Protecting Personally Identifiable Information (PII) with Classification and Content Inspection

TITUS White Paper

At TITUS we work to help businesses better manage and secure valuable corporate information. Our focus is on building policy management solutions that make it easier for IT administrators to protect and manage corporate correspondence including email and documents.

For further information, contact us at (613) 820-5111 or email us at info@titus.com

www.titus.com

Table of Contents

1.0 | Executive Summary

Personally Identifiable Information (PII) refers to information that can be used to uniquely identify or locate a single person, or can be used with other sources to uniquely identify a single individual. PII has become much more important as information technology and the Internet have made information easier to collect, leading to a profitable market in collecting and reselling this information. PII can also be exploited by criminals to stalk, or to steal the identity of a person.

As a response to these threats, lawmakers have enacted a series of legislations to limit the distribution and accessibility of PII. This paper discusses issues related to protection of PII within large organizations, and provides IT professionals and executives with an overview of the issues related to PII and privacy. It describes information labeling and content inspection strategies to comply with requirements to manage private personal information in documents and email. It also describes how to involve users in the process of protecting PII by using strategies that promote user awareness and education.

2.0 | The Privacy Challenge

Organizations of all sizes and types rely on electronic interchange of information and the Internet to communicate with clients and customers, partners and suppliers. This information, which often includes personal information about citizens and customers, is the lifeblood of government, commercial, and military organizations.

New privacy and breach legislation establishes the rules that govern the collection, use and disclosure of this personal information. Due to privacy and breach legislation, organizations must act in a manner that recognizes the right of privacy of individuals with respect to their personal information. While there is a recognized need for organizations to collect, use or disclose personal information, procedures for doing so must reflect appropriate care when handling personal information.

Examples of personal information to be protected include:

- Name, identification numbers, credit card numbers, and income
- Evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, and loan records
- Information on medical or health conditions, racial or ethnic origin, and religious beliefs

Privacy and breach rules typically prohibit organizations from collecting, using or disclosing personal information without the knowledge and consent of individuals, except in extremely limited and specific circumstances. Examples of Privacy and Breach Legislation include:

- U.S. standards such as the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (SP 800-122).
- European Union standards such as EU directive 95/46/EC, also referred to as the Data Protection Directive. This directive regulates the processing of personal data within the European Union.
- Canadian standards such as the Personal Information Protection and Electronic Documents Act (PIPEDA), which provides broad protection of personal information held by private organizations and stipulates that this information must be made available on demand to the individuals it relates to.

Other legislation involving the protection of personally identifiable information (PII) includes the California data breach notification law, SB1386, the Massachusetts Data Security Law 201, and many other state breach notification laws.

In order to build the necessary procedures to ensure privacy compliance, organizations must ask questions such as:

- Are there procedures to ensure that personal information is not disclosed to others within the organization and/or third parties, except with the consent of the individual or as required by law?
- Is personal information destroyed, erased or made anonymous when it is no longer needed for the identified purposes or no longer required by law?
- Are audit trails required for all systems that process personal information?
- Have compliance monitoring and enforcement mechanisms been implemented?
- Are physical, organizational and technological security measures used to control access, modification, collection, use, disclosure and/or disposal of personal information?

From a business perspective, the benefits of protecting the personal information of their clients include:

- Protecting the organization's public image and brand
- Enhancing credibility and promoting continued consumer confidence and goodwill
- Achieving a competitive advantage in the marketplace
- Meeting the membership requirements of an industry association
- Efficiently managing personal information and, thereby, reducing administration and avoiding unnecessary financial costs, such as retrofitting information systems

Furthermore, an organization that protects personal information will likely satisfy government and regulatory requirements in North America and abroad.

3.0 | Information Labeling and Content Inspection

Electronic tagging or labeling of PII contained in electronic documents and email is a technique for complying with the requirement for protecting private personal information. With information labeling, organizations have an effective strategy for managing and controlling the distribution of private personal information via email and electronic documents.

Content inspection of email correspondence and electronic documents is another effective method of controlling the distribution of information containing PII. Technologies that can scan email and electronic documents and find potential PII can be used to warn users or block sending of the information.

The following sections describe ways in which information labeling and content inspection can be used in several example industries.

