NIST Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2010

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

Table of Contents

Appendices

2. Introduction to PII

One of the most widely used terms to describe personal information is PII. Examples of PII range from an individual's name or email address to an individual's financial and medical records or criminal history. Unauthorized access, use, or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail, or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability. This section explains how to identify and locate PII[14] maintained within an organization's environment and/or under its control, and it provides an introduction to the Fair Information Practices. Sections 3 and 4 discuss factors for assigning PII impact levels and selecting safeguards, respectively. Section 5 discusses incident response for breaches involving PII.

2.1 Identifying PII

PII is "any information about an individual maintained by an agency, 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."[15]

To *distinguish* an individual[16] is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data.[17] In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.[18]

To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status. For example, an audit log containing records of user actions could be used to trace an individual's activities.

Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.

[14] Even if an organization determines that information is not PII, the organization should still consider whether the information is sensitive or has organizational or individual risks associated with it and determine the appropriate protections.

[15] GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008, http://www.gao.gov/new.items/d08536.pdf.

[16] The terms "individual" and "individual's identity" are used interchangeably throughout this document. For additional information about the term *individual*, see Appendix B.

[17] These data elements are included in a list of identifying information from the Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998).

[18] Information elements that are not sufficient to identify an individual when considered separately might nevertheless render the individual identifiable when combined with additional information. For instance, if the list of credit scores were to be supplemented with information, such as age, address, and gender, it is probable that this additional information would render the individuals identifiable.

Organizations are required to identify all PII residing within their organization or under the control of their organization through a third party (e.g., a system being developed and tested by a contractor). Organizations should use a variety of methods to identify PII. Privacy threshold analyses (PTAs), also referred to as initial privacy assessments (IPAs), are often used to identify PII.[19] Some organizations require a PTA to be completed before the development or acquisition of a new information system and when a substantial change is made to an existing system. PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs are usually submitted to an organization's privacy office for review and approval. PTAs are comprised of simple questionnaires that are completed by the system owner in collaboration with the data owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer. Other examples of methods to identify PII include reviewing system documentation, conducting interviews, conducting data calls, using data loss prevention technologies (e.g., automated PII network monitoring tools), or checking with system and data owners. Organizations should also ensure that retired hardware no longer contains PII and that proper sanitization techniques are applied.[20]

2.2 Examples of PII Data

The following list contains examples of information that may be considered PII.

- 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, patient identification number, and financial account or credit card number[21]
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- 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).

[19] Some organizations have similar processes in place and do not call them PTA or IPA. For example PTA/IPA templates, see http://www.usdoj.gov/opcl/initial-privacy-assessment.pdf or http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf.

[20] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[21] Partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual.

2.3 PII and Fair Information Practices

The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal law.[22] The Privacy Act, as well as other U.S. privacy laws, is based on the widely-recognized Fair Information Practices, also called Privacy Principles. The Organisation for Economic Co-operation and Development (OECD)[23] Privacy Guidelines are the most widely-accepted privacy principles, and they were endorsed by the Department of Commerce in 1981.[24] The OECD Fair Information Practices are also the foundation of privacy laws and related policies in many other countries, (e.g., Sweden, Australia, Belgium).[25] In 2004, the Chief Information Officers (CIO) Council issued the Security and Privacy Profile for the Federal Enterprise Architecture[26] that links privacy protection with a set of acceptable privacy principles corresponding to the OECD's Fair Information Practices.

The OECD identified the following Fair Information Practices.

- **Collection Limitation—**There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality—**Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification—**The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation—**Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
- **Security Safeguards—**Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness—**There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation—**An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given

[22] This document focuses on protecting the confidentiality of PII. Protecting the privacy of PII is a broader subject, and information about the Fair Information Practices is provided to increase reader awareness and to improve reader understanding of the relationship between privacy and security.

[23] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* 1980.

[24] Report on OECD Guidelines Program, Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981), as cited in GAO Report 08-536.

[25] GAO Report 08-536.

[26] The Security and Privacy Profile was updated in 2009. For additional information, see Appendix D.

reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

- **Accountability—**A data controller should be accountable for complying with measures which give effect to the principles stated above.

Privacy is much broader than just protecting the confidentiality of PII. To establish a comprehensive privacy program that addresses the range of privacy issues that organizations may face, organizations should take steps to establish policies and procedures that address all of the Fair Information Practices. For example, while providing individuals with notice of new information collections and how their personal information will be used and protected is central to providing individuals with privacy protections and transparency, it may not have a significant impact on protecting the confidentiality of their personal information. On the other hand, the Fair Information Practices related to establishing security safeguards, purpose specification, use limitation, collection limitation, and accountability are directly relevant to the protection of the confidentiality of PII. As a result, these principles are highlighted throughout this document as appropriate.

For more information on the Fair Information Practices, see Appendix D.

3. PII Confidentiality Impact Levels

This publication focuses on protecting PII from losses of confidentiality. The security objective of confidentiality is defined by law as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[27]

The security objectives of integrity and availability are equally important for PII, and organizations should use the NIST Risk Management Framework[28] to determine the appropriate integrity and availability impact levels. Organizations may also need to consider PII-specific enhancements to the integrity or availability impact levels. Accuracy is a required Fair Information Practice for most PII, and the security objective of integrity helps to ensure accuracy. Integrity is also important for preventing harm to the individual and the organization. For example, unauthorized alterations of medical records could endanger individuals' lives, and medical mistakes based on inaccurate information can result in liability to the organization and harm to its reputation.

