Proofpoint Regulatory Compliance Module

Large enterprises, universities, and government organizations are now subject to a growing number of privacy-related regulations that govern the handling of certain types of non-public information (NPI). These regulations extend to the content of email messages leaving the organization.

comprehensive compliance

Ensuring outbound email compliance

The Proofpoint Regulatory Compliance™ module, an optional component of the Proofpoint Messaging Security Gateway™ and the Proofpoint Protection Server®, makes it easy to ensure that outbound messages comply with many different types of email-related regulations, including HIPAA, GLBA, PCI compliance guidelines and SEC regulations. Predefined dictionaries and "smart identifiers" automatically scan for a wide variety of non-public information, including PHI (protected health information as defined by HIPAA) and PFI (personal financial information as defined by GLBA) and let you take appropriate actions on noncompliant communications.

Rules can be easily created or modified via a point-and-click interface to support compliance with many other types of information privacy and data security regulations, such as state regulations (for example, California AB 1950 and California SB 1386), Canada's PIPEDA, and various European privacy directives.

features

Detect all types of privacy data inside email

Proofpoint Regulatory Compliance includes a wide variety of out-of-the-box features that help keep your organization compliant with today's information privacy rules. Proofpoint Regulatory Compliance monitors all outgoing email to detect NPI based on dictionaries as well as common NPI identifiers.

Predefined and custom dictionaries

A variety of predefined dictionaries and sample policies are included. These dictionaries define common protected health information code sets—such as standard disease, drug, treatment, and diagnosis codes used by the healthcare industry (see sidebar on reverse)— to simplify HIPAA compliance. Proofpoint also includes a variety of financial privacy dictionaries—such as SEC, insider trading and trade confirmation terms used in the financial services industry—to aid with compliance with GLBA, PCI and SEC compliance.

New dictionaries can also be defined. These dictionaries can support both exact matches as well as regular expressions. The included HIPAA dictionaries can be expanded to include terms and codes specific to your medical environment, and new dictionaries can be added to support additional regulations such as NASD, PIPEDA, and others. Dictionary terms can be weighted to increase or decrease the matching strength of any term, or to allow exceptions. The Proofpoint Dynamic Update Service™ ensures that installed dictionaries are always up to date with the latest codes.

NPI identifiers

Proofpoint Regulatory Compliance can also scan for common NPI identifiers such as Social Security numbers, ABA routing numbers, and credit card numbers. These "smart identifiers" are more sophisticated than simple regular expressions. The module looks for the correct number of digits, but also computes checksums to confirm that numerical strings that appear to be NPI are actually protected information. This technique greatly reduces the chance of false positives. Custom smart identifiers can easily be added to support customer-specific data types such as account numbers, patient numbers, medical record numbers, billing codes and local forms of ID. Like Proofpoint's built-in smart identifiers, custom-created identifiers can perform complex, algorithmic processing to ensure high detection accuracy while minimizing false positives.
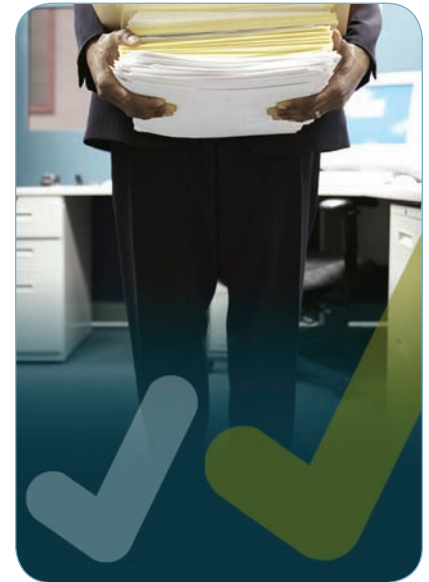
Flexible Message Actions

Messages that are identified as containing NPI can be handled using any of Proofpoint's standard message dispositions, including:

- Encrypt or reroute to an encryption device. For example, messages that contain more than three terms from the PHI dictionaries can be automatically routed to the Proofpoint Secure Messaging module.
- Redirect. Send the message to a legal or compliance officer for further review, or send the message to an archive mailbox for an archiving and audit trail.
- Quarantine. Send the message to a specific folder for later review.
- Reply to sender. Email the sender with text describing the breach and a link to an intranet site explaining your organization's privacy policy.
- Reject or block. If you choose to adopt a strict policy, these options can be used to ensure that noncompliant messages never leave your organization.
- Add X-Header. Add a string to the message header to track all messages that have been filtered by the Regulatory Compliance module.
- Annotate. Add a disclaimer to the message as a footer or an annotation in the subject line.