3.1 | Example – Financial Industry

Over the past several years, insider trading, misrepresentation of the prospects of securities and inadvertent disclosure of sensitive private information in the financial services industry have led to more stringent laws governing their behaviour.

Financial services companies face a wide range of regulations that impact information technologies in general and email in particular. In the United States, for instance, the Financial Modernization Act, also known as the Gramm-Leach-Bliley or GLB Act, aims to protect the privacy of customer information held by financial institutions. GLB stipulates stiff penalties and extends to electronic data including email in transmission and in storage.

Regulations from the Securities and Exchange (SEC) restrict forward-looking statements at certain times and enforce quiet times associated with registration filings. Other SEC rules stipulate that a wide range of records and communications be maintained and readily accessible for examination for significant periods of time, including interoffice memoranda and communications.

The Fair Credit Reporting Act places the responsibility for maintaining the privacy of personal credit information squarely on credit bureaus.

Content inspection at the desktop can be used to prevent the loss of personal or customer information. Content inspection can scan outgoing email or documents for information such as customer numbers, social security numbers, credit card numbers, driver license numbers etc. Some technologies can warn users as soon as such information is found, providing targeted security education at the time of the policy violation. In other cases, a gateway appliance may scan for information and return as non-deliverable a message with this type of information. Generally, the shorter the delay between the user

hitting Send and when the user receives a policy warning the better. Policy warnings which appear as soon as the user hits Send can also serve as a means of reinforcing training and corporate policy on how to handle private information.

In situations where financial services companies have divisions or groups that could be put into an ethical conflict by sensitive customer information, such as where the possibility of insider trading exists, particular care must be taken to ensure that email systems protect ethical walls. Information labeling can be used to effectively manage and control email and meet a variety of challenges faced by financial institutions. Labeling can be used to enforce internal ethical walls by preventing sensitive information from being shared inappropriately. Email and documents labels are used as visual indicators to warn readers of the sensitivity of the information. These labels promote awareness of sensitive information which leads to better handling, storage and distribution of the information. In the financial industry, email or documents containing sensitive private customer information could be labeled "CONFIDENTIAL" or "SENSITIVE – PRIVATE" ensuring all staff are aware of the sensitivity of the information.

3.2 | Example – HIPAA and the Health Industry

Email has the potential to improve efficiency and reduce costs in health care delivery. For example, patient records can be quickly and efficiently shared between general practitioners, specialists, hospitals and insurers. Information labeling and security are paramount to enabling this efficiency within stringent legislative frameworks.

The Health Insurance Portability and Accountability Act (HIPAA) encourages the secure use of email for communications not only for collaborative access to patient records, but billing and administrative functions as well. HIPAA places great emphasis on the privacy and security of patient records. HIPAA specifically allows patient records to be shared by health care professionals to facilitate patient care. It forbids the sharing of these same records with third parties such as insurers, without the consent of the patient. HIPAA's restrictions on the use of patient information can extend to government departments, pharmaceutical companies running hosted trials and employers that provide group health care plans.

There have been many cases of organizations being fined for failure to maintain electronic records securely. For example, the pharmaceutical maker Ely Lilly faced sanctions when a clerk accidentally sent email reminders to over 600 trial participants using the TO field rather than the BCC field, thus exposing their identities.

Information labeling can protect against inadvertent leaks of patient information. By implementing a system that requires medical staff to label patient information, sensitive records can be used in accordance with HIPAA requirements while preventing unauthorized disclosure to insurers or other third parties. Email or documents containing sensitive private patient information could be labeled "CONFIDENTIAL" or "SENSITIVE – PATIENT INFO" ensuring staff are aware of the sensitivity of the

information. Many employers with group health insurance face similar requirements and can also realize benefits from email and document labeling systems.

Content inspection can also be used to scan outgoing email or documents for information such as patient numbers, medical history, U.S. Social Security numbers, and U.S. National Provider Identifiers. For example, if an email user accidentally attaches a spreadsheet that contains health information, content inspection can detect the mistake and prevent a HIPAA violation before the email leaves the desktop. The user receives immediate feedback about the policy violation, helping to reinforce corporate policy and prevent mistakes in the future.

3.3 | Example – Government and Military

Both government and military organizations must balance the need to share information with the need to protect it. For government agencies, the challenge is to maintain government transparency while protecting sensitive employee and citizen information. For military organizations, mission effectiveness requires information sharing, yet national security requires sensitive information to be protected from unauthorized disclosure.

