Privacy Overlays

1. Identification

This document is comprised of four Privacy Overlays that identify security and privacy control specifications required to protect personally identifiable information (PII), including protected health information (PHI), in National Security Systems (NSS) and reduce privacy risks to individuals throughout the information lifecycle.[1] The Privacy Overlays support implementation of but are not intended to, and do not, supersede privacy requirements of statute, regulation, or Office of Management and Budget (OMB) policy.

Since the Privacy Act of 1974 established the requirement for "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" and "to protect… the integrity" of systems, both the technology and threats thereto have evolved and organizations have had to change the way they protect their information.[2] The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, and Committee on National Security Systems Instruction (CNSSI) 1253 provide the underlying controls necessary to protect national security systems (NSS). Based on the Fair Information Practice Principles (FIPPs)[3] and federal privacy requirements, these Privacy Overlays provide a consistent approach for organizations to implement "appropriate administrative, technical, and physical safeguards" to protect PII in information systems irrespective of whether the organization maintains the PII as part of a system of records.[4] The Privacy Overlays provide a method within existing NIST and CNSS structures to implement the security and privacy controls necessary to protect PII in today's technology-dependent world.

All PII is not equally sensitive and therefore all PII does not require equal protection. PII with higher sensitivity requires more stringent protections, while PII with lower sensitivity requires less stringent protections. There are three overlays that address the varying sensitivity of PII; Low, Moderate, and High. PHI is a subset of PII and in addition to sensitivity considerations, PHI requires a minimum set of protections that are based on the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules. Therefore, PHI is addressed under a fourth overlay, which is applied on top of the Privacy Overlay determined by the sensitivity of the PHI, i.e., Low, Moderate, or High.

---

[1] For additional information about PII and PHI, see Section 7, "Definitions."

[2] "Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any unanticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. §552a(e)(10).

[3] Committee Report No. 93-1183 to accompany S. 3418 (Sep 26, 1974), p 9.

[4] "[A system of records is] a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. §552a(a)(5).

The Privacy Overlays are based on the following laws, policies, and standards:

- The Privacy Act of 1974, as amended, (P.L. 93-579), 5 U.S.C. §552a
- The Freedom of Information Act (FOIA), as amended, 5 U.S.C. §552
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191)
- E-Government Act [includes Federal Information Security Management Act] (P.L. 107-347), December 2002
- Federal Information Security Management Act (P.L. 107-347, Title III), December 2002
- Paperwork Reduction Act (P.L. 104-13), May 1995, as amended (44 U.S.C. §3501, et seq)
- The Clinger-Cohen Act of 1996 (Pub. L. No. 104-106)
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. No. 108-458)
- Federal Agency Data Mining Reporting Act of 2007 *(*P.L. 109-177)
- Federal Records Act (P.L. 90–620), as amended, (44 U.S.C. §3301)
- Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106, *Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106)
- Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, April 2010
- Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Security Control Selection for National Security Systems,* March 2014
- OMB Circular A-130*,* Transmittal Memorandum #4*, Management of Federal Information Resources,* November 2000
- Office of Management and Budget Memorandum 99-18, *Privacy Policies on Federal Web Sites*, June 1999
- Office of Management and Budget Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003
- Office of Management and Budget Memorandum 04-04, *E-Authentication Guidance*, December 2003
- Office of Management and Budget Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*, February 2005
- Office of Management and Budget Memorandum 06-15, *Safeguarding Personally Identifiable Information*, May 2006.
- Office of Management and Budget Memorandum 06-16, *Protection of Sensitive Agency Information*, June 2006
- Office of Management and Budget Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security and Agency Information Technology Investments*, July 2006
- Office of Management and Budget Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007
- Office of Management and Budget Memorandum 08-09, *New FISMA Privacy Reporting Requirements for FY 2008*, January 2008

- Office of Management and Budget Memorandum 10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 2010
- Office of Management and Budget Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 2010
- Office of Management and Budget Memorandum 11-02, *Sharing Data While Protecting Privacy*, November 2010
- Office of Management and Budget Memorandum 11-27, *Implementing the Telework Enhancement Act of 2010: Security Guidelines*, July 2011
- Office of Management and Budget Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013
- *Federal Agency Responsibilities* (44 U.S.C. §3506)
- *National Security System* (40 U.S.C. §11103)
- The HIPAA Privacy, Security, and Breach Rules, at 45 C.F.R. Parts 160 and 164 (2013)
- *Federal Acquisition Regulation (FAR)*, Parts 24, 39, and 52 (48 C.F.R. Parts 24, 39, and 52)
- Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004
- National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
- National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, February 2010
- National Institute of Standards and Technology Special Publication SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (Includes Updates as of 15 January 2014)
- National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security,* July 2008
- National Institute of Standards and Technology Special Publication 800-57, *Recommendation for Key Management* (Parts 13), 23 January 2015
- National Institute of Standards and Technology Special Publication 800-60, Volume II, Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
- National Institute of Standards and Technology Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization*, December 2014
- National Institute of Standards and Technology Special Publication 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 2007
- National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008

