alyne

Comprehensive Compliance with HIPAA Part 164:

Data Privacy, Security Controls and Breach Notifications Rules.

WHITE PAPER

JUNE 2021

PUBLIC

ABOUT THIS PAPER

The rate of digitalisation and an increased threat landscape, paired with highly aware consumers, has not made compliance with HIPAA a straightforward task, leaving many Covered Entities lacking the appropriate measures and unsure of how to comply with all HIPAA Rules set out in Part 164. Technology can be a great facilitator to help simplify requirements, provide greater risk transparency, educate and train employees, and even act as a centralised source of data, alleviating pressure from the audit process. Learn about Alyne's capabilities and comprehensive mapping of Part 164 of the HIPAA regulation, covering the provisions of the HIPAA Security and Privacy, and Breach Notification Rules.

Introduction

The **Health Insurance and Accountability Management Act (HIPAA)** enacted into law in 1996, has arguably been one of the most important pieces of healthcare legislation to be introduced in the United States. The law was designed to provide consumers with greater access to healthcare insurance, reduce fraud, protect the privacy and security of healthcare information and promote efficiency and standardisation within the sector. HIPAA regulates the privacy and protection of Personal Health Information (PHI) held by the organisations, and provides individuals' rights to understand and control how their health information is used or disclosed.

Alyne's coverage of HIPAA primarily focuses on **Part 164** of the regulation, which covers the **HIPAA Security and Privacy** rules. The HIPAA Privacy Rule (Subpart E) focusses on allowed and prohibited uses and disclosures of **Personal Health Information (PHI)** and Personally Identifiable Information (PII) along with data subject rights. Additionally, the Security Rule (Subpart C) is the security standard for the protection of PHI, defining both technical and non-technical requirements for safeguarding health information.

The HIPAA regulations apply to any Covered Entities which handles health or healthcare-related data, including financial clearinghouses, and any provider that uses or transmits PHI. In the 2013 amendment, the changes were added by the Secretary of Health and Human Services to expand HIPAA so that all PHI users (not just healthcare entities), including third-party service providers, adhere to the same data privacy and protection laws under HIPAA. Those that meet the definition of a Covered Entity under HIPAA must comply with the rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information or the transmission, storage, and disclosure of Protected Health Information and electronic PHI.

While the HIPAA law presents clear definitions of security and privacy requirements, some of its terms are broadly defined. Regulations and requirements for compliance with HIPAA are oftentimes difficult to interpret, leading organisations astray or forcing reliance on external consultants to derive the correct controls based on requirements relevant to their organisation. Additionally, to be in compliance with HIPAA, your checklist should cover all the provisions of the **HIPAA Data Privacy, Security Controls and Breach Notification Rules**, which is why within Alyne, we have chosen to provide comprehensive coverage of HIPAA Part 164.

HIPAA Coverage: Who Must Comply?

1 Healthcare Providers

A healthcare provider is defined as an individual health professional or a health facility licensed to provide healthcare diagnosis and treatment services including medication, surgery and medical devices.

This covers providers who transmit any health-related information:

- Hospitals
- Doctor Clinics
- Psychologists
- Dentists
- Physiotherapists
- Nursing Homes

2 Health Plans

A health plan refers to an individual or group plan that provides or pays the cost of medical care.

They cover a wide range of applications which include:

- Company-Sponsored Health Plans
- Health Insurance Companies
- Health Maintenance Organisations
- Government Health Programs

3 Healthcare Clearinghouses

A healthcare clearinghouse is a public or private entity, including a billing service, repricing company, or community healthcare information system, which processes non-standard data or transactions received from one entity into standard transactions or data elements, or vice versa.

4 Business Associates

A Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a Covered Entity. A member of the Covered Entity's workforce is not a Business Associate. A covered healthcare provider, health plan, or healthcare clearinghouse can be Business Associate of another Covered Entity.

- A third-party administrator that assists a health plan with claims processing
- A CPA firm providing service to a healthcare provider involves access to protected health information
- An attorney whose legal services to a health plan involve access to protected health information
- A consultant that performs utilisation reviews for a hospital
- A healthcare clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a healthcare provider and forwards the processed transaction to a payer

5 Third-Party Service Providers

In the 2013 amendment, HIPAA regulation was expanded to include "third-party service providers". Entities who qualify as third-party service providers are those who help to carry out healthcare activities and functions such as storage and transmission services, claims processing services, analytics, or billing services on behalf of the organisations that handle health-related information.