The confidentiality of PII should be protected based on its impact level. This section outlines factors for determining the PII confidentiality impact level for a particular instance of PII, which is distinct from the confidentiality impact level described in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.[29] The PII confidentiality impact level takes into account additional PII considerations and should be used to determine if additional protections should be implemented. The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. Once the PII confidentiality impact level is selected, it should be used to supplement the provisional confidentiality impact level, which is determined from information and system categorization processes outlined in FIPS 199 and NIST Special Publication (SP) 800-60, *Volumes 1 and 2: Guide for Mapping Types of Information and Information Systems to Security Categories*.[30] Supplementation of the provisional confidentiality impact level should be included in the documentation of the security categorization process.

Some PII does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly (e.g., an organization publishing a phone directory of employees' names and work phone numbers so that members of the public can contact them directly). In this case, the PII confidentiality impact level would be *not applicable* and would not be used to supplement a system's provisional confidentiality impact level. PII that does not require confidentiality protection may still require other security controls to protect the integrity and the availability of the information, and the organization should provide appropriate security controls based on the assigned FIPS 199 impact levels.

3.1 Impact Level Definitions

The harm caused from a breach of confidentiality should be considered when attempting to determine which PII confidentiality impact level corresponds to a specific set of PII. For the purposes of this document, *harm* means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are

[27] 44 U.S.C. § 3542, http://uscode.house.gov/download/pls/44C35.txt

[28] For additional information about the NIST Risk Management Framework, see: http://csrc.nist.gov/groups/SMA/fisma/framework.html.

[29] http://csrc.nist.gov/publications/PubsFIPS.html.

[30] http://csrc.nist.gov/publications/PubsSPs.html.

not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

The following describe the three impact levels—low, moderate, and high—defined in FIPS 199, which are based on the potential impact of a security breach involving a particular system:[31]

> "The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
>
> The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
>
> The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

Harm to individuals as described in these impact levels is easier to understand with examples. A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number. The types of harm that could be caused by a breach involving PII at the moderate impact level include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail. Harm at the high impact level involves serious physical, social, or financial harm, resulting in potential loss of life, loss of livelihood, or inappropriate physical detention.

3.2 Factors for Determining PII Confidentiality Impact Levels[32]

Determining the impact from a loss of confidentiality of PII should take into account relevant factors. Several important factors that organizations should consider are described below. It is important to note that relevant factors should be considered together; one factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor. Also, the impact

[31] This document pertains only to the confidentiality impact and does not address integrity or availability.

[32] Portions of this section were submitted as contributions to the ISO/IEC 29101 *Privacy Reference Architecture* and the ISO/IEC 29100 *Privacy Framework* draft standards.

levels suggested for these factors are for illustrative purposes; each instance of PII is different, and each organization has a unique set of requirements and a different mission. Therefore, organizations should determine which factors, including organization-specific factors, they should use for determining PII confidentiality impact levels and should create and implement policy and procedures that support these determinations.

3.2.1 Identifiability

Organizations should evaluate how easily PII can be used to identify specific individuals. For example, PII data composed of individuals' names, fingerprints, or SSNs uniquely and directly identify individuals, whereas PII data composed of individuals' ZIP codes and dates of birth can indirectly identify individuals or can significantly narrow large datasets.[33] However, data composed of only individuals' area codes and gender usually would not provide for direct or indirect identification of an individual depending upon the context and sample size.[34] Thus, PII that is uniquely and directly identifiable may warrant a higher impact level than PII that is not directly identifiable by itself.

3.2.2 Quantity of PII

Organizations may also choose to consider how many individuals are identified in the information (e.g., number of records). Breaches of 25 records and 25 million records may have different impacts, not only in terms of the collective harm to individuals, but also in terms of harm to the organization's reputation and the cost to the organization in addressing the breach. For this reason, organizations may choose to set a higher impact level for particularly large PII datasets than would otherwise be set. However, organizations should not set a lower impact level for a PII dataset simply because it contains a small number of records.

3.2.3 Data Field Sensitivity

Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.[35] For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code. Organizations often require the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present. Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others. Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use. For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites.

[33] A Massachusetts Institute of Technology study showed that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth. L. Sweeney, *Computational Disclosure Control: A Primer on Data Privacy Protection*, Doctoral Dissertation, 2001, as cited in American Statistical Association, *Data Access and Personal Privacy: Appropriate Methods of Disclosure Control*, December 6, 2008, http://www.amstat.org/news/statementondataaccess.cfm.

[34] Section 4.2 discusses how organizations can reduce the need to protect PII by removing PII from records.

[35] Some organizations have defined certain types or categories of PII as sensitive and assign higher impact levels to those types of PII. For example, in its PIA policy, the Census Bureau has defined the following topics as sensitive: abortion; alcohol, drug, or other addictive products; illegal conduct; illegal immigration status; information damaging to financial standing, employability, or reputation; information leading to social stigmatization or discrimination; politics; psychological well-being or mental health; religion; same-sex partners; sexual behavior; sexual orientation; taxes; and other information due to specific cultural or other factors. http://www.census.gov/po/pia/pia_guide.html.

3.2.4 Context of Use

The context of use factor is related to the Fair Information Practices of Purpose Specification and Use Limitation. *Context of use* is defined as the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated. Examples of context include, but are not limited to, statistical analysis, eligibility for benefits, administration of benefits, research, tax administration, or law enforcement. Organizations should assess the context of use because it is important in understanding how the disclosure of data elements can potentially harm individuals and the organization. Organizations should also consider whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual. For example, law enforcement investigations could be compromised if the mere fact that information is being collected about a particular individual is disclosed.

