PII. For example, if your organization provides telephonic assistance, develop a verbal script and process to document and retain a consumer's oral authorization.

Have a checklist in place to assist a consumer. This helps you to take your consumers' written or oral authorization before beginning the session.

Create a standard operating procedure to record whenever a consumer withdraws or limits their authorization to access their PII.

Having got the consumer's general authorization that allows you to access his or her PII along with their preferred contact information that you can use to set up appointments or to follow up with the consumer in the future to know if there are any applications or enrollment issues.

5.3 What is Data Protection Impact Assessment (DPIA)?

DPIA helps you to identify and minimize data protection risks of a project. Your DPIA must provide the scope, nature, purpose, and context to:

DPIA

- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to individuals
- Identify any additional steps to mitigate those risks. **know if there are any applications or enrollment issues.**

5.4 Concept of Data Protection Officer (DPO)

DPO should ensure that the organization processes the personal data of its staff, customers, providers, or any other individuals in compliance with the applicable data protection rules.

BREACH NOTIFICATION AND REPORTING

6

6. Breach Notification and Reporting

6.1 Definition of breach of data protection under these three acts

a. As per GDPR, a personal data breach is an accidental or unlawful destruction, alteration, loss, unauthorized disclosure, or access of personal data transmitted, stored, or processed (Article 4, definition 12).

b. As per HIPAA, the breach is unauthorized use or exposure that compromises the security or privacy of the protected health information.

c. According to CCPA, a personal breach is stealing personal information such as consumer's first name and last name along with any of these data:

- driver's license number, social security number, passport number, military identification number, tax identification number, or other unique identification number issued by the government.

6.2 When and to whom data breach has to be notified and reported?

- For consumer complaints regarding GDPR, you can complain to the supervisory authority.
- According to HIPPA, following a breach of unsecured protected health information, covered entities must provide notification of the infringement to affected individuals, the Secretary, and, in certain circumstances, to the media. Also, business associates must notify covered entities if a breach occurs at or through them.
- For consumer complaints against a business/company under CCPA, you can raise a complaint on the CCPA website.

PENALTIES

7

7. Penalties

GDPR, HIPAA, and CCPA Fines and Liabilities in the Event of Non-Compliance

7.1 Penalty for CCPA violation

Civil penalties range between $2500-$7500, depending upon intentional or unintentional nature and the severity of the violation. If the violation is rectified within a month of the event, the organization may get out of the liabilities for the breach. Apart from the direct penalties, compliance costs should also be accounted for as extra charges. The average rate of manually processing one Do-Not-Sell record comes to approximately $1,400, while the cost of complying with these requests per million data points comes to over $200,000. Fraudulent requests, which have so far accounted for about 40% of the DNS requests, are also a major concern.

(For a detailed review of the CCPA penalties, visit this link.

7.2 Penalty as per GDPR violations

GDPR penalties can be in the range of up to EUR 20 million or 4% of the global revenues of the firm breaching the guidelines. Compliance is still a major challenge.

As of January 2020, the Netherlands, Germany, and the United Kingdom had reported the highest number of total breaches. The Netherlands was the country with the highest number of breaches, with the total breaches number crossing 40,000 and the number of breaches per 100,000 people standing at 147.20. While France was not in the top three countries with the highest number of breaches by any means, it had the highest levels of imposed fines, with the imposed fines crossing EUR 51.1 million.

(To know more about GDPR violations and their consequent penalties, visit link)

7.3 Penalty for HIPPA Violation

The two major categories of fines and charges are Reasonable Cause and Willful Neglect. Reasonable Cause ranges from $100 to $50,000 per incident and does not involve any jail time. Willful neglect ranges from $10,000 to $50,000 for each experience and can result in criminal charges.

The US Department of Health and Human Services has put together a comprehensive list of examples that show real-world violations, their implications, and attached penalties. Two of the more common examples include one which entails how a general hospital dealt with confidential communications as per the HIPAA regulations and how a private practice incorrectly charged a patient a 'report review fee.'
(To know more about GDPR violations and their consequent penalties,
Visit this link.

ENFORCEMENT & GDPR, HIPAA, AND CCPA: TOWARDS SAFER AND MORE TRUST WORTHY DATA PRACTICES

8&9

8. Enforcement

8.1 GDPR Enforcement

The GDPR authorities shall take the necessary steps in relation to third countries and international organizations. They are to:

- Create mechanisms for international cooperation that helps to enforce the legislation to protect personal data
- Offer international mutual cooperation to enforce the legislation to protect personal data through notification, complaint referral, investigative assistance, and information exchange that is subject to appropriate safeguarding to protect personal data and other fundamental rights and freedoms
- Involve related stakeholders to discuss activities that aim to expand international cooperation to enforce legislation and protect personal data
- Promote the documentation and exchange of personal data protection legislation and practice that includes jurisdictional conflicts with third countries.

8.2 HIPAA Enforcement

HIPAA helps to:

- Investigate the complaints received
- Conduct compliance reviews
- Educate compliance requirements
- Indicate any criminal violations

8.3 CCPA Enforcement

Privacy Enforcement Actions taken by CCPA on the various organizations vary as per the severity of the damage caused due to leakage of personal data. This ranges from $250,000 to $600 million.

9. GDPR, HIPAA, and CCPA: Towards Safer and More Trustworthy Data Practices

It may seem that GDPR, HIPAA, and CCPA have been designed entirely for protecting consumer rights. While that assertion is not entirely incorrect, it would be inaccurate to state that the regulations are not helping businesses that are complying with these new regulations. The same laws are also strengthening cybersecurity infrastructure across different scales of businesses by making firms focus on adequate administrative and technical measures to establish stronger and safer data-management practices. The laws are also reducing obsolescent technology-use, redundancies in data sharing, and erasure of sensitive data, hence creating an avenue for reduced costs of data storage.

In the long run, these laws will make businesses more responsible data-aggregators and data-consumers while giving the customers a believable reason to put more faith in the businesses and systems they interact with. The businesses that comply with the laws can expect to witness reduced costs of collecting and storing data while still garnering stronger customer loyalty.

Network Intelligence

We are a global cybersecurity provider founded in 2001 with more than 600 team members working out of our New York, Amsterdam, Sydney, Riyadh, Dubai, Mumbai, and Singapore offices. We offer cybersecurity services using a comprehensive framework – ADVISE. The ADVISE framework empowers us to Assess, Design, Visualize, Implement, Sustain, and Evolve your cybersecurity posture as a long-term partner to your organization. By incorporating AI technologies, we revolutionize the way organizations approach security. We serve customers across industry verticals such as Banks and Financial Services, Technology and Media, Oil & Power, Airlines, E-commerce, Retail, Healthcare etc.

ABOUT US

NETWORK INTELLIGENCE

The Digital Security Company

New York | Sydney | Amsterdam | Riyadh | Dubai | Qatar | Mumbai | Bengaluru | Singapore

niiconsulting.com

@niiconsulting

info@niiconsulting.com