The organisation must have a written contract or other arrangements with the third-party providers that establish specifically what the third-party service providers have been engaged to do and require the third-party providers to comply with the rules' requirements to protect the privacy and security of protected health information.

What is considered Protected Health Information under HIPAA?

Under HIPAA, PHI is considered to be Personally Identifiable Information (PII) relating to the health status of an individual that is created, collected, or transmitted, or maintained by the organisation.
PHI relates to physical records, while ePHI is any PHI that is created, stored, transmitted, or received electronically.

This includes confidential information such as:

- National identification numbers or social security numbers
- Demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information
- Diagnoses
- Treatment information
- Medical test results
- Prescription information
- Device identifiers and serial numbers
- Biometric Information

The Importance of HIPAA Compliance: Protecting PHI under HIPAA Security and Privacy Rule

Digitalisation and the adoption of online technologies have transformed the way healthcare-related information is shared and used. In the healthcare industry, upholding compliance is critical to ensure the best patient experience and treatment journey.

Healthcare organisations must meet this accelerated demand for digital efficiency, whilst complying with HIPAA and protecting PHI. Implementing an efficient and effective compliance program not only aids in providing high-quality healthcare, but also helps to steer Covered Entities away from financial penalties that might otherwise be imposed on the organisation. However, meeting these requirements is oftentimes challenging, as HIPAA is not technology-specific, and safeguards for confidentiality, integrity and availability of PHI are left to the discretion of the Covered Entity.

Let's explore some reasons which support healthcare providers and their third-party providers to remain in compliance with HIPAA.

1 Patient Confidence Through Trust and Transparency

Maintaining the security and protecting the confidentiality of the patient's medical health records are of utmost importance for public confidence in healthcare services. HIPAA laws hold the organisations and their third-party service providers accountable for managing and protecting the sensitive information of their patients. Beyond just protecting patients from identity theft, HIPAA ensures patients can control who has access to their PHI. They may want their sensitive health information kept from family members or employers, thus providing a high level of confidentiality is important. This also means providers will be held accountable for disclosing PHI to co-workers or people outside of work, or any unauthorised person or entity and will operate with more confidentiality within the organisation. More importantly, being in compliance with HIPAA ensures that patients are in control of decisions regarding their health and well-being.

Under HIPAA, organisations can only share PHI with other entities or third-party service providers on a need to know basis. When required, patients can grant permission for: family members, other Covered Entities, employers, etc., to have access to their PHI only if they provide prior written authorisation. The organisation must not use or disclose PHI except:

- If the Privacy Rule allows or requires it
- If an individual or their representative authorises the disclosure of their information in writing
- To individuals (or their representatives) when they request access to their PHI
- When an organisation conducts a law enforcement investigation or action
- Used for their own treatment, payment and healthcare operations activities
- Where informal and written consent is obtained by asking that person directly
- As part of a limited data set with certain direct identifiers have been removed, and the data can be utilised for research, health care improvements and other public purposes

With that being said, there are no restrictions on the use or disclosure of information that cannot be used to identify an individual.

Among many other responsibilities, the organisations must keep track of any kind of PII disclosures, must document any changes to its privacy policies and procedures, must appoint a privacy officer, and must train all members of staff in relevant procedures.

2 Varying Costs of Non-Compliance

Financial penalties are intended to act as a deterrent for preventing violations of HIPAA rules, while also ensuring that the organisations are held accountable for their actions - or their negligence in regards to protecting patient privacy and health data. Anyone can file a health information or security complaint with the Office for Civil Rights (OCR).

The HIPAA Violation Penalty Structure is classified differently depending on the intent of the violation. The penalty is decided based on a Tier structure, where there is a minimum fine of $100 to $50,000 per violation, depending on its severity.

The common violations encountered when handling PHI:

- Unauthorised uses and disclosures of protected health information
- Lack of safeguards of protected health information
- Insufficient granting of access to patient's protected health information
- Uses or disclosures of more than the necessary protected health information
- Lack of administrative safeguards of ePHI

$100 - $50k	**HIPAA Violation: Unknowing** Penalty Range: $100 - $50k per violation, with an annual maximum of $25k for repeating violations.
$1k - $50k	**HIPAA Violation: Reasonable Cause** Penalty Range: $1k - $50k per violation, with an annual maximum of $100k for repeating violations.
$10k - $50k	**HIPAA Violation: Willful Neglect Fixed within the Required Time Period** Penalty Range: $10k - $50k per violation, with an annual maximum of $250k for repeating violations.
$50k - $1.5m	**HIPAA Violation: Willful Neglect Not Fixed within the Required Time Period** Penalty Range: $50k per violation, with an annual maximum of $1.5m.

