FORTRA

WHITE PAPER (Titus)

Three Steps to Protecting PII in the Government

Executive Summary

Government agencies acquire, use and store personally identifiable information (PII) about citizens, employees, patients and other individuals. Much of the sensitive information is held in unstructured formats such as documents, emails and various other file types. The exact location and storage of this unstructured information is difficult to track. This poses a significant risk for government organizations as it is hard for an organization to protect what it does not know exists.

The escalation of security breaches involving PII has contributed to the loss of millions of records over the past number of years. Breaches involving PII can harm both individuals and organizations due to identity theft, loss of public trust, legal liability or remediation costs.

This paper will discuss strategies for complying with PII privacy requirements, as well as tools designed to help organizations identify and protect unstructured PII data.

The Privacy Challenge

Organizations of all sizes and types rely on electronic interchange of information and the Internet to communicate with employees and customers, partners and suppliers. Both government and commercial organizations must collect personal information on their citizens and customers. 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 rights and 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.

This paper discusses the three key steps that must be taken by government organizations to protect PII they have in their possession.

1. Identify your PII through marking and metadata tagging
2. Educate and build awareness of the organization’s PII among employees, contractors, and partners
3. Select the appropriate controls to protect PII

Step 1 – Identify Your PII

Recently we’ve seen many examples of government breaches of information containing PII. In order to prevent these leaks, organizations must identify their PII, and must protect the PII via systems such as encryption or data loss prevention (DLP) tools.

The first and most important step in protecting PII involves the identification of PII. The types of information that should be considered PII are fairly well known, and are outlined in the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Examples are provided below.

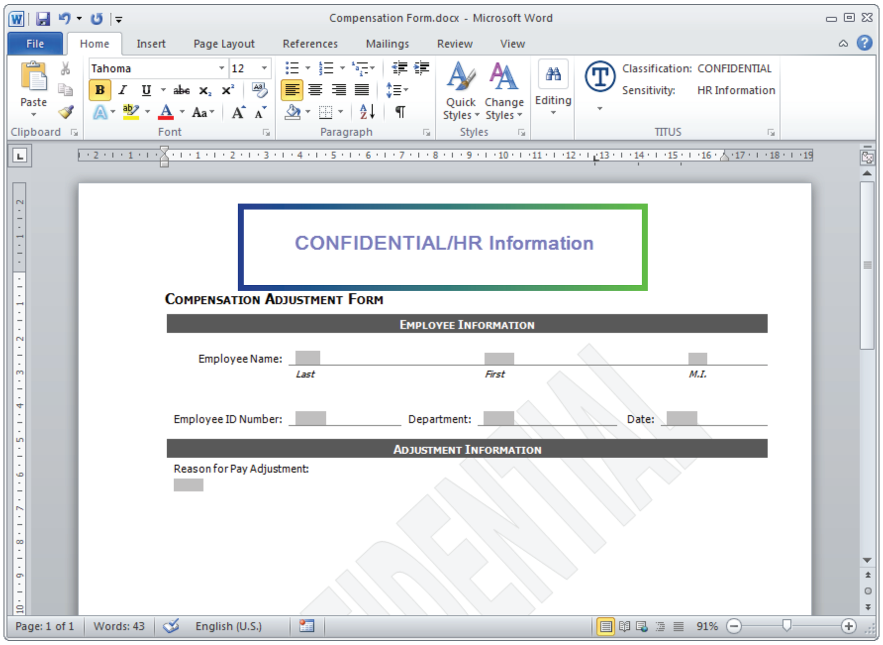
- Name, such as full name, maiden name, mother’s maiden name, or alias; address information, such as street address or email address; telephone numbers, including mobile, business, and personal numbers

- Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number

- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

Gartner estimates that in 5 years, unstructured information will grow by 650% - this roughly equates to 50% year over year growth.



Classification: CONFIDENTIAL

Sensitivity: HR Information

CONFIDENTIAL/HR Information

COMPENSATION ADJUSTMENT FORM

EMPLOYEE INFORMATION

Employee Name: Last First M.I.

