IDERA® | Database Tools Whitepaper

PROTECTING PERSONALLY IDENTIFIABLE INFORMATION IN DATABASES

INTRODUCTION

The data resources of an organization are one of its most valuable assets. Except for its people, the information contained in enterprise databases and how it is used is one of the most differentiating factors when comparing similar companies. Productive utilization of data assets through analytics can result in obtaining substantial competitive advantages in the marketplace.

Information streams such as big data and the Internet of Things (IoT) have increased the volume of data, its diversity, and the rate at which it is generated and collected. The differences in structured and unstructured data elements further complicate thoroughly processing and categorizing the information that ends up in databases of an organization.

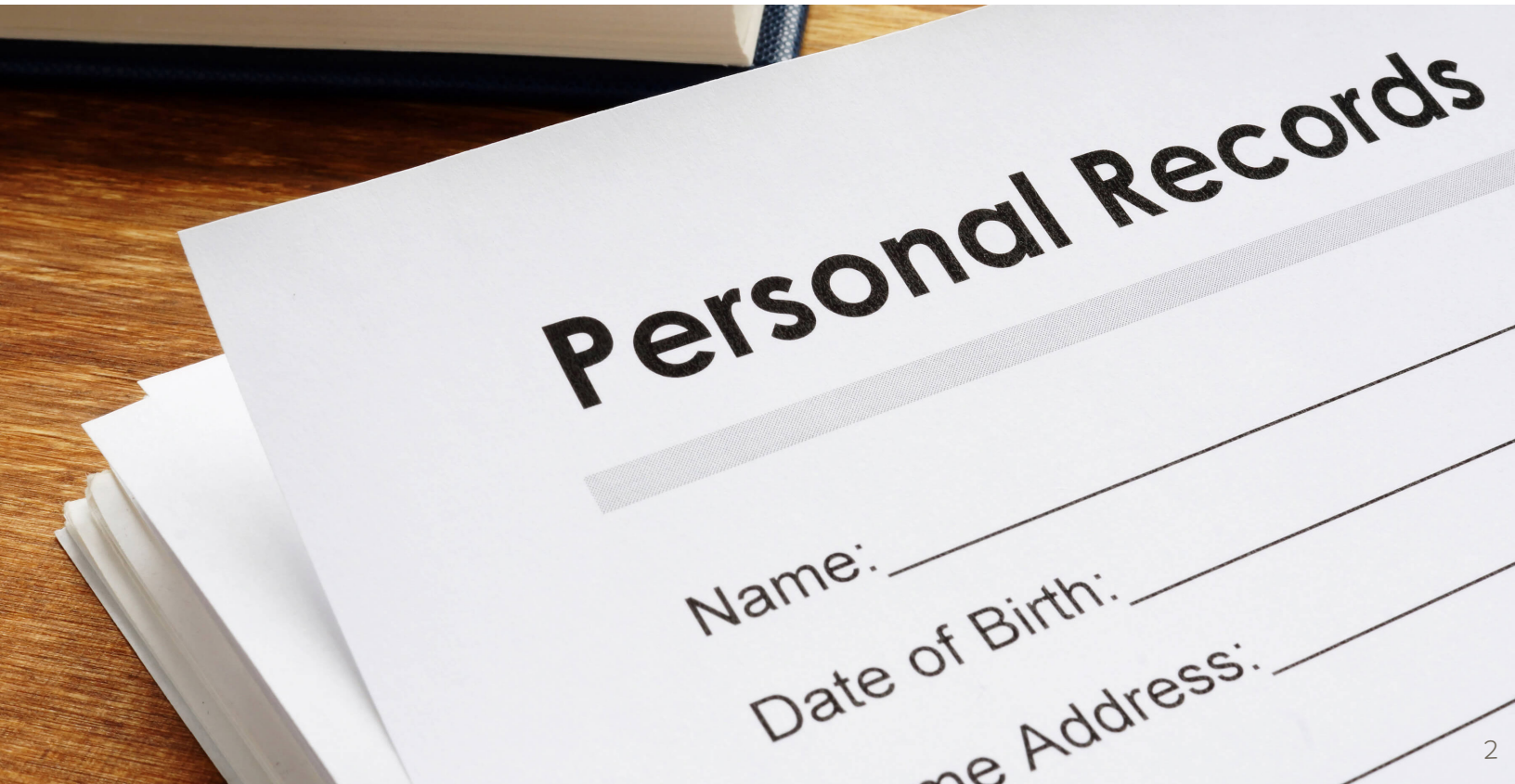
Not all data is of equal importance to the entities responsible for its creation and storage. In particular, personally identifiable information (PII) needs to be handled more securely than the average data. In this paper, we will discuss the methods and techniques that should be used to protect PII to safeguard the individuals identified by the data and the organizations that store these resources in enterprise databases.

