Gurzu QA Docs

- HIPAA COMPLIANCE
- HIPAA COMPLIANCE RULES
- GDPR
- Release Note Template
- Diagnostic Report Template

HIPAA COMPLIANCE

HIPAA COMPLIANCE

- The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection.
- Companies that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance.
- Covered entities (anyone providing treatment, payment, and operations in healthcare) and business associates (anyone who has access to patient information and provides support in treatment, payment, or operations) must meet HIPAA Compliance. Other entities, such as subcontractors and any other related business associates must also be in compliance.

ELECTRONIC PROTECTED HEALTH INFORMATION

Electronic protected health information includes:

1. Names
2. Addresses
3. Dates(Date of Birth, Admission date, discharge date, date of death, Date of Doctor's Visit)
4. Phone/fax numbers
5. E-mail
6. Social Security Number
7. Medical Record Number
8. Health plan beneficiary number
9. Account and certificate number
10. Identification number
11. Photos
12. Biometric data
13. Bank Accounts and Insurance Cards
14. Website links or URL
15. Device/Vehicle numbers and serial numbers

COVERED ENTITIES

The following types of individuals and organizations are subject to the Privacy Rule and considered covered entities:

1. Healthcare providers
2. Health plans
3. Healthcare clearinghouses
4. Business associates

HIPAA COMPLIANCE CHECKLIST

- Security Rule comprises three types of addressable safeguards: Administrative, Physical and Technical safeguards.
  - The Administrative and Physical Safeguards are more focused on action protocols for Covered Entities and Business Associates, device use policies, physical access control, and other aspects that are rather distant from software development.
  - The Technical Safeguards, on the other hand, contain requirements that must be fulfilled by developers to make the resulting programming product HIPAA-compliant. It will only focus on the Technical Safeguards and exclude the Physical and Administrative Safeguards from the following description:


Checklist for HIPAA compliance

COMMON HIPAA VIOLATIONS

- Stolen devices with access to ePHI
- Stolen drives with ePHI stored on them
- Hacking, malware, and ransomware attack
- Business associate breach
- EHR breach
- Physical on-site break-ins
- Negligence in transmitting PHI
- Openly discussing PHI in public areas

HOW TO PROTECT THE DATA?

1. Securing your devices and networks
   a. Encrypt your data
   b. Backup your data
   c. Anti-malware protection is must
   d. Secure your wireless network
   e. Use Firewall
2. Data protection tips for mobile devices
   a. Consciously check and configure app privacy settings.
   b. Enable remote location and device-wiping.
   c. Use an on-device, personal firewall.
3. Protect your identitya. Decide what you define as Personally Identifiable Information (PII).
   b. Use passwords(uppercase, lowercase, numbers, special characters)
4. Use two-step verification/authentication
5. Block the user's access if there are multiple wrong password attempts.

18 HIPAA IDENTIFIERS

- The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted.
- Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services.
- PHI includes health records, health histories, lab test results, and medical bills. many common identifiers such as patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, when they are linked with health information.
- The 18 identifiers that make health information PHI are:
  - Name
  - Geographic data (all geographic subdivisions smaller than state, including street address, city county, and zip code)
  - Date ((All elements (except years) of dates related to an individual including birthdate, admission date, discharge date, date of death, and exact age if over 89)
  - Telephone numbers
  - Fax number
  - Email address
  - Social Security Number
  - Medical record number
  - Health plan beneficiary number
  - Account number
  - Certificate or license number
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Device identifiers and serial numbers
  - Web URL
  - Internet Protocol (IP) Address
  - Biometric identifiers(Finger or voice print, retinal scan)
  - Full face photos and comparable images
  - Any unique identifying number or code

THE MOST RECENT HIPAA UPDATES

- ***Updated penalties for HIPAA violations***
- ***Better Enforcement and Accountability of Violations***
- ***Potential Permanent Audit Program***
- ***Additional Guidance or Regulations Regarding Opioids***

HIPAA COMPLIANCE IN THE COVID-19 LANDSCAPE

It’s an understatement to say the world is different due to the pandemic. Healthcare is, almost undoubtedly, set to change the most over the next several years. Maintaining privacy compliance is also more difficult. Factors increasing the risk of private health information include:

- **Telehealth Visits:** The number of healthcare provider visits conducted over the web has skyrocketed. Patients who typically make short trips to the clinic or office decide to stay home and see their physician virtually, unless an in-person visit is absolutely necessary. Data protection over the Internet is difficult if proper precautions are overlooked.
- **Increased Patient Count (post-lockdown):** Now that many states allow most procedures and visits to occur, there has been an onslaught of appointments. When paired with physical distancing guidelines, offices are often short on staff when schedules are maxed out. This situation creates an opportunity for HIPAA compliance mistakes.
- **Multiple Care Providers:** Patients often see multiple doctors. However, increased testing and varied result times make things cloudy. Primary care physicians receiving updates from multiple testing labs, patients, or hospitals means data is moving in and out at a faster pace (if dealing with potential virus cases).

STAY UP-TO-DATE TO AVOID ISSUES

- The Department of Health and Human Services (HHS) has proactively updated those who fall under HIPAA coverage (aka, “covered entities”). With the increase in telehealth options, HHS has to say:

  > “A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients. OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency. This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19.” (Source: HHS)

- Communications are likely to provide guidance on the most prominent issues caused by the pandemic, such as increased appointments, data threats, and mitigation techniques.

Source:

https://www.cdc.gov/phlp/publications/topic/hipaa.html

https://light-it.net/blog/hipaa-compliance-checklist-for-software/

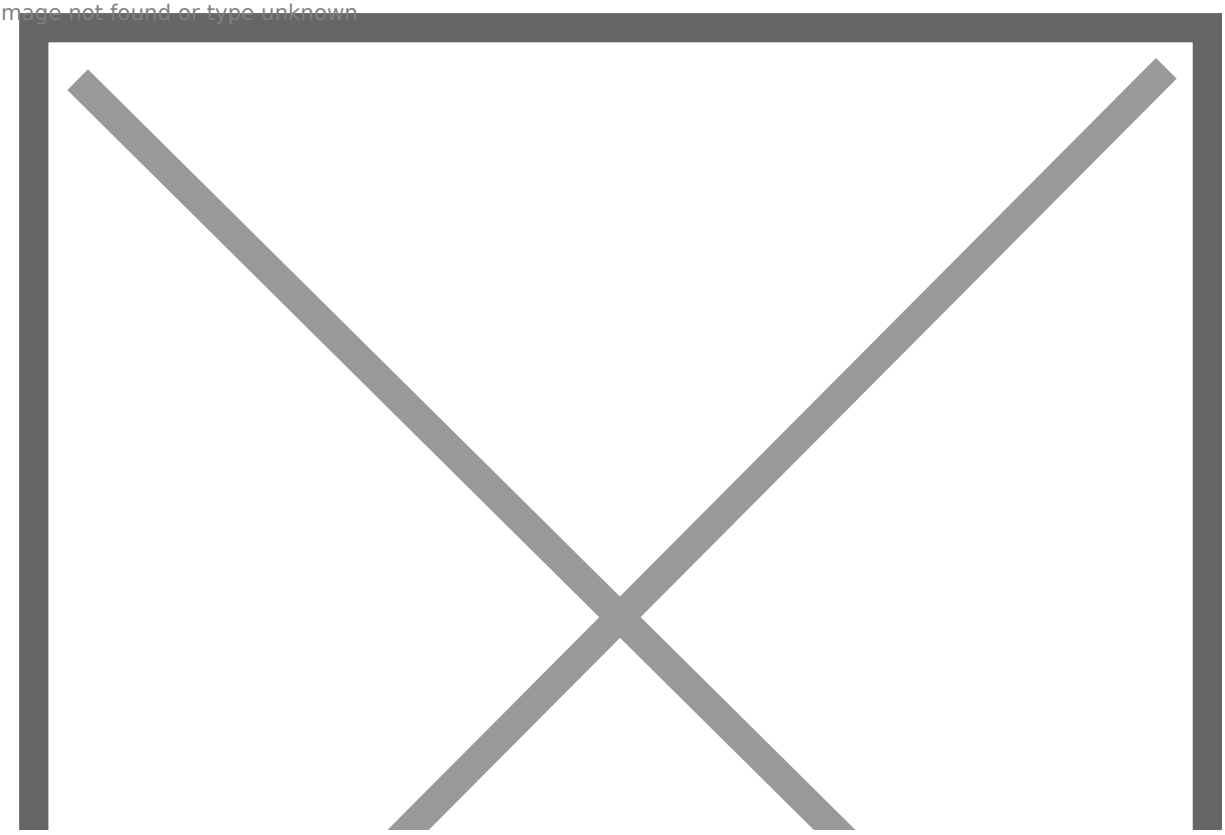
https://www.hipaajournal.com/considered-phi-hipaa/

