



Personally Identifiable Information and HIPAA

Breaking down Personally Identifiable Information (PII) and its relation to HIPAA compliance, is an essential subject **when defending healthcare companies** from Cyber attacks. Lets explore the definition of PII, the problems associated with protecting it, and how **cutting-edge encryption technology** can help organizations protect PII, and improve compliance.

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) is any information that can be used to identify a specific individual, either on its own, or when combined with other relevant data points. This includes unique identifiers like social security numbers or passport details that directly pinpoint a person. It also encompasses quasi-identifiers such as race, gender, or birthdate which may not identify someone by themselves, but could enable identification when aggregated together or linked with other information.

1

Sensitive PII

Sensitive personally identifiable information can include your full name, Social Security Number, driver's license, financial information, and **medical records**.

2

Non-Sensitive PII

Non-sensitive personally identifiable information is easily accessible from public sources and can include your zip code, race, gender, and date of birth.

3

PII Examples for Healthcare

DOB, SSNs, Medical Records, Test and Lab results, Health Insurance details, Device identifiers and serial numbers, biometric identifiers, to name a few!

The Perils of Personal Data in Healthcare Organizations

In our increasingly connected world, vast amounts of personally identifiable information (PII) are being collected, stored, and shared at an unprecedented scale. This proliferation of sensitive data has caught the attention of malicious actors, leading to a surge in data breaches and cyberattacks targeting individuals and Healthcare organizations, big and small.

- **Florida Healthy Kids Corp. (2020):** 3.5M records exposed, including SSNs
- **20/20 Eye Care Network (2021):** 3.25M records with personal & health info
- **Advocate Aurora Health (2022):** 3M patient records, SSNs & medical data
- **Shields Health Care Group (2022):** 2M records, personal & medical info
- **Forefront Dermatology (2021):** 2.4M records with health insurance IDs

As the value of personal information becomes more apparent, regulatory bodies are scrambling to implement stringent laws and guidelines to safeguard consumer data privacy. Meanwhile, concerned users are seeking out privacy-enhancing technologies and anonymous digital solutions to protect their online presence.



How Cutting-Edge Cloud Encryption protects PII & de-risks exposure in the event of a Breach

Securing the Data

You can't run your business without accessing, storing or sending Patient Data and PII, but a breach or exposure scenario will have a significant material impact.

MDRN's approach to Data Encryption, at rest and in-transit, allows an organization to secure its data across **Web, Mobile & API**, while eliminating the risk, probability, and likelihood of a breach accessing any sensitive information.

All about Improving Compliance

While rendering the data invisible to hackers, organizations can also improve compliance by utilizing a single product, with no external or third-party dependencies to compliance with various regulatory frameworks: **SOX, PCI, HIPAA, PID, PHI, & GDPR**

Quantum Resistant Cryptographic Encryption

Our cutting-edge data protection solution, that is validated to the highest **Cryptographic Certifications** in the world, ensures the confidentiality of sensitive patient information & PII, as it travels between endpoints. Our innovative encryption technology seamlessly safeguards application data in transit, without compromising the user experience.



Effortless integration into existing systems, requiring no changes to the end-user workflow

End Impact

We know that handling PII comes with an increasing risk of breach, and exposure. Healthcare organizations are a high target industry for Cyber criminals.

We understand you will already be taking measures to protect your organization. Defending **revenue, compliance, litigation** and **consumer trust**.

With **MDRNs Encryption solution**, you take that level of protection to a whole new level, only previously seen in very large scale industrial and military applications. Its designed to be simple, and effective in eliminating potential exposure to your underlying data, and increasing your levels of compliance.

Not to mention your levels of confidence, and sleep at night.