3 Business Disruption and Other Non-Financial Impacts

Further to being penalised by the authorities, there are other costs that your organisation should take into account, such as business interruption and reputational damage. The primary goal of the HIPAA regulation aims to ensure that healthcare entities maintain the integrity, availability and confidentiality of PHI and ePHI and hence, with a violation of HIPAA, it goes beyond regulatory fines.

In most cases, a violation of HIPAA represents a business interruption as businesses have to spend a significant amount of time and resources to rectify an incident through corrective measures. While the cost involved in setting up a HIPAA compliance program may seem daunting, business leaders should consider reputational damage and customer loss due to lack of trust that can incur as a result of improper practices.

What can your organisation do to remain compliant with HIPAA?

1 Conduct Regular Risk Assessments and Analysis

Within your organisation, the main task of the HIPAA Security Officer is to conduct a risk assessment to identify where ePHI is being used and to whom it is disclosed, and to identify weaknesses where breaches may occur and ensure that both the integrity and confidentiality of ePHI and PHI will not be compromised.

HIPAA requires annual audits which will assess technical, physical and administrative gaps and so it is important to continuously review and periodically re-assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI and ePHI held by the Covered Entity and Business Associates.

2 Active Enforcement of Privacy, Security Policies and Procedures

Policies and procedures for Covered Entities and Business Associates need to be established based on HIPAA regulatory standards. Some policies include the governing of access and usage of ePHI, and security measures to identify malicious attacks or malware.

After performing each risk assessment, it is important to regularly update policies and procedures to account for any changes to the organisation. In the event where there are any changes, these amendments should be clearly documented and communicated across your enterprise.

3 Maintain Strict Business Associate Agreements (BAA)

The HIPAA Privacy Rule requires that all Covered Entities have a signed Business Associate Agreement (BAA) with any Business Associate that may deal with PHI. As most Covered Entities engage with external vendors to achieve business objectives and to support their business operations, this is a vital agreement to have in place with business partners, suppliers, or third-party vendors before establishing a contract. It is important to maintain a credible and reliable partnership, and for the Covered Entities to put in place agreements to ensure that their Business Associates are in compliance with HIPAA.

4 Proactive and Regular Training for Employees

HIPAA violation often happens when an employee is not familiar with HIPAA regulations. Organisations typically carry out compliance training, but in some cases, it is not conducted across the enterprise, leaving many staff who handle PHI unaware and easily subject to violations.

The HIPAA law requires anyone with access to patient information to receive regular compliance training – claiming ignorance is not an excuse for violation of HIPAA laws. Ensure that your training materials are always updated, and that training is performed regularly to prevent potential violations.

Further to your risk management plan, employee training and third-party governance, there are additional protection and precautionary measures that will help to maintain HIPAA compliance.

1 Physical Safeguards

- Maintain strict access control to physical workstations where PHI is stored
- Have an inventory of all hardware containing ePHI, with a record for location, or relocation
- Implement policies that cover the access of workstations, and use such as transferring, removing, deleting and re-using ePHI

2 Technical & Data Protection

- Maintain strict control for ePHI access, supported by multi-factor authentication
- Devices must enable the encryption of messages
- Activity logs and audit controls on accesses of ePHI data
- Automated and time-sensitive logoffs of devices to prevent unauthorised use
- Protection against unauthorised public access of ePHI, across email, internet, private network or private cloud

Comprehensive Coverage of HIPAA Part 164: Security and Privacy within Alyne

When working to achieve compliance with HIPAA, companies often focus exclusively on § 164 Subpart C (Security Standards). Technically, to ensure full compliance with HIPAA, Covered Entities will need to also apply the rules set out in § 164 Subpart D (Breach Notification) and § 164 Subpart E (Privacy Aspects).

Within Alyne, we offer a comprehensive mapping of Part 164 of the HIPAA regulation, covering the provisions of the HIPAA Data Privacy, Security Controls and Breach Notification Rules.