- National Institute of Standards and Technology Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013
- National Institute of Standards and Technology Special Publication 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, February 2013
- Information Sharing Environment Privacy Guidelines, ise.gov, (December 2006)
- Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment, Version 1.0, ise.gov, (September 2007)
- Intelligence Community Standard (ICS) 502-01, *Intelligence Community Computer Incident Response and Computer Network Defense*, (December 2013)
- Intelligence Community Standard 500-27, *Collection and Sharing of Audit Data* (June 2011)
- Intelligence Community Standard 700-2, *Use of Audit Data for Insider Threat Detection* (June 2011)
- Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, (March 2012)

The Privacy Overlays should be evaluated for revision if subsequent laws or guidance modifies the methodology for evaluating the sensitivity of PII or requirements for security and privacy controls related to PII, including PHI.

2. Overlay Characteristics

NIST has noted that the "[t]reatment 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."[5] Privacy and security controls selected to protect PII in information systems are distinct from the security controls selected to enforce security classifications. Security classifications focus on protecting national security interests, while selection of privacy and security controls focus on protecting individuals and organizations from potential harms specific to privacy risks. To accomplish these distinct objectives, the Privacy Overlays provide four baseline-independent overlays to support compliance with federal privacy requirements. The Privacy Overlays assist privacy officers, information system security officers, system owners, program managers, developers, and those who maintain information systems by identifying the security and privacy control specifications that implement the privacy requirements of federal statutes, regulations, policies, and standards. Security and privacy professionals often have differing backgrounds and levels of understanding for each other's requirements and activities. The Privacy Overlays include information to help the privacy and security communities understand each other and to collaborate to protect PII.

It is critical that information technology (IT) security and privacy offices work together early and throughout the System Development Life Cycle (SDLC) and the Risk Management Framework (RMF), and when conducting the analysis of ***PII confidentiality impact level***[6] necessary to identify the applicable Privacy Overlays. This interdisciplinary collaboration is necessary to

[5] NIST SP 800-122, Section 2.3, "PII and Fair Information Practices," pp. 2-3.
[6] See Section 2.5 under "Categorization of PII Using NIST SP 800-122."

ensure privacy requirements and risks are addressed both early in the SDLC and RMF processes and whenever a system or system requirement changes.[7] Coordination early in the process benefits the organization by minimizing the need to retrofit privacy protections into information systems, decreasing the likelihood of privacy breaches and mishandling of PII, and reducing the potential for litigation against the organization.

2.1 Selecting Privacy Overlays

One or more of the Privacy Overlays may apply, depending on the type of PII maintained. All PII must be evaluated to determine whether the low, moderate, or high Privacy Overlay applies. In addition, PHI must also be protected by applying the PHI Privacy Overlay.

2.1.1 Low, Moderate, and High Privacy Overlays

The analysis described in Section 3 identifies the value of the PII confidentiality impact level which selects the low, moderate, or high privacy overlay. The low, moderate, and high columns of Table 3 identify the security and privacy control specifications applicable to the system based on the identified value of the PII confidentiality impact level (low, moderate, or high).

2.1.2 PHI Privacy Overlay

PHI is a subset of PII that has its own specific statutory and regulatory requirements. Therefore, in addition to the low, moderate, or high Privacy Overlay identified in section 2.1.1, organizations with PHI must apply the PHI Privacy Overlay. The PHI column of Table 3 identifies the PHI Privacy Overlay establishing the minimum requirements concerning PHI. Organizations must follow the guidance in section 2.3.2 in applying the PHI Privacy Overlay.

