Pdiver In Action

Prevent Data Breach in Email

HiFiData LLC

Version 1.2

2024-09-28

1. Introduction

Email is a vital communication tool for businesses and organizations, but it also poses significant risks for unintentional data breaches. Sensitive information, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), can easily be shared mistakenly—whether internally across departments or externally with unauthorized recipients. Such privacy leaks can lead to serious compliance violations under regulations like HIPAA, resulting in costly financial penalties and lasting reputational damage.

In 2017, a major U.S. health insurance company experienced a massive data breach where **78.8 million healthcare records** were compromised According to the report. Analysis from the HIPAA Journal indicates that the frequency of healthcare data breaches has been steadily increasing over the past 14 years, with 2021 seeing more breaches than any other year on record. This growing trend emphasizes the need for organizations to adopt stronger safeguards to protect sensitive information communicated via email.

The scale of this issue is highlighted by real-world statistics. The *Office for Civil Rights* at the *U.S. Department of Health and Human Services (HHS)* maintains a breach report tracking incidents involving unsecured PHI that affected 500 or more individuals. Over the past two years, 174 breaches were caused by email-related incidents, impacting about 5 million individuals representing more than 20% of all reported healthcare breaches during this period. These statistics highlight how vulnerable email systems are when handling sensitive data.

The consequences of such unintentional data leaks go beyond compliance penalties. Organizations risk facing fines, lawsuits, and reputational damage. The need to prevent these breaches is critical, and that's where HiFiData Pdiver comes into play. Pdiver provides a proactive, automated solution for protecting sensitive data in emails, ensuring businesses comply with data protection regulations while minimizing the risk of exposure.

2. Limitations of Email Platforms in Preventing Data Breaches

While email platforms like Gmail and Office365 offer basic security features such as rules and filters, they are primarily designed for communication, not for handling the complex requirements of privacy protection and regulatory compliance. These limitations include:

- **Complex Rule/Filter Configurations:** Setting up rules and filters to detect sensitive data requires manual configuration of numerous elements, a tedious and error-prone process. As privacy regulations and company policies evolve, frequent updates are needed, increasing the risk of misconfigurations that leave critical gaps in email protection.
- **Inefficient Sensitive Data Recognition:** Most platforms lack advanced detection capabilities, making it difficult to identify sensitive data in varying contexts or writing styles. Basic keyword-based filtering often misses nuanced information, such as obfuscated identifiers or indirect references, leaving sensitive data vulnerable.
- **Limited Adaptability:** Server-side rules, while useful, are often rigid and difficult to customize for different departments or user needs. This lack of flexibility results in inconsistent enforcement of privacy protection policies across the organization, leading to uneven data security practices.
- **Block-Only Response:** Many email platforms block emails containing disallowed content. Although this prevents data breaches, it disrupts workflows by requiring users to manually review or modify emails. A smarter solution—like automated data transformation—would allow emails to be sent securely without halting productivity.

- **Limited Data Transformation Capabilities:** Crude blocking mechanisms force users to manually manage sensitive data without system support. This inefficiency increases the risk of human error and makes compliance more challenging.
- **Compliance Complexity:** Without built-in tools to manage and transform sensitive data according to regulations like HIPAA, organizations face increased risks of non-compliance. Relying on basic encryption or user-side configurations leaves gaps in data security and privacy management.

3. How Pdiver Secures Email Communications

Unlike traditional solutions that block emails after detecting sensitive content, HiFiData Pdiver offers a fundamentally different approach. Following the High Fidelity Data specification, Pdiver transforms sensitive data while preserving the visual, statistical, population, and ownership integrity of the email. This means that the content, meaning, and intent of the email remain intact, and the recipient's experience is unchanged—except that the privacy-sensitive data has been securely transformed, or "Pdived."

By transforming sensitive data in real-time before the email is sent, Pdiver prevents breaches proactively, rather than reacting after the fact. This ensures seamless email communication without disrupting the flow or clarity of the message.

Pdiver eliminates the tedious and complex process of manually configuring numerous sensitive data elements in "rules/filters," automating the entire data protection process. It handles all the intricacies of data transformation, allowing users to focus on their core tasks. This makes Pdiver a user-friendly, automated solution that significantly reduces the burden of ensuring privacy in email communications.

HiFiData Pdiver also provides flexible integration options at both the server and client levels, ensuring comprehensive email protection. With multiple integration points, organizations can safeguard sensitive data throughout the entire email workflow.

4. Configure Pdiver on Email Server

By integrating Pdiver at the email server level, organizations can automate the detection and transformation of sensitive data before emails leave the organization's domain. This ensures that any privacy-sensitive information is desensitized or pdived in real-time, preventing accidental exposure without interrupting the email workflow.

Let’s walk through how this works using Gmail as an example:

- *Defining a Content Compliance Rule*: The administrator can define a new Content Compliance Rule within the Gmail Admin Console. This rule will apply to all users across the company, ensuring that emails containing sensitive data are automatically processed.
- Integration with Pdiver API: Pdiver API follows the High Fidelity Data specification, offering two essential functions:
    1. **Detection:** Identifies sensitive information within the email content, such as Social Security numbers, credit card details, or healthcare data, based on predefined sensitive data elements.
    2. **Transformation:** Automatically transforms sensitive content while preserving the email’s meaning, intent, and structure, ensuring compliance without disrupting communication clarity.
- Defining Sensitive Data: On the server side, the definitions of sensitive data is centrally managed and applied to all users within the organization. This centralization ensures consistent protection across the entire organization, regardless of which employee sends the email.