The context of use factor may cause the same types of PII to be assigned different PII confidentiality impact levels in different instances. For example, suppose that an organization has three lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization. The second list is people who have filed for retirement benefits, and the third list is individuals who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each of the three lists. Based on context of use only, the three lists are likely to merit impact levels of low, moderate, and high, respectively.

3.2.5 Obligation to Protect Confidentiality

An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Many organizations are subject to laws, regulations, or other mandates[36] governing the obligation to protect personal information,[37] such as the Privacy Act of 1974, OMB memoranda, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Additionally, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to additional specific legal obligations to protect certain types of PII.[38] Some organizations are also subject to specific legal requirements based on their role. For example, organizations acting as financial institutions by engaging in financial activities are subject to the Gramm-Leach-Bliley Act (GLBA).[39] Also, some agencies that collect PII for statistical purposes are subject to the strict confidentiality requirements of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).[40] Violations of these laws can result in civil or criminal penalties. Organizations may also be obliged to protect PII by their own policies, standards, or management directives.

Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time.

[36] See Appendix G for additional resources.

[37] Personal information is defined in different ways by different laws, regulations, and other mandates. Many of these definitions are not interchangeable. Therefore, it is important to use each specific definition to determine if an obligation to protect exists for each type of personal information. See Appendix C for a listing of common definitions of personal information.

[38] The Census Bureau has a special obligation to protect based on provisions of Title 13 of the U.S. Code, and the IRS has a special obligation to protect based on Title 26 of the U.S. Code. There are more agency-specific obligations to protect PII, and an organization's legal counsel and privacy officer should be consulted.

[39] For additional information, see GLBA, 15 U.S.C. § 6801 et seq.

[40] CIPSEA is Title 5 of the E-Government Act of 2002, Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101 et seq. CIPSEA covers all types of data collected for statistical purposes, not just PII. For additional information, see the OMB Implementation Guidance for CIPSEA, http://www.whitehouse.gov/omb/fedreg/2007/061507_cipsea_guidance.pdf.

3.2.6 Access to and Location of PII

Organizations may choose to take into consideration the nature of authorized access to PII. When PII is accessed more often or by more people and systems, there are more opportunities for the confidentiality of the PII to be compromised. Another aspect of the nature of access to PII is whether PII is being stored on or accessed from teleworkers' devices or other systems and other systems, such as web applications, outside the direct control of the organization.[41] These considerations could cause an organization to assign a higher impact level to widely-accessed PII than would otherwise be assigned to help mitigate the increased risk caused by the nature of the access.

Additionally, organizations may choose to consider whether PII that is stored or regularly transported off-site by employees should be assigned a higher PII confidentiality impact level. For example, surveyors, researchers, and other field employees often need to store PII on laptops or removable media as part of their jobs. Another example is the offsite storage of backup and archive data. PII located offsite could be more vulnerable to unauthorized access or disclosure because it is more likely to be lost or stolen than PII stored within the physical boundaries of the organization.

3.3 PII Confidentiality Impact Level Examples

The following examples illustrate how an organization might assign PII confidentiality impact levels to specific instances of PII. The examples are intended to help organizations better understand the process of considering the various impact level factors, and they are not a substitute for organizations analyzing their own situations. Certain circumstances within any organization or specific system, such as the context of use or obligation to protect, may cause different outcomes.

Obligation to protect is a particularly important factor that should be determined early in the categorization process. Since obligation to protect confidentiality should always be made in consultation with an organization's legal counsel and privacy officer, it is not addressed in the following examples.

3.3.1 Example 1: Incident Response Roster

A Federal government agency maintains an electronic roster of its computer incident response team members. In the event that an IT staff member detects any kind of security breach, standard practice requires that the staff member contact the appropriate people listed on the roster. Because this team may need to coordinate closely in the event of an incident, the contact information includes names, professional titles, office and work cell phone numbers, and work email addresses. The agency makes the same types of contact information available to the public for all of its employees on its main web site.

Identifiability: The information directly identifies a small number of individuals using names, phone numbers, and email addresses.

Quantity of PII: The information directly identifies fewer than twenty individuals.

Data field sensitivity: Although the roster is intended to be made available only to the team members, the individuals' information included in the roster is already available to the public on the agency's web site.

[41] Systems containing PII that are owned and/or maintained at contractor site for a Federal agency are subject to same controls and authorization requirements as if the systems were located at a Federal agency site. See NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

Context of use: The release of the individuals' names and contact information would not likely cause harm to the individuals, and disclosure of the fact that the agency has collected or used this information is also unlikely to cause harm.

Access to and location of PII: The information is accessed by IT staff members who detect security breaches, as well as the team members themselves. The PII needs to be readily available to teleworkers and to on-call IT staff members so that incident responses can be initiated quickly.

Taking into account these factors, the agency determines that unauthorized access to the roster would likely cause little or no harm, and it chooses to assign the PII confidentiality impact level of *low*.[42]

3.3.2 Example 2: Intranet Activity Tracking

An organization maintains a web use audit log for an intranet web site accessed by employees. The web use audit log contains the following:

- The user's IP address
- The Uniform Resource Locator (URL) of the web site the user was viewing immediately before coming to this web site (i.e., referring URL)
- The date and time the user accessed the web site
- The web pages or topics accessed within the organization's web site (e.g., organization security policy).

Identifiability: By itself, the log does not contain any directly identifiable data. However, the organization has a closely-related system with a log that contains domain login information records, which include user IDs and corresponding IP addresses. Administrators who have access to both systems and their logs could correlate information between the logs and identify individuals. Potentially, information could be stored about the actions of most of the organization's users involving web access to intranet resources. The organization has a small number of administrators who have access to both systems and both logs.