Proofpoint Regulatory Compliance Module

features

Flexible privacy rules and policy definitions

A point-and-click interface makes defining and modifying even complex privacy rules quick and easy. Rules can be configured to apply to individual occurrences of NPI or when a certain count of dictionary or NPI identifiers is reached. For example, a rule for tracking fraud or theft of credit card numbers can be set up to trigger only if more than three credit card numbers are detected in a message.

Any number of privacy rules can be defined to support specific compliance requirements. Multiple rules can be mapped into policies; for example, a HIPAA policy, a GLBA policy, and an AB 1950 policy. Policies can be further customized to apply only to lists of business partners or only to specified inbound or outbound message routes.

Encryption support

Many regulations specify that non-public data must be transmitted in a secure or encrypted format. Proofpoint Regulatory Compliance supports several types of encryption:

- **TLS (Transport Layer Security)**

  When used with the Proofpoint Messaging Security Gateway appliance, the Regulatory Compliance module can be used to define a set of business partners with whom email should always be encrypted. Messages sent to those partners are automatically transmitted using the TLS gateway-to-gateway encryption protocol.

- **Proofpoint Secure Messaging and other third-party encryption solutions**

  Automatic, content-aware encryption of messages is enabled by the Proofpoint Secure Messaging™ module. Policies can easily be configured to encrypt messages based on detected NPI content, sender, recipient and other conditions. Additionally, Proofpoint Regulatory Compliance easily integrates with a wide variety of third-party secure messaging solutions.

Reporting

Proofpoint Regulatory Compliance helps your organization monitor or track compliance progress with graphical reports that show the number of regulatory breaches over a given timeframe as well as the top offenders of these policies. Reports can be emailed on a scheduled basis or published to an intranet site.

In most enterprises, content security policies are managed by a variety of business users who own responsibility for compliance or data protection. Proofpoint Compliance Incident Manager™ reports makes it easy for these managers to track and review content security violations and take appropriate actions on non-compliant messages. Managers are immediately notified of policy violations and associated severity levels, so business users can easily and effectively review non-compliant messages and release, reroute, approve or otherwise dispose of such messages using Proofpoint's graphical user interface.

As a first step to understanding their regulatory risk exposure in email, organizations can deploy Proofpoint Regulatory Compliance in an audit mode, which monitors all regulatory breaches without altering messages in any way. Reports can then be used to quantify your organization's level of risk.

Attachment scanning and support for custom or proprietary document types

Built-in attachment scanning capabilities allow you to apply your Regulatory Compliance policies to the contents of message attachments. Policies can be enforced on content in more than 300 types of document attachments. In addition to the hundreds of built-in document types that Proofpoint's outbound email security modules natively understand, administrators can use Proofpoint's File Type Profiler to easily extend support to new, custom or proprietary file types (e.g., proprietary CAD/CAM formats).

Compliant Security

Many privacy and data security regulations not only specify rules for handling non-public information, but also define security requirements for systems that process this information. Proofpoint provides the security and access control features required to meet these regulations.

Stringent password policies

Servers can be configured to require arbitrarily stringent passwords and enforce password expiration dates.

Access control capabilities

Access to the Regulatory Compliance module can be restricted to select individuals and groups, so only authorized staff can create and modify compliance policies.

Dictionaries and Identifiers

Includes the essential building blocks to meet a wide variety of privacy regulations.

Healthcare code sets

The module includes a large assortment of dictionaries preloaded with code sets for PHI detection, required for compliance with HIPAA and other healthcare regulations.

- ICD-9-CM diagnosis and procedure codes
- HCPCS common procedure codes
- NDC drug codes
- Numerous other medical code sets

Financial & privacy smart identifiers

Includes "smart identifiers" for personal identity and PFI detection, such as:

- US Social Security, Canadian Social Insurance, UK National Insurance, Japanese residence registration and driver's license IDs, and other unique personal identifiers
- ABA routing numbers
- Credit card numbers (US & international)
- CUSIP securities identifiers, SEC filings, trade confirmations

Customized smart identifiers

A plug-in architecture allows organizations to add their own custom "smart identifiers" for customer- or location-specific data types such as:

- Medical record numbers
- Financial services account numbers
- Local forms of ID