§ 164 - HIPAA SECURITY RULES

The HIPAA Security Rule (Part 164 Subpart C) is the security standard for the **protection of electronic PHI (e-PHI)**. This set of rules ensures that there are both technical and non-technical safeguards (which include administrative and physical) to ensure that ePHI is transmitted and handled in a secured and responsible manner.

§ 164 - HIPAA PRIVACY RULES

The HIPAA Privacy Rule (Part 164 Subpart E) focusses on the many **uses and disclosures** of Personal Health Information (PHI) and Personally Identifiable Information (PII) with **data subject rights**. This includes medical records and other personal health information, and it applies to health plans, healthcare clearinghouses, and healthcare providers that conduct certain healthcare transactions electronically.

§ 164 - HIPAA BREACH NOTIFICATION RULES

The HIPAA Breach Notification Rule (Part 164 Subpart D) requires Covered Entities and their Business Associates to **notify affected individuals and the media** of a breach of unsecured PHI. Depending on its severity, if the data breach affects 500 and more individuals, the Secretary of Health and Human Services has to be informed no later than 60 days following the breach.

Included within this mapping are the following subparts:

- **Subpart A**—General Provisions
- **Subpart C***—Security Standards for the Protection of Electronic Protected Health Information
- **Subpart D**—Notifications in the Case of Breach of Unsecured Protected Health Information
- **Subpart E**—Privacy of Individually Identifiable Health Information

Where Alyne's Technology Can Help

Alyne helps to make compliance and risk management transparent, providing best practices and guidance for organisations aligning with HIPAA. Leveraging Alyne's workflow approach, Covered Entities are able to digitise their HIPAA compliance efforts.

*HIPAA Part 164 currently does not contain a Subpart B.

1 Out-of-the-Box Content

While the HIPAA law presents clear definitions of privacy and security requirements, some of its terms are broadly defined. Regulations and requirements for compliance with HIPAA are oftentimes difficult to interpret, leading organisations astray or forcing reliance on external consultants to derive the correct Controls based on requirements relevant to their organisation.

Alyne simplifies regulations and their requirements. The requirements for HIPAA have been interpreted and mapped into a set of **480 robust Controls** that are easily actionable, specific and measurable for business leaders to implement.

Furthermore, Alyne offers a feature called '**Continuous Controls**' which provides an automated ability to monitor and easily **track the maturity** deviation of HIPAA -related Controls over time.

Since there is no certification scheme available for HIPAA, companies can leverage Alyne's data privacy and information security Controls and Assessments to set up security safeguards relevant for HIPAA.

2 Documents & Policy Management

The platform provides an easy, convenient and maintainable way of integrating your organisation's HIPAA **policy documents**, which can further be used to derive additional unique Controls, relevant to your organisation, through Alyne's intelligent and **automated Control-matching** capabilities.

3 Risk Assessment & Identification

In some cases, your organisation may be required to adhere to multiple compliance requirements (such as **SOX, SOC 2, COBIT, ISO 27001, or NIST CSF**). This can be achieved by using Alyne's **multi-compliance Assessments** to identify any gaps within the organisation or with third-party service providers.

Within Alyne, you can configure your Assessments based on your internal and external requirements and set necessary enforcement(s) to capture required information on your organisation as well as vendors. Submitted responses are measured against the original targeted maturity to **automatically identify potential gaps and corresponding risks**.