Employee ID Number: Department: Date:

ADJUSTMENT INFORMATION

Reason for Pay Adjustment:

Figure 1 - Example of a document marking with Titus Classification for Microsoft Office

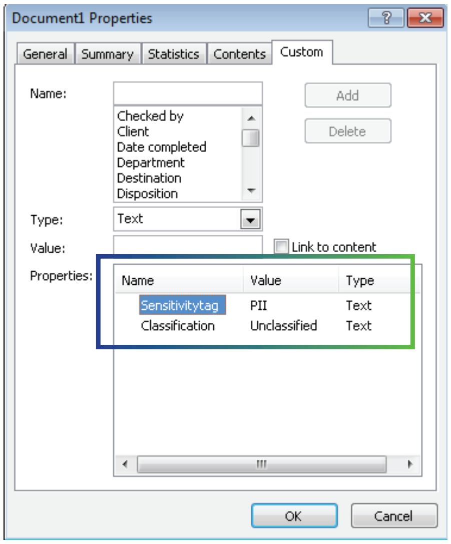
Once the types of information considered PII are understood, there remains the challenge of determining where this information is located and stored. The information generally resides in either structured data sources such as databases, or in unstructured information such as electronic documents, emails and other file types. Unstructured information poses the greater challenge as it can travel anywhere – from desktop computer to tablet to server to mobile phone. Organizations must determine how to identify which unstructured information contains PII, and how to make their employees, contractors and partners aware that certain files contain PII. Automated categorization, marking, and metadata tagging of PII are key processes which can be used to meet these objectives.

1. Automated categorization can be used to scan existing documents and emails to try to identify PII. This is a recommended method when searching a large repository of files. The disadvantages of automated categorization include false positives and false negatives which indicate sensitive information was flagged when it did not really exist or sensitive information existed but was not detected.

2. Marking and metadata tagging are two methods that can be used to identify PII as information is being created. Marking is the process of inserting visual markings in emails or documents to identify that they contain sensitive PII information.Marking has been used for decades to identify government classified information. Government directives have extended the need for marking to Controlled Unclassified Information (CUI) such as PII.

Metadata tagging of unstructured information is the process of inserting metadata into unstructured information. This metadata can be used to tag files that contain sensitive PII. Other systems such as email gateways, DLP systems, and search engines are able to read this electronic metadata and take appropriate action. Figure 2 provides an example of metadata that has been added to a Microsoft Word document.

Inadvertent data loss via employees is the #1 cause of data breach. We cannot entirely depend on people as they can make mistakes and accidentally leak sensitive PII. We need the help of electronic systems to track and find PII. Without metadata tagging there is no reliable way for systems such as email gateways, DLPs etc. to verify the sensitivity of information before it is released outside the organization.



Name	Value	Type
Sensitivitytag	PII	Text
Classification	Unclassified	Text

Figure 2 - Metadata added to Microsoft Word document

> Most data breaches are caused by mundane events such as employees losing, having stolen or simply unwittingly misusing corporate assets.
> Forrester Research

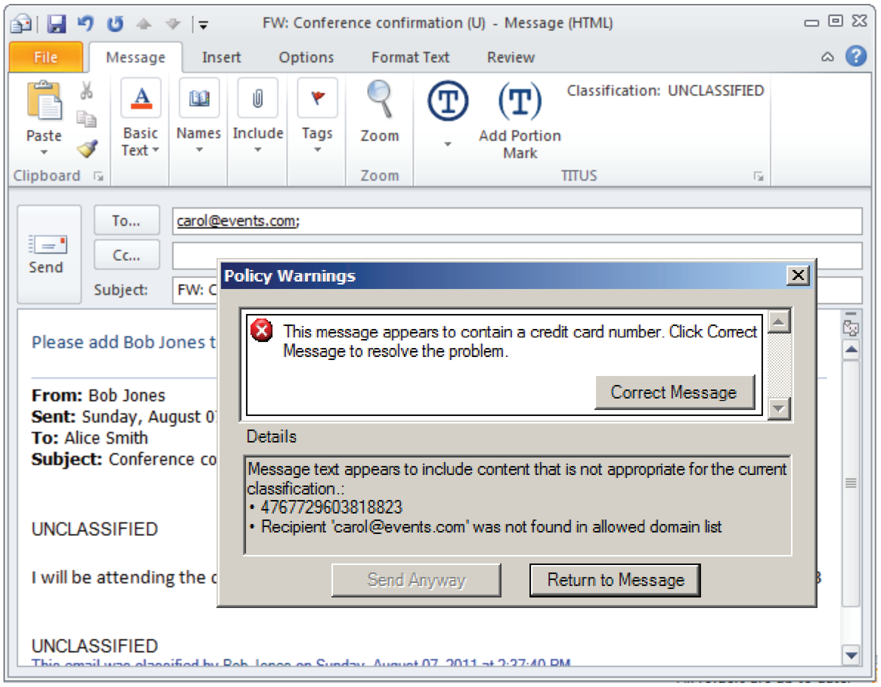
Step 2 – Educate and Build Awareness of PII

The NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* proscribes two types of operational safeguards for PII protection: policy and procedure creation; and education, training, and awareness. Organizations should develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and where appropriate, at the system level.