In both cases, personally identifiable information must be protected. A failure to do so can result in the loss of public trust, significant remediation costs, damaged reputations, criminal penalties, and even threats to public safety and security.

Government and military organizations must comply with a range of regulations to safeguard PII, such as FISMA and NIST SP 800-122 in the U.S., and Directive 95/46/EC in the European Union. Many countries also have protective marking regulations that can be used to safeguard PII, such as GPMS in the U.K., CUI and CAPCO in the U.S., and the Email Protective Marking Standard in Australia.

Information labeling is an established method of protecting sensitive information, especially in the military. Users classify their email and documents to identify sensitive content, helping to ensure that the right information reaches the right people. Visual markings, such as “CONFIDENTIAL//PII” can be added to the email and documents so that recipients know how the information should be handled. As well, classification metadata can be used to enforce additional content protection, such as automatically applying encryption to email containing PII, or preventing PII-related documents from being copied to USB drives.

Content inspection can also be used to warn users when they are about to disclose PII to unauthorized recipients. For example, when a user attempts to send an email attachment with Social Security Numbers, content inspection can detect the policy violation and prevent the data breach before it happens. Users are educated at the time of the policy violation, helping to provide ongoing PII security training and awareness.

4.0 | TITUS Solutions

TITUS offers solutions for Classification, Data Loss Prevention, Compliance, and SharePoint Security for government, military, and commercial organizations. TITUS solutions use labeling and content inspection to help organizations protect sensitive and private information, providing effective privacy awareness and control which scales with the enterprise.

4.1 | Content Inspection

TITUS Message Classification can inspect email and file attachments for potential PII. As soon as a user clicks Send, the TITUS solution can scan the email for any inappropriate content. If any potential PII is found, the solution can prevent the Send, and will immediately warn the user of potential policy violations (as seen in Figure 1 below). This immediate feedback provides targeted and effective training for the user on appropriate handling of PII. The TITUS solution can prevent inadvertent disclosure of sensitive information, thus saving the organization from potential embarrassment or fines.

