



by Ross Federgreen

IDENTITY THEFT

What You Must Know About Personally Identifiable Information (PII)

Everyone is concerned about “identity theft” and all business is subject to these occurrences happening at their facilities. Identity theft is a major concern of the majority of individuals who frequent your casino. The amount of personal individual damage that this has caused has not been lost on regulators.

Privacy is a Defining Issue of the Day for Both the Public and Private Sectors

Citizens are now aware of data breaches, identity theft and the risks that can result from personal information finding its way into illintended hands. Both federal and state legislatures have taken notice of privacy’s importance in recent years. From 2004 to the present, forty-eight state legislatures have enacted data breach notification laws mandating, to varying extents, notification requirements for citizens whose personal information has been compromised by a security breach.

The federal government has codified various elements of identity associated with an individual’s name that if violated constitute violation of Personally Identifiable Information (PII) statutes. These five elements are date of birth, social security number, driver’s license number, credit and debit card numbers, as well as bank routing and account numbers. Multiple federal agencies now have specific regulations as it regards the treatment of PII. These include the Department of Homeland Security, the Department of Defense, Federal Emergency Management Agency (FEMA), the Department of Health and Human Services and many others.

It is important to note that incorporated within the rules of the National Indian Gaming Commission under section 25 CFR 515, titled “Privacy Act Procedures” the importance of the underlying law the Privacy Act of 1974 (Public Law 93-579) codified at 5 USC 552a are delineated. This demonstrates a keen awareness of these growing and important issues. Further, the National Indian Gaming Association recognizes in their training and publications the need to be cognizant of the various rules as they relate to privacy on the part of the casinos and their employees, as well as their guests.

However, the issue of PII and the data elements that contribute to these issues is broader than the above and various regulatory agencies may take a more sweeping view. From the broadest and therefore most conservative view, PII is defined as any information that can be used to trace and specify a unique individual. CSRSI defines PII as any

information about an individual including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother’s maiden name, or alias.
- Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, or financial account or credit card number.
- Address information, such as street address or email address.
 - Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric 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).

From the view of management of these data elements, every operator must know the specific lifecycle of these elements within their operating environment. You must be able to understand why you have these pieces of information, who has access to them, how you retain them and for how long and why. The focus must be around efforts in the areas of governance, enterprise architecture efforts, policy, business processes and practices, laws and regulations, security and data protection, communications and awareness.

Lifecycle

There are four steps in the lifecycle of all data elements which are acquisition, utilization, storage and disposable. The very first question that must be answered is, why gather the information in the first instance? There must be a compelling business reason and convenience is not an acceptable response. You must be able to answer the questions of how the business environment would be served by acquiring this

information and whether there are alternatives that might substitute for this information acquisition. Whatever the reason is, the answer must be codified in a policy directive that specifies the reason for the activity.

How the information is utilized and by whom really describes the essence of the issue of utilization. How long you retain the information and what safeguards are put in place to protect the information and limit the access to the information is part of the central responsibility of the organization that handles PPI. Finally, under what circumstances and what method you dispose of the protected information completes the life cycle of each piece of protected data.

It is beneficial to state the continuous gold standard approach that should be employed when dealing with information that is classified as within the guidelines of Personally Identifiable Information. There are four steps in the process. These are (1) assessment, (2) strengthening of controls, (3) enforcement and (4) monitoring. Strengthening of controls is further subdivided into three areas of technical, managerial and operational focus.

What the above demonstrates is that once the decision to require the utilization of PII is made then a concerted and continuous effort must be made to manage in the appropriate manner the material that is obtained. This includes assessment of ongoing as well as new threats and weakness in the defensive barriers.

Examples of areas that are left unattended in many enterprises are ongoing background checks of individuals and destruction protocols for gathered information. Many of the rules that apply to PII are similar as those that apply to the PCI DSS (Payment Card Industry Data Security Standard). One of these critical components is the ongoing background check of employees, vendors and other third parties that have access to protected information. The background check process should be done on an annual basis. The background check should include financial, civil and criminal information. Changes and/or concerns in these findings should serve as an immediate red flag that further investigation is warranted and that the individual should be removed from access to PII until the issues are resolved.

Destruction policies are central to the lifecycle management of protected information. Many times destruction procedures and policies are codified and simply not followed. This leads to the unenviable position of not being able to document PII flow. In addition this leads to accumulation of this data in either or both a physical or electronic format which then becomes a source of theft. Destruction policies and procedures must be monitored and enforced. Elements of the destruction policy that should be considered include method

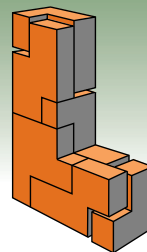
of destruction, documentation of destruction, frequency of destruction, transit points of the information through the destruction chain and others. At a minimum, the rule must be to destroy protected information so that the material is retained for the shortest period possible in the least number of physical and electronic places possible with the least number of individuals having access to the material as possible.

PII on Premises

There are multiple areas that casinos commonly collect PII data. Some examples include player's cards, guest portfolios, markers, and acceptance of electronic payments. Each of these areas must be fully evaluated to determine weakness and non-compliance with the multiple rule sets, as well as threat vulnerability likelihood. ♣

Ross Federgreen is founder of CSRSI. He can be reached by calling (866) 462-7774 ext.1 or email rfedergreen@csrsi.com.

Complete Turn-Key Services from Pre-Construction through Installation



**Your Premiere
Design/Build Partner**

LEXINGTON
DESIGN + FABRICATION

12660 BRANFORD ST | LOS ANGELES, CA 91331
818.768.5768 • WWW.LEX-USA.COM