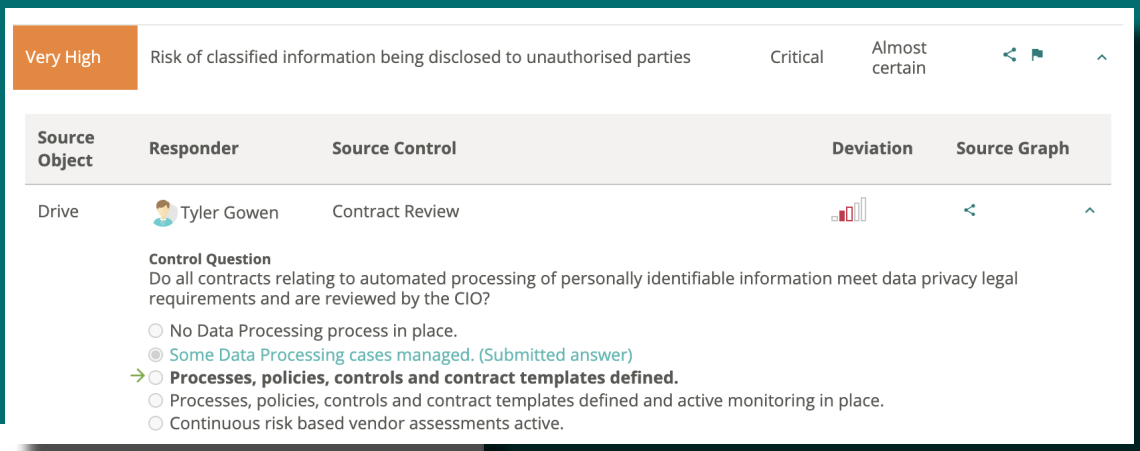
4 Intuitive Reporting

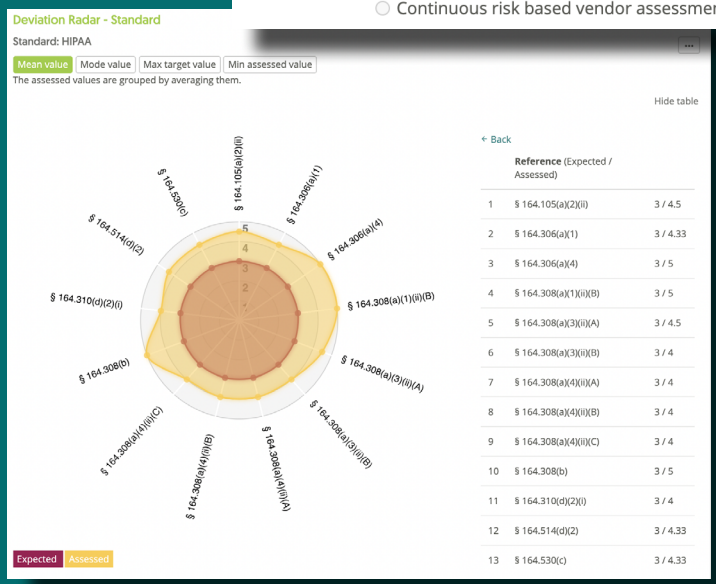
Alyne's Risk Reports automatically summarises the **identified and qualified risks** based on Assessments and presents results visually, in the context of standards, laws and regulations. To provide a clearer view on a certain topic, drill-down Alyne's Reports further in reference to a specific standard, such as HIPAA.

5 Risk Management

Record identified risks, directly within the Alyne Risk Register and document mitigation measures. Alyne's dynamic Risk Management Dashboard provides a **holistic view** of your organisation's HIPAA compliance maturity.