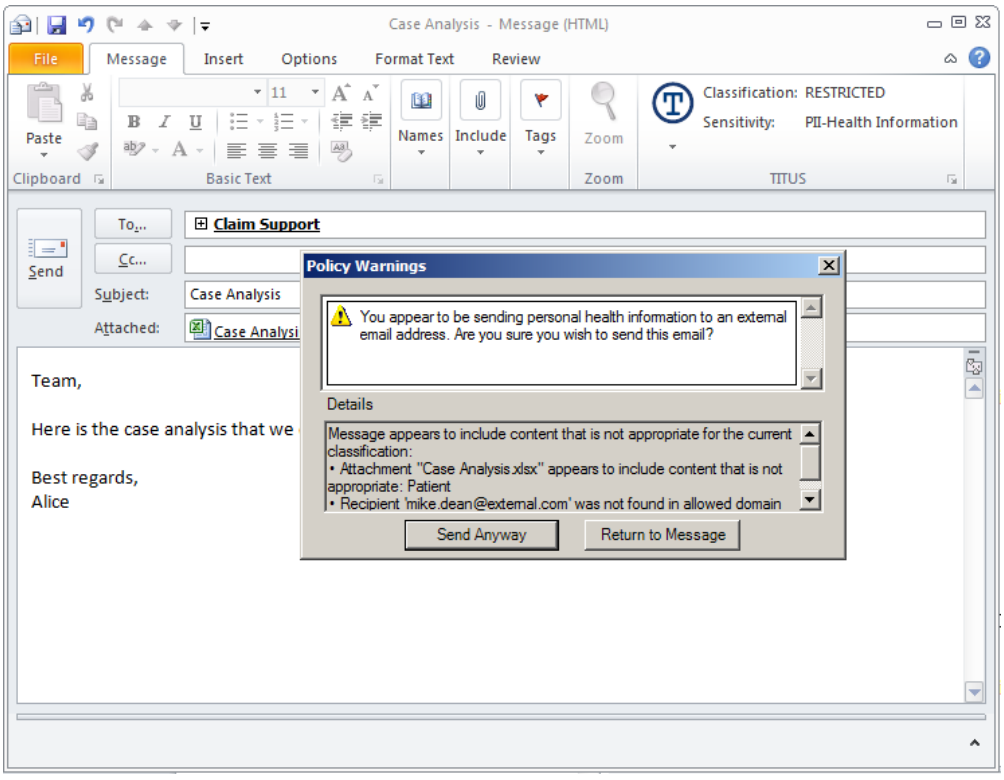

Figure 1 - Example of content inspection warning

4.2 | Information Labeling

The TITUS Message Classification and Classification for Office products provide classification and labeling for Microsoft Outlook email and Microsoft Office documents. Enforced labeling at the desktop serves to ensure that users: a) consider the ramifications of sending sensitive information, b) double-check recipients of the email, and c) verify sensitive attachments to messages. It also helps ensure that email archived for regulatory or business intelligence purposes are categorized into an effective knowledge management and retrieval schema.

TITUS Message Classification supports information labeling of Microsoft Outlook and Outlook Web Access (OWA) email, and TITUS Classification for Office supports labeling of Microsoft Word, Excel and PowerPoint documents. Labels can optionally be inserted on the first line of the message, as automated abbreviations in message subjects, and in the document header and footer, raising awareness among recipients (as seen in Figure 2 below). Labels are embedded as metadata in message and document properties and can be read by perimeter security devices and data loss prevention (DLP) solutions. Users can be forced to label a message before it can be sent, or a document before it can be saved or printed ensuring that users make conscious decisions about the handling of the information.

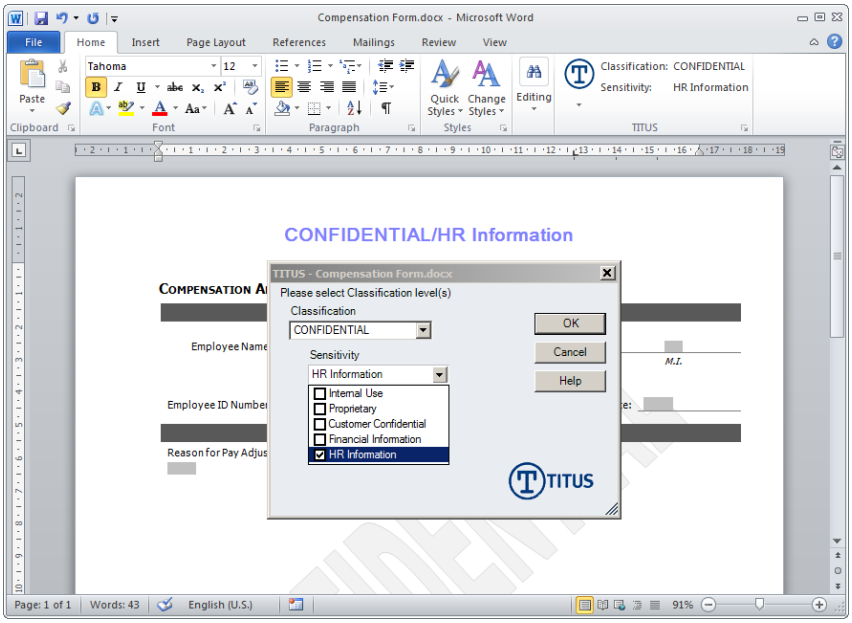

Figure 2 – Example of TITUS document labeling

Information labeling is the basis for effective control. TITUS solutions ensure that information labeled as sensitive cannot be distributed outside the organization, or sent to certain groups or individuals who should not have access to the information.

5.0 | Conclusion

Email has historically been a weak link in organizational security. While organizations have emphasized protection against threats posed by inbound messages, little has been done to protect against risks based on outbound content. Over the past several years, new privacy and breach regulations require the protection and safeguarding of private personal information. Organizations in a wide range of sectors, including the government, finance, and health industries need to respond to these more rigorous requirements.

Information labeling and content inspection tools such as TITUS Classification solutions provide organizations with the ability to protect sensitive PII. Content inspection can be used to ensure that email leaving the organization does not contain sensitive private information. TITUS' immediate policy warnings stop inadvertent leaks and reinforce corporate policy for employees. In addition, TITUS solutions place accountability on users to exercise appropriate care and caution when creating electronic email or documents. By building management and control infrastructure on top of information labeling, advantages extend from enhanced security and regulatory compliance to creation of rich, practical pools of business intelligence.