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

Personally identifiable information is defined as data that can be used to distinguish or trace the identity of an individual. That PII can be either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples of PII include your name, work email, home address, and phone number. This type of information enables someone in possession of it to contact an individual directly, either physically or online.

A subset of PII that demands even more stringent protective measures is sensitive personally identifiable information (SPII). SPII is personally identifiable information, which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. The increased risk to individuals that accompanies compromised SPII as well as its potential value to hackers and malicious entities makes it critically important that the proper measures are taken to protect it.

Organizations need to ensure that all the PII data resources that they collect, store, and process are adequately protected. In cases where SPII is involved, the level of protection needs to be strengthened. It is never a poor idea to treat all enterprise PII and SPII with the same degree of care. Overprotection of PII is always preferred over lax security that puts the data at risk. An additional consideration is that the sensitivity of PII can change from when it was first collected.



CATEGORIZING DATA RESOURCES

An essential characteristic of PII data elements is that they can present different levels of sensitivity when viewed as stand-alone items as when used in conjunction with other pieces of information. An example is the full name of an individual which, when taken in isolation, is considered a piece of PII. When the name is part of the patient list of a doctor, it rises to the level of SPII. Information such as the name and credit card number of a customer are more sensitive when they are viewed together than when seen as individual items.

These different levels of sensitivity complicate the task of categorizing the information stored in databases of an organization. Some of the individual parts of a database record may be innocuous as a stand-alone piece of information and not be considered SPII. When the complete record is viewed, the components can constitute PII or SPII. For this reason, care needs to be taken when determining which databases need the full protection afforded to SPII data resources. It is never a poor policy to err on the side of caution and provide stringent protection to data assets that may contain sensitive information in any form.

Some examples of stand-alone SPII include

- Social security numbers;
- Financial account numbers;
- Drivers' license or state identification numbers.

These items, in combination with other data components, can result in SPII:

- Medical information;
- Account passwords;
- Last four digits of a social security number;
- Date of birth;
- Criminal history.

When classifying data as PII or SPII, database records should be categorized based on the security needs of their most sensitive components. Records that contain the name, address, and order history of a customer may be viewed as PII. When payment information is added to the record, the classification rises to the level of SPII.

STEPS TO PROTECT PII AND SPII IN DATABASES

Fully protecting the PII and SPII in enterprise databases is a non-trivial exercise that requires a comprehensive, multi-step strategy. Some steps involve technical solutions, while others may require an evolution of corporate policies and additional training throughout the organization. Here are the best practices to implement when PII and SPII need to be protected.

IDENTIFY THE PII COLLECTED AND STORED BY THE ORGANIZATION

The identification of PII is a crucial first step that sets up all subsequent security procedures. It is impossible to successfully protect resources that have not been appropriately identified. An organizational view must be used to determine the kind of data that needs to be protected. The type of business or organization may play a role in the specific forms of PII stored in its databases.

LOCATE WHERE PII IS STORED

Once the PII that an organization uses is identified, all places where the data is stored need to be found. Some locations may include on-premises and cloud databases, file servers, and laptops of employees. The data resources encompass three states that all need to be addressed to protect PII fully.

- **Data in use** refers to data being used by employees to perform their jobs.
- **Data at rest** is data stored in databases, disk drives, and other storage media.
- **Data in motion** is information that is transitioning between locations..

Considering the data resources that occupy these states will clarify where PII resides, how the organization uses it, and which systems need additional security.

CLASSIFY DATA SENSITIVITY

Data resources need to be classified to develop a viable protection strategy. Depending on the organization and the market sector it inhabits, compliance issues may inform the way information is classified. A minimal classification scheme will identify data in the following categories.

- Public data is low-risk information with negligible or no access restrictions.
- Private data can cause moderate levels of damage to the organization or identified individuals if it is compromised. This data should only be accessible by users performing specific functions within the enterprise.
- Restricted data comprises SPII that would cause substantial damage if compromised. Access to data at this level is severely restricted throughout the organization.

DEVELOP AN ACCEPTABLE USAGE POLICY

Policies need to be implemented that define who can access PII and under what circumstances it can be used. These policies can be codified into technological solutions that enforce proper access and usage throughout the computing environment. Internal audits should be performed to ensure that these policies are being followed. Regulatory compliance concerns should be taken into account when devising the usage policy.

ENCRYPT PII AND SPII

PII and SPII should be encrypted when in use, at rest, and in motion. That encryption implies that databases, employee laptops, file servers, and any other locations that contain PII need to be encrypted. Having encrypted data can negatively affect the performance of databases and other information systems. That performance degradation needs to be accepted as a consequence of storing PII and should be a non-negotiable aspect of the enterprise computing environment. The security of PII needs to take precedence over the performance of systems that use it.

Often overlooked when considering encryption are backups of an organization. They also need to be encrypted to protect the information on storage media that may be kept in long-term and offsite facilities.