https://digitalguardian.com/blog/what-hipaa-compliance

HIPAA COMPLIANCE RULES

HIPAA COMPLIANCE RULES FOR SOFTWARE DEVELOPMENT

Image not found or type unknown



Today, electronic PHI storage solutions have replaced traditional paper-based methods. However, the same electronic modes pose additional risks of data breach.

Most often, PHI data breaches result in financial loss irrespective of the number of records stolen. Hackers steal private information with the intention of selling it for money. However, unauthorized exposure of data is only one of the risks involved.

Modifications in the classified data is not an uncommon threat. Moreover, changes made in a patient's medical records and certain diagnoses can mislead the course of treatment. Such situations put the patients at a greater risk of personal damage and can even prove to be fatal for them.

To avoid all the above risks and disasters, the HIPAA defines 5 major rules that all healthcare software applications must follow:

1. ***HIPAA PRIVACY RULES***
    - The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the

Privacy Rule.

- These individuals and organizations are called “covered entities.” The rule describes those certain situations under which certain people can access PHI without patient authorization. It also defines the limitations and rights of the patients.
- The Privacy Rule also contains standards for individuals’ rights to understand and control how their health information is used.
- A major goal of the Privacy Rule is to ensure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well-being.
- The patients can examine their personal medical records and request copies of the same. In case of a mismatch or an error, the patients may also request corrections.

2. ***HIPAA SECURITY RULES***
   - The HIPAA Security Rule lays down conditions for PHI security(technical and non technical safeguards). It includes specific recommendations and limitations regarding health information security.
   - Essentially, this rule helps in identifying, correcting and preventing future security risks.

     The rule dictates that the covered entities are required to conduct a periodic data breach risk analysis in order to ascertain reliable PHI protection.
   - To comply with the HIPAA Security Rule, all covered entities must do the following:
     - Ensure the confidentiality, integrity, and availability of all electronic protected health information
     - Detect and safeguard against anticipated threats to the security of the information
     - Protect against anticipated impermissible uses or disclosures
     - Certify compliance by their workforce
3. ***HIPAA ENFORCEMENT RULES***
   - The HIPAA Enforcement Rule clarifies the investigation provisions and financial penalties in situations of a data breach. However, the penalty amount varies with the number of medical records exposed and the frequency of data breaches in an organization.
   - Generally, a first-time breach can cost an organization from $100 to $50,000 but the subsequent breaches can cost as high as $1.5 million.
4. ***BREACH NOTIFICATION RULE***
   - Ensure that a breach is notated with:
     - A description of the ePHI
     - Who gained unauthorized access
     - The degree that the data’s integrity was misused or corrupted
     - How well the safeguards mitigated any damages
5. ***THE OMNIBUS RULE***
   - This rule extends the obligations of business associates to comply with the HIPAA rules while dealing with PHI.
   - Update Business Associate Agreements to indicate the amendments of the Omnibus Rule.
   - Retrieve newly signed copies of BAAs that incorporate the Omnibus information.

- Update privacy policies to include the Omnibus changes.
- Update NPPs to address the changes to authorizations and the right to privacy.

Source:

https://www.thirdrocktechkno.com/blog/complete-hipaa-compliance-checklist-for-software-development/

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

GDPR

GDPR(General Data Protection Regulation)

- It is the core of Europe's digital privacy legislation.
- GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.
- Almost every aspect of our lives revolves around data and almost every service we use, from social media companies to banks, retailers and governments involves the collection and analysis of personal data.
- According to the GDPR directive, personal data is any information related to a person such as a name, a photo, an email address, bank details, updates on social networking websites, location details, medical information, or a computer IP address.

GDPR COMPLIANCE

- Under the EU's GDPR, it is the legal responsibility of website owners and operators to make sure that personal data is collected and processed lawfully.
- Data breaches inevitably happen like information gets lost, stolen or released into the hands of people who were never intended to see it and often those people have malicious intent.
- Under the terms of GDPR, not only do organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it are obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so.