Quantity of PII: The log contains a large number of records containing linked PII.

Data field sensitivity: The information on which internal web pages and topics were accessed could potentially cause some embarrassment if the pages involved certain human resources-related subjects, such as a user searching for information on substance abuse programs. However, since the logging is limited to use of intranet-housed information, the amount of potentially embarrassing information is minimal.

Context of use: Creation of the logs is known to all staff members through the organization's acceptable use policies. The release of the information would be unlikely to cause harm, other than potential embarrassment for a small number of users.

Access to and location of PII: The log is accessed by a small number of system administrators when troubleshooting operational problems and also occasionally by a small number of incident response

[42] This scenario is presented for illustrative purposes only. It is possible that this type of information could be used for a social engineering attack. Organizations may consider their particular circumstances and assign a higher impact level for this scenario.

personnel when investigating incidents. All access to the log occurs only from the organization's own systems.

Taking into account these factors, the organization determines that a breach of the log's confidentiality would likely cause little or no harm, and it chooses to assign the PII confidentiality impact level of *low*.

3.3.3 Example 3: Fraud, Waste, and Abuse Reporting Application

A database contains web form submissions by individuals claiming possible fraud, waste, or abuse of organizational resources and authority. Some of the submissions include serious allegations, such as accusing individuals of accepting bribes or not enforcing safety regulations. The submission of contact information is not prohibited, and individuals often enter their personal information in the form's narrative text field. The web site is hosted by a server that logs IP address and referring web site information.

Identifiability: By default, the database does not request PII, but a significant percentage of users choose to provide PII. The web log contains IP addresses, which could be identifiable. However, the log information is not linked or readily linkable with the database or other sources to identify specific individuals.

Quantity of PII: A recent estimate indicated that the database has approximately 50 records with PII out of nearly 1000 total records.

Data field sensitivity: The database's narrative text field contains user-supplied text and frequently includes information such as name, mailing address, email address, and phone numbers.

Context of use: Because of the nature of the submissions (i.e., reporting claims of fraud, waste, or abuse), the disclosure of individuals' identities would likely cause some of the individuals making the claims to fear retribution by management and peers. Additionally, it could negatively impact individuals about whom accusations are made. The ensuing harm could include blackmail, severe emotional distress, loss of employment, and physical harm. A breach would also undermine employee and public trust in the organization.

Access to and location of PII: The database is only accessed by a few people who investigate fraud, waste, and abuse claims. All access to the database occurs only from the organization's internal systems.

Taking into account these factors, the organization determines that a breach of the database's confidentiality would likely cause catastrophic harm to some of the individuals and chooses to assign the PII confidentiality impact level of *high*.

4. PII Confidentiality Safeguards

PII should be protected through a combination of measures, including operational safeguards, privacy-specific safeguards, and security controls. Many of these measures also correspond to several of the Fair Information Practices. Organizations should use a risk-based approach for protecting the confidentiality of PII. The PII safeguards provided in this section are complementary to other safeguards for data and may be used as one part of an organization's comprehensive approach to protecting the confidentiality of PII and implementing the Fair Information Practices.

4.1 Operational Safeguards

This section describes two types of operational safeguards for PII protection: policy and procedure creation; and education, training, and awareness. Organizations can choose whether these policy, education, and awareness activities are combined with related security controls (e.g., AT-1, AT-2) or are separated as part of a privacy program.

As agencies work to establish a variety of safeguards to protect the confidentiality of PII, they must also ensure that mechanisms are in place to make certain that individuals are held accountable for implementing these controls adequately and that the controls are functioning as intended. Accountability is also an important Fair Information Practice. In this context, agencies may already have some pre-established processes for providing oversight and accountability for the implementation of key controls, such as those related to information system assessment and authorization, Privacy Impact Assessments, and Privacy Act compliance. However, some additional oversight mechanisms or amendments to pre-existing procedures could be necessary to ensure that all measures for protecting PII are being considered and properly implemented.

4.1.1 Policy and Procedure Creation

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.[43] Some types of policies include foundational privacy principles, privacy rules of behavior, policies that implement laws and other mandates, and system-level policies. The foundational privacy principles reflect the organization's privacy objectives. Foundational privacy principles may also be used as a guide against which to develop additional policies and procedures. Privacy rules of behavior policies provide guidance on the proper handling of PII, as well as the consequences for failure to comply with the policy. Some policies provide guidance on implementing laws and OMB guidance in an organization's environment based upon the organization's authorized business purposes and mission. Organizations should consider developing privacy policies and associated procedures for the following topics:

- Access rules for PII within a system
- PII retention schedules and procedures
- PII incident response and data breach notification

[43] There are laws and OMB guidance that provide agency requirements for policy development. For example, OMB Memorandum 05-08 requires that a "senior agency official must…have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues…." Additionally, the Privacy Act requires agencies to "establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of…" the Privacy Act "including any other rules and procedures adopted…and the penalties for noncompliance." 5 U.S.C. § 552a(e)(9).

- Privacy in the system development life cycle process
- Limitation of collection, disclosure, sharing, and use of PII
- Consequences for failure to follow privacy rules of behavior.

If the organization permits access to or transfer of PII through interconnected systems external to the organization or shares PII through other means, the organization should implement the appropriate documented agreements for roles and responsibilities, restrictions on further sharing of the information, requirements for notification to each party in the case of a breach, minimum security controls, and other relevant factors. Also, Interconnection Security Agreements (ISA) should be used for technical requirements as necessary.[44] These agreements ensure that the partner organizations abide by rules for handling, disclosing, sharing, transmitting, retaining, and using the organization's PII.