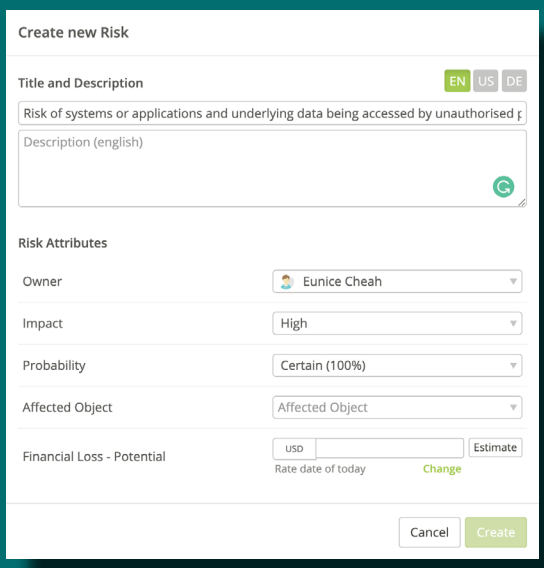
Risk Assessments





Risk Reporting - Deviation Radar

Risk Register

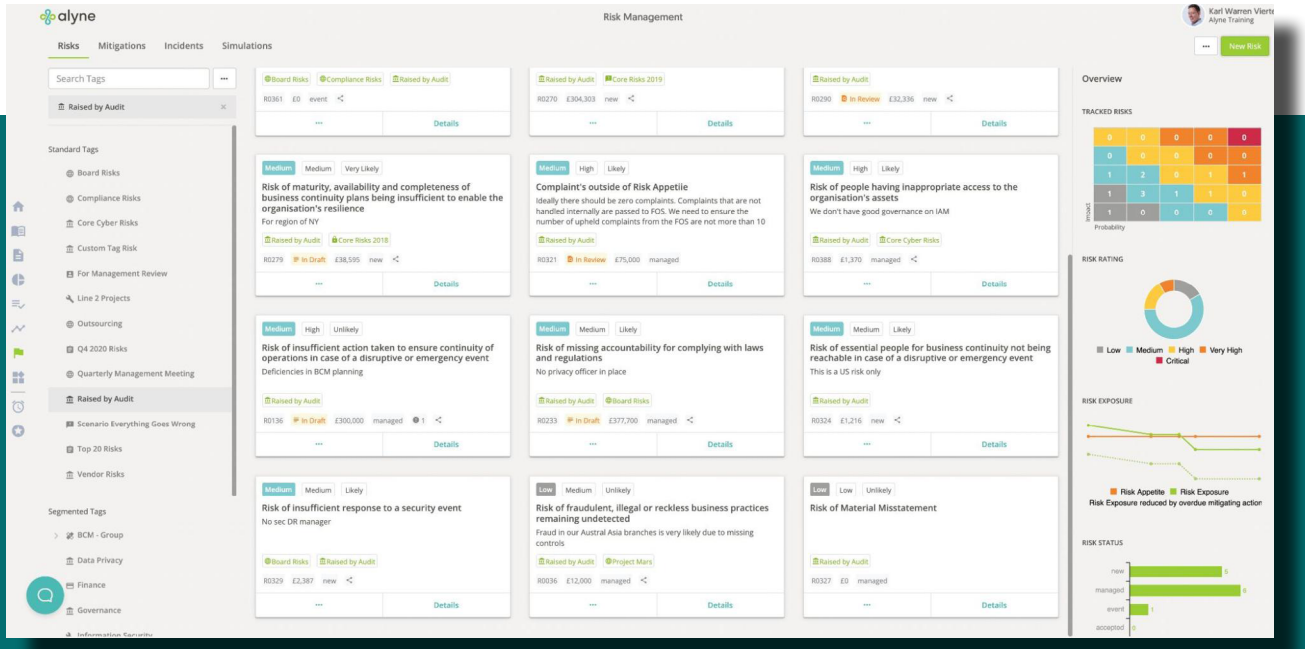


In Closing

Although HIPAA requirements have been in effect for over two decades, the rate of digitalisation, an increased threat landscape, paired with highly aware consumers, has not made compliance with HIPAA a straightforward task. This has left many Covered Entities and Business Associates lacking the appropriate measures, or even simply struggling to determine the correct checklist, applicable to their organisation.

Leveraging technology as a means to facilitate a more agile process can be a tremendous help in your HIPAA compliance efforts, as it can simplify requirements, provide greater risk transparency, help to educate and train employees, and even act as a centralised source of data – alleviating pressure from the audit process.

Alyne provides a centralised platform that simplifies HIPAA compliance, enabling risk and compliance teams to measure and manage regulatory expectations, and drive efficiency without sacrificing on quality of risk management.



Risk Management Dashboard

Schedule a meeting with an Alyne expert and learn more about Alyne's HIPAA capabilities.

Credits & Content

Writers & Contributors
- Moiz Ahamed
- Eunice Cheah
- Bayley Benton

Design & Layout
- Javier Gutierrez

Photography
- Javier Gutierrez

References

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf

https://www.hipaajournal.com/

https://healthitsecurity.com/features/ensuring-security-access-to-protected-health-information-phihttps://securenetmd.com/blog/hipaa-compliance-important-healthcare-providers/

alyne

Founded in 2015 with the vision to build technology that is easy to use and that simplifies risk management for all organisations, Alyne now operates globally to provide extensive capabilities in managing Cyber Security, Governance, Risk Management and Compliance processes through a Software as a Service platform. Alyne's technology is powered by industry experts and enables risk and assurance professionals to easily understand complex data and gain actionable insights, through it's powerful Content Library, Assessments and Risk Reporting features - mapped to relevant standards, laws and regulations. Keep your organisation at the forefront of Cyber Security, Risk Management and Compliance with Alyne as your Mission Control.

Alyne USA Inc.
43 West 23rd Street,
NY 10010, New York

Alyne GmbH
Ganghoferstr. 70a
80339 Munich, Germany

Alyne UK Ltd.
41 Luke St, Shoreditch,
London EC2A 4DP, UK

Alyne Australia Pty Ltd.
Level 1 Front Suite
19 to 21 Toorak Rd
South Yarra VIC 3141, Australia

For more information, visit **www.alyne.com**