8 BASIC RIGHTS OF GDPR

- Under the GDPR, individuals have:
  - The right to access –this means that individuals have the right to request access to their personal data and to ask how their data is used by the company after it has been gathered. The company must provide a copy of the personal data, free of charge and in electronic format if requested.
  - The right to be forgotten –Under the GDPR, companies will erase all personal data when asked to do so by the data subject. At that point, the company will cease further dissemination of the data, and halt all processing. Valid conditions for deletion of data include situations where the data is no longer relevant, or the original purpose has been satisfied, or merely a data subject's subsequent withdrawal of consent.
  - The right to data portability - Individuals have a right to transfer their data from one service provider to another, free of charge. And it must happen in a commonly used

and machine readable format.
    - The right to be informed – this covers any gathering of data by companies, and individuals must be informed before data is gathered. Consumers have to opt in for their data to be gathered, and consent must be freely given rather than implied.
    - The right to have information corrected – this ensures that individuals can have their data updated if it is out of date or incomplete or incorrect.
    - The right to restrict processing – Individuals can request that their data is not used for processing. Their record can remain in place, but not be used.
    - The right to object – this includes the right of individuals to stop the processing of their data for direct marketing. There are no exemptions to this rule, and any processing must stop as soon as the request is received. In addition, this right must be made clear to individuals at the very start of any communication.
    - The right to be notified - If there has been a data breach which compromises an individual's personal data, the individual has a right to be informed within 72 hours of first having become aware of the breach.

GDPR CHECKLIST COMPLIANCE

- The General Data Protection Regulation (GDPR) represents one of the most comprehensive reforms to data regulation in recent times. It affects how companies around the globe approach their strategies for external data protections (like data security), as well as internal data access and usage.
- The purpose is to give EU and UK individuals more transparency and control over their personal data. Additionally, it modernizes and consolidates the data protection rules of individual EU Member States under the previous EU Directive into a single regulation.
- The necessary checklist to achieve and maintain GDPR are as follows:
    - Obtain board-level support and establish accountability
    - Scope and plan your GDPR compliance project
    - Conduct a data inventory and data flow audit
    - Undertake a comprehensive risk assessment
    - Conduct a detailed gap analysis
    - Develop operational policies, procedures and processes
    - Secure personal data through procedural and technical measures
    - Ensure teams are trained and competent
    - Monitor and audit compliance

SEVEN PRINCIPLES FOR DATA PROTECTION

The GDPR sets out seven principles for the lawful processing of personal data. Processing includes the collection, organisation, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of personal data. Broadly, the seven principles are :

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy

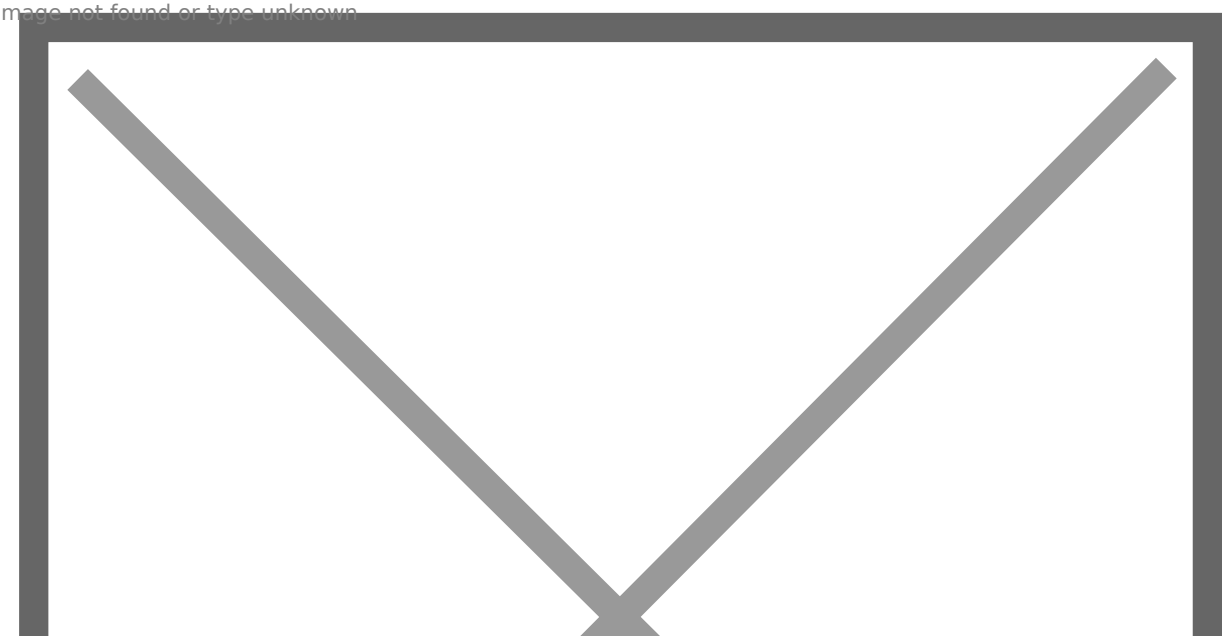
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Types of privacy data does the GDPR protect