PII maintained by the organization should also be reflected in the organization's incident response policies and procedures. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly. OMB M-07-16 sets out specific requirements for reporting incidents involving the loss or inappropriate disclosure of PII. For additional information, see Section 5.

4.1.2 Awareness, Training, and Education

Awareness, training, and education are distinct activities, each critical to the success of privacy and security programs.[45] Their roles related to protecting PII are briefly described below. Additional information on privacy education, training, and awareness is available in NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

Awareness efforts are designed to change behavior or reinforce desired PII practices. The purpose of awareness is to focus attention on the protection of PII. Awareness relies on using attention-grabbing techniques to reach all different types of staff across an organization. For PII protection, awareness methods include informing staff of new scams that are being used to steal identities, providing updates on privacy items in the news such as government data breaches and their effect on individuals and the organization, providing examples of how staff members have been held accountable for inappropriate actions, and providing examples of recommended privacy practices.

The goal of training is to build knowledge and skills that will enable staff to protect PII. Laws and regulations may specifically require training for staff, managers, and contractors. An organization should have a training plan and implementation approach, and an organization's leadership should communicate the seriousness of protecting PII to its staff. Organizational policy should define roles and responsibilities for training; training prerequisites for receiving access to PII; and training periodicity and refresher training requirements. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training. Depending on the roles and functions involving PII, important topics to address may include:

- The definition of PII

[44] See NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, http://csrc.nist.gov/publications/PubsSPs.html.

[45] Some organizations have chosen to combine their security and privacy awareness, education, and training, whereas other organizations have chosen to keep them separate. Additionally, the Privacy Act and OMB guidance specifically require privacy training.

- Applicable privacy laws, regulations, and policies
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognition of a security or privacy incident involving PII
- Retention schedules for PII
- Roles and responsibilities in responding to PII-related incidents and reporting.

Education develops a common body of knowledge that reflects all of the various specialties and aspects of PII protection. It is used to develop privacy professionals who are able to implement privacy programs that enable their organizations to proactively respond to privacy challenges.

4.2 Privacy-Specific Safeguards[46]

Privacy-specific safeguards are controls for protecting the confidentiality of PII. These controls provide types of protections not usually needed for other types of data. Privacy-specific safeguards help organizations collect, maintain, use, and disseminate data in ways that protect the confidentiality of the data.

4.2.1 Minimizing the Use, Collection, and Retention of PII

The practice of minimizing the use, collection, and retention of PII is a basic privacy principle.[47] By limiting PII collections to the least amount necessary to conduct its mission, the organization may limit potential negative consequences in the event of a data breach involving PII. Organizations should consider the total amount of PII used, collected, and maintained, as well as the types and categories of PII used, collected, and maintained. This general concept is often abbreviated as the “minimum necessary” principle. PII collections should only be made where such collections are essential to meet the authorized business purpose and mission of the organization. If the PII serves no current business purpose, then the PII should no longer be used or collected.

Also, an organization should regularly review[48] its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization’s business purpose and mission.[49] If PII is no longer relevant and necessary, then PII should be properly destroyed. The destruction or disposal of PII must be conducted in accordance with any litigation holds and the Federal Records Act and records control schedules approved by the National Archives and Records Administration (NARA).[50] Organizations should also ensure that retired hardware has been properly

[46] Portions of this section were submitted as contributions to the ISO/IEC 29100 *Privacy Framework* draft standard.

[47] Fair Information Practices are also referred to as privacy principles. See Appendix D for additional information.

[48] The frequency of reviews should be done in accordance with laws, regulations, mandates, and organizational policies that apply to the collection of PII.

[49] The Privacy Act requires that Federal agencies only maintain records relevant and necessary to their mission. 5 U.S.C. § 552a(e)(1). Also, OMB directed Federal agencies to review their PII holdings annually and to reduce their holdings to the minimum necessary for proper performance of their missions. OMB M-07-16.

[50] The Federal Records Act, 44 U.S.C. § 3301, defines records as “[a]ll books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or

sanitized before disposal (e.g., no disk images contain PII, the hard drive has been properly sanitized).[51] The effective management and prompt disposal of PII, in accordance with NARA-approved disposition schedules, will minimize the risk of unauthorized disclosure.

4.2.2 Conducting Privacy Impact Assessments

PIAs are structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system. According to OMB, PIAs are "structured reviews of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form[52] in an electronic information system, and (iii) to identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."[53] If used effectively, a PIA should address confidentiality risks at every stage of the system development life cycle (SDLC). Many organizations have established their own templates that provide the basis for conducting a PIA. The following are some topics that are commonly addressed through the use of a PIA:

- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- How the information will be secured
- What choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

4.2.3 De-Identifying Information

Full data records are not always necessary, such as for some forms of research, resource planning, and examinations of correlations and trends. The term *de-identified information* is used to describe records that have had enough PII removed or *obscured*, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.[54] De-identified information can be re-identified

appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them." Agencies are required to create and maintain "adequate and proper documentation" of their organization, mission, functions, etc., and may not dispose of records without the approval of the Archivist of the United States. This approval is granted through the General Records Schedules (GRS) and agency specific records schedules.

[51] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[52] See Appendix C for additional information about information in identifiable form (IIF).

[53] OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* http://www.whitehouse.gov/omb/memoranda/m03-22.html. For additional PIA information specific to Federal agencies, see Appendix B.