- Creating one or more Rules: Administrators can define multiple Content Compliance Rules, each associated with a different set of sensitive data definitions. For instance: First rule could transform emails containing PII when sent outside the company. Second rule could ensure that internal business documents are properly secured when shared between departments. Third rule could handle email attachments, transforming sensitive content in PDFs, Excel sheets, so on.

Advantages of Server-Side Integration

- Centralized Control: all email communications are protected under consistent rules, reducing the likelihood of human error or inconsistent application of privacy policies.
- Real-Time Transformation: Pdiver automatically detects and desensitizes sensitive content as the email is processed, transforming it in real time before it is sent externally or internally to unintended recipients. This helps prevent breaches before they occur.
- Scalability: Pdiver's server-side integration is scalable, making it easy for administrators to define multiple rules and sensitive data elements, applying them flexibly across departments or teams.
- Compliance: Pdiver helps ensure compliance with privacy regulations such as HIPAA, transforming sensitive data consistently across the entire organization.
- Minimal Disruption: Employees continue their normal email workflow without needing to manually identify or handle sensitive data, as Pdiver operates automatically in the background.
- Cost-Effective: Centralized desensitization reduces the need for complex user training or additional software, offering an efficient, scalable, and cost-effective solution to data protection.

By configuring Pdiver at the server level, organizations can proactively prevent data breaches and ensure compliance with privacy regulations. This centralized approach offers robust protection for all email users, ensuring that sensitive data is automatically transformed before leaving the organization's control.

With Pdiver, the focus shifts from detecting potential issues after they occur to preventing leaks before they happen - making email communication both secure and seamless. Upcoming articles will provide practical guides on integrating Pdiver with email clients.

5. Configure Pdiver on Email Clients

While server-side rules provide organization-wide privacy protection, end users often need more customized safeguards that aren't fully covered by centralized settings. Pdiver can be integrated directly into popular email platforms like Gmail and Office365 to offer an additional, customizable layer of privacy protection. This client-side integration allows users to manually trigger the transformation of sensitive data before sending an email, ensuring more granular control over privacy compliance tailored to individual, departmental, or workflow-specific needs.

Desktop email clients, such as Thunderbird and Microsoft Outlook, provide flexibility for integrating Pdiver directly into the application, enabling users to manually desensitize sensitive data before sending an email. This approach offers greater control over the privacy protection process.

Thunderbird Integration: Adding a "Pdiver" Button

In Thunderbird, users can add a custom "Pdiver" button that triggers Pdiver's API call for data transformation:

- Follow the Thunderbird Add-on Guide: exploring the code example.

- **Create the "Pdiver" Button:** When composing an email with sensitive data, users can click the "Pdiver" button to activate the API, transforming sensitive elements while preserving the email's structure, content, and intent.
- **Advanced Customization:** Thunderbird's extension framework allows users to customize the functionality, such as transforming specific sections of the email (e.g., the message body), providing flexible privacy protection options.

Microsoft Outlook Integration: Creating Add-ins

In Microsoft Outlook, Pdiver can be integrated via custom add-ins:

- **Navigate to Add-in Settings:** Open Outlook, then go to Tools > Get Add-ins.
- **Create a Custom Add-in:** Use the configuration dialog to create a Pdiver add-in that connects with the Pdiver API. This allows users to manually trigger data transformation when sending emails containing sensitive information.
- **Advanced Outlook Options:** Outlook's add-ins can be customized to target specific components of the email, allowing users to control which parts are desensitized, providing flexible privacy management.

Advantages of Client-Side Integration

- **Flexibility:** Users control which parts of the email need desensitization, making it ideal for cases where automated filters are too broad.
- **Customization:** Client-side integration offers personalized privacy protection tailored to specific needs without affecting overall email usability.
- **Ease of Use:** Once set up, users can easily desensitize sensitive information with a single click, minimizing disruptions to workflow.
- **Seamless Integration:** Pdiver integrates smoothly with web and desktop email clients, ensuring consistent privacy protection across platforms without requiring additional software or extensive training.
- **Real-Time Protection:** Emails are desensitized before being sent, reducing the risk of data breaches and ensuring regulation compliance.

Summary

Unintentional data breaches through email can result in significant financial, reputational, and legal consequences for organizations, particularly when dealing with sensitive data like PII or PHI. HiFiData Pdiver transforms sensitive data in real time and can be seamless integrated with popular platforms such as Gmail and Office365* make it an effective and flexible solution for preventing email breach.

By deploying Pdiver at multiple stages, organizations can effectively balance privacy compliance and email usability.

Server-side integration automates the transformation of sensitive data for all users, ensuring that emails are secured before sending whether internally across departments or externally with unauthorized recipients. Client-side integration allows users to manually transform sensitive content, offering greater flexibility and control, especially in complex or sensitive email scenarios.