1. Basic identity information such as name, address and ID numbers
2. Web data such as location, IP address, cookie data and RFID tags
3. Health and genetic data
4. Biometric data
5. Racial or ethnic data
6. Political opinions
7. Sexual orientation

HOW TO ENSURE YOUR BUSINESS IS GDPR COMPLIANT?

Image not found or type unknown



1. ***Map your Data:*** The first step to solve any problem is by admitting you have it. Therefore, start your data processing changes by reviewing all the user data you store. Map where you get the information, how long it is stored, how it is processed and with whom it is shared. The map you create should give you a clear picture of the data flow in and out of your system and the critical points you need to address to make your company meet the new EU regulation.
2. ***Cover the Lawfulness of Data Processing:***Before you process the user's personal data, you need to ensure you have the legal right to do so. If you outsource data processing to third parties, your contract should include GDPR-compliance clauses. Otherwise, you will need to find new partners. Your data processing is lawful if:
   - You have a legitimate interest in processing the users' data, and they reasonably expect you to process it. Business' legitimate interest does not override an individual's interest and should have minimal effect on privacy.

- Data processing is covered by contractual arrangements, like the use of cookies to track items added to the cart.
- You have gotten consent for data storage and processing from the user. Do not assume users' consent. It should always be an opt-in option, not an opt-out. Explain in simple words how the information will be used and get consent before May 25 to ensure your data processing falls under GDPR before its coming into force.

3. ***Update Privacy Notices:*** You need to review all your internal and external privacy notices and update them according to new EU regulations. Your notices should include answers to these questions:
   - Which data do you need to collect?
   - How will it be processed?
   - What is the lawful basis for each processing action?
   - How long will the data be stored?
   - How can users exercise their rights?
   - Implement The Means For Data Subjects To Exercise Their Rights
4. ***Employ New Internal Processes For Data Protection:*** Personal data protection should become a part of your company's everyday processes. For this, you will need to update data security and implement breach notification protocols. All employees should go through data protection training to prevent accidental breaches.

Source:

https://www.superoffice.com/blog/gdpr/

https://www.itgovernance.co.uk/gdpr-compliance-checklist

https://www.onetrust.com/blog/gdpr-principles/

https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

https://freshcodeit.com/freshcode-post/what-is-gdpr-and-how-will-it-affect-business

Release Note Template

Image not found or type unknown

Release Note

(Name of the Project)

Date: Release Date (MM-DD-YYYY)

Version: Release Version (Version X.X.X)

Credential: Mention the Credential of the release version. (Optional)

Feature Updates

- Include the new features that were updated/added in this release.
- (eg: Ability to login using valid credentials)

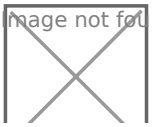
Optimization

- Include those features which we optimized if any

Bug Fixes

- This section includes the issue fixes from the past release.

Diagnostic Report Template



Diagnostic Report

Name of Project

Date: Mention the date of diagnosis report preparation. (MM-DD-YYYY)
Reported By: Mention the name who reported the issue.
Resolved By: Mention the name of the developer who resolved the issue.

Problem Statement:

Mention the issue that occurred and its effect on the system. Mention the Priority and Severity of the issue. Mention the cause of occurrence of the issue.

Diagnosis:

Mention the findings of the diagnosis here. (Like the cause of the issue, who the issue was detected etc)

Solution:

Mention and explain the possible solution to the issue.

Timeline

Mention the timeline of issues that occurred and the issue resolved.