[54] For the purpose of analysis, the definition for de-identified information used in this document is loosely based on the requirements for de-identified data defined in the HIPAA Privacy Rule, and it is generalized to apply to all PII. This definition differs from the HIPAA definition in that it is applied to all PII and does not specifically require the removal of all 18 data elements described by the HIPAA Privacy Rule. The HIPAA Privacy Rule recognizes two ways to de-identify data such that it is no longer considered to be protected health information (PHI). First, 18 specific fields can be removed, such as name, SSN, and phone number. Second, a person with appropriate knowledge and experience in statistical methods

(rendered distinguishable) by using a code, algorithm, or pseudonym that is assigned to individual records. The code, algorithm, or pseudonym should not be derived from other related information[55] about the individual, and the means of re-identification should only be known by authorized parties and not disclosed to anyone without the authority to re-identify records. A common de-identification technique for obscuring PII is to use a one-way cryptographic function, also known as a hash function, on the PII.[56] De-identified information can be assigned a PII confidentiality impact level of *low*, as long as the following are both true:

- The re-identification algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access to the re-identification information.
- The data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data.

For example, de-identification could be accomplished by removing account numbers, names, SSNs, and any other identifiable information from a set of financial records. By de-identifying the information, a trend analysis team could perform an unbiased review on those records in the system without compromising the PII or providing the team with the ability to identify any individual. Another example is using health care test results in research analysis. All of the identifying PII fields can be removed, and the patient ID numbers can be obscured using pseudo-random data that is associated with a cross-reference table located in a separate system. The only means to reconstruct the original (complete) PII records is through authorized access to the cross-reference table.

Additionally, de-identified information can be aggregated for the purposes of statistical analysis, such as making comparisons, analyzing trends, or identifying patterns. An example is the aggregation and use of multiple sets of de-identified data for evaluating several types of education loan programs. The data describes characteristics of loan holders, such as age, gender, region, and outstanding loan balances. With this dataset, an analyst could draw statistics showing that 18,000 women in the 30-35 age group have outstanding loan balances greater than $10,000. Although the original dataset contained distinguishable identities for each person, the de-identified and aggregated dataset would not contain linked or readily identifiable data for any individual.

4.2.4 Anonymizing Information

Anonymized information[57] is defined as previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.[58] Anonymizing information

applies de-identification methods, determines the risk is very small, and documents the justification. 45 C.F.R. § 164.514, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

[55] This is not intended to exclude the application of cryptographic hash functions to the information.

[56] Hashing may not be appropriate for de-identifying information covered by HIPAA. 45 C.F.R. § 164.514 (c)(1) specifically excludes de-identification techniques where the code is derived from the PII itself. Organizations should consult their legal counsel for legal requirements related to de-identification and anonymization.

[57] For additional information about anonymity, see: A. Pfitzmann and M. Hansen, *A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, updated 2009, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.32.pdf.

[58] Based on the Common Rule, which governs confidentiality requirements for research, 15 C.F.R. Part 27. Some organizations do not distinguish between the terms de-identified and anonymized information and use them interchangeably. Additionally, the amount of information available publicly and advances in computational technology make full anonymity of released datasets (e.g., census data and public health data) difficult to accomplish. For additional information, see: American Statistical Association, *Data Access and Personal Privacy: Appropriate Methods of Disclosure Control*, December 6, 2008, http://www.amstat.org/news/statementondataaccess.cfm.

usually involves the application of statistical disclosure limitation techniques[59] to ensure the data cannot be re-identified, such as: [60]

- **Generalizing the Data**—Making information less precise, such as grouping continuous values
- **Suppressing the Data—**Deleting an entire record or certain parts of records
- **Introducing Noise into the Data—**Adding small amounts of variation into selected data
- **Swapping the Data—**Exchanging certain data fields of one record with the same data fields of another similar record (e.g., swapping the ZIP codes of two records)
- **Replacing Data with the Average Value—**Replacing a selected value of data with the average value for the entire group of data.

Using these techniques, the information is no longer PII, but it can retain its useful and realistic properties.[61]

Anonymized information is useful for system testing.[62] Systems that are newly developed, newly purchased, or upgraded require testing before being introduced to their intended production (or live) environment. Testing generally should simulate real conditions as closely as possible to ensure the new or upgraded system runs correctly and handles the projected system capacity effectively. If PII is used in the test environment, it is required to be protected at the same level that it is protected in the production environment, which can add significantly to the time and expense of testing the system.

Randomly generating fake data in place of PII to test systems is often ineffective because certain properties and statistical distributions of PII may need to be retained to effectively test the system. There are tools available that substitute PII with synthetic data generated by anonymizing PII. The anonymized information retains the useful properties of the original PII, but the anonymized information is not considered to be PII. Anonymized data substitution is a privacy-specific protection measure that enables system testing while reducing the expense and added time of protecting PII. However, not all data can be readily anonymized (e.g., biometric data).

4.3 Security Controls

In addition to the PII-specific safeguards described earlier in this section, many types of security controls are available to safeguard the confidentiality of PII. Providing reasonable security safeguards is also a Fair Information Practice. Security controls are often already implemented on a system to protect other types of data processed, stored, or transmitted by the system. The security controls listed in NIST SP 800-53 address general protections of data and systems. The items listed below are some of the NIST SP 800-53 controls that can be used to help safeguard the confidentiality of PII. Note that some of these

[59] Both anonymizing and de-identifying should be conducted by someone with appropriate training. It may be helpful, as appropriate, to consult with a statistician to assess the level of risk with respect to possible unintended re-identification and improper disclosure. For additional information on statistical disclosure limitation techniques, see OMB's Statistical Policy Working Paper #22, http://www.fcsm.gov/working-papers/spwp22.html. See also Census Bureau, *Report on Confidentiality* and Privacy 1790-2002, http://www.census.gov/prod/2003pubs/conmono2.pdf.