DELETE OBSOLETE PII

Sensitive data that is no longer needed by the organization should be deleted from all systems and storage media. Such sensitive data includes backups and may necessitate new backup policies to address this issue. Specific compliance regulations, such as the General Data Protection Regulation (GDPR), grant users the right to request that their personal information be deleted from enterprise databases. Policies need to be in place to handle this situation as well as purging data from entities that are no longer associated with or required by an organization.

REVIEW AND RESOLVE PERMISSION ERRORS

Inappropriate permissions can result in unauthorized access to PII and SPII. The principle of least privilege should be enforced throughout the organization so that only those with a valid reason to access sensitive data can do so. This principle restricts access rights to the lowest level possible while allowing employees to do their work. Using this strategy provides enhanced security by controlling unauthorized access and limits the damage that the computer of the user can cause if it is compromised by malware.

When implementing the principle of least privilege, users should first be assigned minimal access rights even if they are insufficient to perform their jobs adequately. That principle eliminates the possibility of providing higher privileges than necessary. It is a better policy to add access rights as needed rather than trying to remove those that are excessive.

EDUCATE EMPLOYEES REGARDING PII

Every employee should be educated regarding the usage policy surrounding PII and engage in training to ensure they understand their responsibilities in protecting enterprise data resources. Part of this education should include establishing a method of communicating suspicious behavior to management. New employees should be required to take this training before obtaining credentials on any systems that may contain sensitive information.

CREATE STANDARD PROCEDURES FOR EMPLOYEES LEAVING THE ORGANIZATION

Former employees can remain an internal threat to data privacy after they have left an organization. Several steps can be taken to guard against this possibility, including:

- Immediately removing all user accounts and access to computing resources;
- Obtaining a signed confidentiality agreement;
- Communicating the responsibilities of the individual concerning enterprise PII.

REASONS TO PROTECT PII AND SPII

There are some compelling reasons why an organization should be concerned with protecting the PII and SPII in their databases. Failure to keep sensitive data secure can have ramifications that challenge the ability of an enterprise to maintain its operation.

The inability to safeguard PII results in data breaches in which unauthorized entities gain access to sensitive information. A data breach causes the following problems for the affected organization.

- Financial penalties can be enforced by regulatory agencies who determine that the enterprise was not exercising the proper procedures to remain compliant with privacy standards. These penalties can be very severe and are designed to force companies to take the protection of PII and SPII more seriously. As more jurisdictions implement privacy guidelines, the financial implications of non-compliance will continue to grow.

- Financial restitution to the individuals impacted by a data breach can also negatively affect the bottom line of an organization. It is a common practice to offer credit and identity protection to people whose information has been compromised due to a data breach. Depending on the number of records involved in the violation, this can be a costly proposition.

- The repercussions on customer confidence may wind up being the most expensive outcome of a data breach. It can take years to rebuild the trust that can be destroyed when an organization loses control over the SPII of its customers. In many instances, a company may never regain its standing with previous customers and be challenged with finding new customers in the wake of a data breach.

TOOLS FOR PROTECTING PII AND SPII IN DATABASES

The complexity of modern, multi-platform database environments makes it impossible to implement manually the steps required to protect PII and SPII in databases fully. Automated processes and tools are needed to augment the training and assist the organization in several ways.

- Identifying and locating PII requires tools that can interrogate databases and discover where sensitive data resides. These software solutions are necessary to identify the systems that need protection and should be used regularly to stay abreast of changes in the environment.
- Managing permissions is an ongoing process that requires robust monitoring and regular auditing. Attempts at accessing systems by unauthorized entities can be discovered and addressed by monitoring tools. Periodically auditing the permissions currently in place can identify credentials that should be eliminated or modified to afford better protection for sensitive data.
- Demonstrating compliance with regulatory regulations is an essential task that demands flexible reporting tools. The ability to produce informative reports is instrumental in replying to requests from auditors and can be used to identify security gaps that can be closed before a data breach occurs.

By using comprehensive policies and the right set of software tools, organizations can give PII and SPII the care they deserve. Failure to take the necessary steps to protect this information exposes organizations to damages to their finances and reputation that may be impossible to reverse.

IDERA'S SOLUTION

SQL Compliance Manager

Monitor, audit, and alert on user activity and data changes in SQL Server databases.

Simplify your SQL Server audits. SQL Compliance Manager is a comprehensive auditing solution that monitors and tracks changes to SQL Server objects and data, and sends alerts on suspicious activity. Obtain detailed visibility to determine who did "what", "when", "where", and "how", whether the event is initiated by privileged users or hackers. SQL Compliance Manager also helps ensure compliance with industry regulatory and data security requirements. SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of all data access, selects, updates, schema modifications and permission changes to SQL Server databases.

Start a free, fully-functional, 14-day trial today!

Start for FREE