But even the most carefully crafted PII handling policies and procedures are unlikely to succeed if the organization does not involve its information creators in the protection of PII as part of their standard way of doing business.

Awareness and training for end users – whether through standalone educational programs, or through real-time notification of policy violations by way of the technical solutions which are deployed – helps not only to create a general awareness of security and compliance for sensitive PII, but also to foster a greater accountability for the data creators to see that information is properly protected.

Training on the proper identification and handling of PII is a must for any organization. But often end users tend to forget their training after a few weeks or months. Some method is needed to continue to educate users while they are working. Automated content warnings and markings are two excellent ways to keep users engaged in the process of protecting PII. Automated content warnings should be built into the end user's normal process. For instance, if the user is creating a document that contains PII, they should be immediately warned to mark and tag the document. In addition, if they are sending an email that contains PII (either in the message or an attachment) they should be immediately warned, especially if some of the recipients are outside the organization. Figure 3 below provides an example of a content warning system built into Microsoft Outlook. These types of warnings provide ongoing education to the user on how to handle sensitive PII, and create awareness of the organization's desire to continually protect sensitive information.



Classification: UNCLASSIFIED

To: carol@events.com;

Subject: FW: C

Please add Bob Jones t

From: Bob Jones
Sent: Sunday, August 0
To: Alice Smith
Subject: Conference co

UNCLASSIFIED

I will be attending the c

UNCLASSIFIED

This message appears to contain a credit card number. Click Correct Message to resolve the problem.

Message text appears to include content that is not appropriate for the current classification.:
• 4767729603818823
• Recipient 'carol@events.com' was not found in allowed domain list

Figure 3 - User receives warning of PII in email with Titus Classification for Microsoft Outlook

Step 3 – Select the Appropriate Controls to Protect Your PII

Many types of security controls are available to safeguard the confidentiality of PII. The items listed below are some of the NIST SP 800-53 controls that can be used to help safeguard the confidentiality of PII.

- Access Enforcement
- Separation of Duties
- Remote Access Controls
- Access Control for Mobile Devices
- Audit Review, Analysis, and Reporting
- Identification and Authentication
- Transmission Confidentiality via Encryption
- Protection of Information at Rest
- Information System Monitoring via Automated Tools

The Titus Advantage

Titus security solutions provide several critical components for an effective data governance strategy. Involving end users allows organizations to ensure all of their important information is identified or classified as it is being created and shared. Whether it is during the creation of emails, documents, or other file types, your users become part of the solution, instead of part of the problem. Titus allows users to identify or classify this unstructured information, and educates them on proper data handling. Because the information is identified, organizations can better manage and secure their information and meet their data governance and compliance requirements.

Titus is uniquely positioned to meet the classification requirements of government and military customers. As the leading provider of user-based email and document classification solutions, Titus offers a complete classification management solution for the Microsoft Office platform. Titus products include:

- Titus Message Classification™ which provides marking, metadata tagging, and automated content warnings for email created in Microsoft Outlook®, Outlook Web Access , Lotus Notes and mobile devices
- Titus Classification for Microsoft Office™ which provides marking, metadata tagging, and automated content warning for Microsoft Word®, PowerPoint®, and Excel® documents
- Titus Classification for Desktop allows all other file types (like PDF, Jpeg, CAD etc…) to be classified by users. So users can classify their files within the Windows Explorer paradigm with a simple right click.
- Metadata security and marking solutions for Microsoft SharePoint®
- File server classification solutions for Microsoft Windows Server 2008 File Classification Infrastructure® (FCI)

Titus solutions are widely deployed in government organizations throughout the world. Customers include the United States Department of Defense, NATO, US Department of Veterans Affairs, Australian Department of Defense, Department of Finance Canada, Danish Defence, and numerous other government organizations. To find out how Titus can help your organization optimize information sharing, please visit www.titus.com.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.