[60] The Federal Committee on Statistical Methodology provides a checklist to assist in the assessment of risk for re-identification and improper disclosure. For additional information, see the Federal Committee on Statistical Methodology: Confidentiality and Data Access Committee, *Checklist on Disclosure Potential of Data Releases*, http://www.fcsm.gov/committees/cdac/.

[61] The retention of useful properties in anonymized data is dependent upon the statistical disclosure limitation technique applied.

[62] Anonymization is also commonly used by agencies to release datasets to the public for research purposes.

controls may not be in the recommended set of security controls for the baselines identified in NIST SP 800-53 (e.g., a control might only be recommended for high-impact systems). However, organizations may choose to provide greater protections than what is recommended; see Section 3.2 for a discussion of factors to consider when choosing the appropriate controls. In addition to the controls listed below, NIST SP 800-53 contains many other controls that can be used to help protect PII, such as incident response controls.

- **Access Enforcement (AC-3).** Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). This can be done in many ways. One example is implementing role-based access control and configuring it so that each user can access only the pieces of data necessary for the user's role. Another example is only permitting users to access PII through an application that tightly restricts their access to the PII, instead of permitting users to directly access the databases or files containing PII.[63] Encrypting stored information is also an option for implementing access enforcement.[64] OMB M-07-16 specifies that Federal agencies must "encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing".

- **Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.

- **Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Concerning PII, the organization can ensure that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- **Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII. If remote access is permitted, the organization should ensure that the communications are encrypted.

- **User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.

- **Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities). Some organizations may choose to restrict remote access involving higher-impact instances of PII so that the information will not leave the organization's physical boundaries. If access is permitted, the organization can ensure that the devices are properly secured and regularly scan the devices to verify their security status (e.g., anti-malware software enabled and up-to-date, operating system fully patched).

- **Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.

[63] For example, suppose that an organization has a database containing thousands of records on employees' benefits. Instead of allowing a user to have full and direct access to the database, which could allow the user to save extracts of the database records to the user's computer, removable media, or other locations, the organization could permit the user to access only the necessary records and record fields. A user could be restricted to accessing only general demographic information and not any information related to the employees' identities.

[64] Additional encryption guidelines and references can be found in FIPS 140-2: *Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/PubsFIPS.html.

- **Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

- **Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.[65] The strength requirement for the authentication mechanism depends on the impact level of the PII and the system as a whole. OMB M-07-16 specifies that Federal agencies must "allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access," and also must "use a 'time-out' function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity."

- **Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.

- **Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled. The organization could exempt specific types of media or output from labeling so long as it remains within a secure environment. Examples of labeling are cover sheets on printouts and paper labels on digital media.

- **Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. One example is the use of storage encryption technologies to protect PII stored on removable media.

- **Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas. Examples of protective safeguards are encrypting stored information and locking the media in a container.

- **Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.[66] An example is degaussing a hard drive—applying a magnetic field to the drive to render it unusable.

- **Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.[67]

- **Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.

- **Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. An example is the use of data loss prevention technologies.

[65] For additional information about authentication, see NIST SP 800-63, *Electronic Authentication Guideline*.

[66] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*.

[67] NIST has several publications on this topic that are available from http://csrc.nist.gov/publications/PubsSPs.html.

5. Incident Response for Breaches Involving PII

Handling incidents and breaches involving PII is different from regular incident handling and may require additional actions by an organization.[68] Breaches involving PII can receive considerable media attention, which can greatly harm an organization's reputation and reduce the public's trust[69] in the organization. Moreover, affected individuals can be subject to embarrassment, identity theft, or blackmail as the result of a breach involving PII. Due to these particular risks of harm, organizations should develop additional policies, such as determining when and how individuals should be notified, when and if a breach should be reported publicly, and whether to provide remedial services, such as credit monitoring, to affected individuals. Organizations should integrate these additional policies into their existing incident handling response policies.[70]

Management of incidents involving PII often requires close coordination among personnel from across the organization, such as the CIO, CPO, system owner, data owner, legal counsel, and public relations officer. Because of this need for close coordination, organizations should establish clear roles and responsibilities to ensure effective management when an incident occurs.

FISMA requires Federal agencies to have procedures for handling information security incidents, and it directed OMB to ensure the establishment of a central Federal information security incident center, which is the U.S. Computer Emergency Readiness Team (US-CERT). Additionally, NIST provided guidance on security incident handling in NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*. In 2007, OMB issued M-07-16, which provided specific guidance to Federal agencies for handling incidents involving PII.[71]

Incident response plans should be modified to handle breaches involving PII. Incident response plans should also address how to minimize the amount of PII necessary to adequately report and respond to a breach. NIST SP 800-61 Revision 1 describes four phases of handling security incidents. Specific policies and procedures for handling breaches involving PII can be added to each of the following phases identified in NIST SP 800-61: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. This section provides additional details on PII-specific considerations for each of these four phases.

5.1 Preparation

Preparation requires the most effort because it sets the stage to ensure the breach is handled appropriately. Organizations should build their response plans for breaches involving PII into their existing incident response plans. The development of response plans for breaches involving PII requires organizations to make many decisions about how to handle breaches involving PII, and the decisions should be used to develop policies and procedures. The policies and procedures should be communicated to the organization's entire staff through training and awareness programs. Training may include tabletop

[68] For the purposes of this document, incident and breach are used interchangeably to mean any violation or imminent threat of violation of privacy or computer security policies, acceptable use policies, privacy rules of behavior, or standard computer security practices. Modified from NIST SP 800-61 Revision 1.

[69] According to a 2007 Government Privacy Trust Survey conducted by the Ponemon Institute, a Federal department fell from being a top five most trusted agency in 2006 to just above the bottom five least trusted agencies after the highly publicized breach of millions of PII records in 2006. http://www.govexec.com/dailyfed/0207/022007tdpm1.htm.

[70] Some organizations choose to have separate policies and procedures for incidents and breaches of PII, which may involve the use of a separate privacy incident response team. If the policies and procedures are separate for incidents and breaches involving PII, then the security incident response plan should be amended so that staff members know when to follow the separate policies and procedures for incidents and breaches involving PII.

[71] Organizations may also want to review *Combating ID Theft: A Strategic Plan* from the President's Task Force on Identity Theft, April 2007, at: http://www.idtheft.gov/.

exercises to simulate an incident and test whether the response plan is effective and whether the staff members understand and are able to perform their roles effectively. Training programs should also inform employees of the consequences of their actions for inappropriate use and handling of PII.

The organization should determine if existing processes are adequate, and if not, establish a new incident reporting method for employees to report suspected or known incidents involving PII. The method could be a phone hotline, email, online form, or a management reporting structure in which employees know to contact a specific person within the management chain. Employees should be able to report any breach involving PII immediately on any day, at any time. Additionally, employees should be provided with a clear definition of what constitutes a breach involving PII and what information needs to be reported. The following information is helpful to obtain from employees who are reporting a known or suspected breach involving PII.[72]

- Person reporting the incident
- Person who discovered the incident
- Date and time the incident was discovered
- Nature of the incident
- Name of system and possible interconnectivity with other systems
- Description of the information lost or compromised
- Storage medium from which information was lost or compromised
- Controls in place to prevent unauthorized use of the lost or compromised information
- Number of individuals potentially affected
- Whether law enforcement was contacted.

Federal agencies are required to report all known or suspected breaches involving PII, in any format, to US-CERT within one hour.[73] To meet this obligation, organizations should proactively plan their breach notification response. A breach involving PII may require notification to persons external to the organization, such as law enforcement, financial institutions, affected individuals, the media, and the public.[74] Organizations should plan in advance how, when, and to whom notifications should be made. Organizations should conduct training sessions on interacting with the media regarding incidents. Additionally, OMB M-07-16 requires federal agencies to include the following elements in their plans for handling breach notification:

- Whether breach notification to affected individuals is required[75]
- Timeliness of the notification
- Source of the notification
- Contents of the notification

[72] U.S. Department of Commerce, *Breach Notification Response Plan*, September 28, 2007

[73] In M-07-16, OMB required Federal agencies to report all known or suspected PII breaches to US-CERT within one hour. This document does not change or affect any US-CERT reporting requirements as required by OMB, other NIST guidance, US-CERT, or statute.

[74] For additional information about communications with external parties, such as the media, see NIST SP 800-61 Revision 1.

[75] For Federal agencies, notification to US-CERT is always required.

- Means of providing the notification
- Who receives the notification; public outreach response
- What actions were taken and by whom

Additionally, organizations should establish a committee or person responsible for using the breach notification policy to coordinate the organization's response. Organizations also need to determine how incidents involving PII will be tracked within the organization.

The organization should also determine what circumstances require the organization to provide remedial assistance to affected individuals, such as credit monitoring services. The PII confidentiality impact level should be considered for this determination because it provides an analysis of the likelihood of harm for the loss of confidentiality for each instance of PII.

5.2 Detection and Analysis

Organizations may continue to use their current detection and analysis technologies and techniques for handling incidents involving PII. However, adjustments to incident handling processes may be necessary, such as ensuring that the analysis process includes an evaluation of whether an incident involves PII. Detection and analysis should focus on both known and suspected breaches involving PII. Detection of an incident involving PII also requires reporting internally, to US-CERT, and externally, as appropriate.

5.3 Containment, Eradication, and Recovery

Existing technologies and techniques for containment, eradication, and recovery may be used for breaches involving PII. However, changes to incident handling processes may be necessary, such as performing additional media sanitization steps when PII needs to be deleted from media during recovery. [76] PII should not be sanitized until a determination has been made about whether the PII must be preserved as evidence.[77] Particular attention should be paid to using proper forensics techniques[78] to ensure preservation of evidence. Additionally, it is important to determine whether PII was accessed and how many records or individuals were affected.

5.4 Post-Incident Activity

As with other security incidents, information learned through detection, analysis, containment, and recovery should be collected for sharing within the organization and with the US-CERT to help protect against future incidents. The incident response plan should be continually updated and improved based on the lessons learned during each incident. Lessons learned might also indicate the need for additional training, security controls, or procedures to protect against future incidents.

Additionally, the organization should use its response policy, developed during the planning phase, to determine whether the organization should provide affected individuals with remedial assistance. When providing notice to individuals, organizations should make affected individuals aware of their options,

[76] For additional information on media sanitization, see NIST SP 800-88.

[77] Often, information involved with an incident will need to be preserved in preparation for prosecution or litigation related to the incident. Legal counsel should be consulted before any PII is sanitized.

[78] For additional information, see NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

such as obtaining a free copy of their credit report, obtaining a freeze credit report, placing a fraud alert on their credit report, or contacting their financial institutions.[79]

[79] Organizations may need to provide other types of remedial assistance for breaches that would cause harm unrelated to identity theft and financial crimes, such as PII maintained for law enforcement, medical care, or homeland security.