2.2 The PII Confidentiality Impact Level

The low, moderate, and high Privacy Overlays use the NIST SP 800-122 concept of ***PII confidentiality impact level*** to select which of the low, moderate, or high Privacy Overlays to apply. NIST SP 800-122 notes the importance of the security objectives of confidentiality, integrity, and availability. While NIST points out that the ***PII confidentiality impact level*** refers to the confidentiality security objective,[8] it advises organizations to consider integrity and availability requirements for PII when applicable.[9] Therefore, the low, moderate, and high Privacy Overlays considered all three security objectives (confidentiality, integrity, availability) as well as privacy objectives historically embodied in the FIPPs to identify control specifications. The low, moderate, and high Privacy Overlays should be viewed to encompass all three security objectives with regard to PII. Organizations should follow the RMF guidance for determining

[7] See, for example, 5 U.S.C. §552a(e)(10), "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."
[8] See NIST SP 800-122, Footnote 31.
[9] See NIST SP 800-122, Section 3, page 3-1.

the integrity and availability impact values as they do for other information types. Note that although the PII confidentiality impact ***level*** sounds similar, it is different from, and does not equate to, the impact ***values***[10] for the security objectives of confidentiality, integrity, and availability *for the system overall*, which are used to determine the security control baselines in CNSSI No. 1253.

The PII confidentiality impact level is not the same, and should not be confused with, the security objective of confidentiality for the system.

See Annex, "Relationship Between the Privacy Overlay and the Risk Management Framework." The PII confidentiality impact level should be used in determining the confidentiality impact value for the PII information type[11] when categorizing systems under CNSSI No. 1253. Section 3 of the Privacy Overlays provides the steps necessary to determine the PII confidentiality impact level.

2.3. Approach to PII in the Privacy Overlays

The OMB encourages agencies to use a Best Judgment Standard and follow a two-step approach regarding an organization's information about individuals: (i) consider whether the information is within scope of the definition of PII, and (ii) consider the sensitivity of the PII in the context in which it appears. The sub-sections below facilitate an organization's completion of the first step of OMB's approach by identifying PII and PHI.[12] Implementation of the second step of OMB's approach is discussed below under "Categorization of PII Using NIST SP 800-122."

2.3.1 PII

OMB memoranda collectively define PII as (i) data elements which alone can distinguish or trace an individual's identity, i.e., unique identifiers; (ii) non-PII that becomes PII when it identifies an individual in aggregate, i.e., compilation effect; and (iii) non-PII that becomes PII when combined with a unique identifier or data elements that have aggregated to become PII,

[10] NIST SP 800-53, Rev. 4, (defines "impact value" as "[t]he assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.")
[11] See FIPS 199. Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.
[12] To protect PII within an information system, system owners must be able to locate and identify the PII and should recognize that inclusion of PII in a system may not be immediately apparent. System owners should be familiar with all aspects of an information system. Examples of where PII may be identified for a system include the data dictionary, the architecture for the data store(s), or the data store(s) themselves. For existing systems, current privacy documentation, such as Privacy Impact Assessments (PIAs) and system of records notices (SORNs), may provide insight into the types of PII in a system, but they may be documented at a higher level of categories or types than is necessary for the categorization of system information and determining privacy risk for the purposes of implementing the Privacy Overlays.

i.e., by association.[13] Data elements which meet one or more of these criteria are PII and should be protected.

(i) Data elements which alone can distinguish or trace an individual's identity

Many types of data elements can uniquely identify an individual without the need to first combine it with other data elements. This category of PII is most commonly encountered when a unique number or other identifier is assigned to an individual (e.g., name,[14] Social Security Number, passport number, or driver's license number) or with respect to unique identifiers that are part of an individual's physical person (e.g., biometrics, such as fingerprints, iris, voice prints, or facial images). These unique identifiers alone can be used to identify a specific individual.

(ii) Non-PII becomes PII when it is combined with other information to identify an individual

Akin to the compilation effect, data elements which alone do not identify an individual and are not PII can become PII if, when combined, they uniquely identify an individual.[15] For example, a zip code, birthdate, or gender alone will not identify someone. However, if these three elements are associated with each other they narrow the scope of reference and enable either identification or re-identification of the individual, thereby making these elements PII.

Accordingly, prevention against re-identification[16] under the compilation effect extends beyond the mere removal of name and social security number. To ensure that information does not compile to become PII, refer to one of the accepted methods of data de-identification such as those prescribed by HIPAA.[17] In the event non-PII compiles into PII, the information system will require re-examination and possible

---

[13] See, for example, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, (22 May 2007); OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, (25 June 2010); OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, (25 June 2010).

[14] An individual's name alone falls within the definition of PII provided by OMB M-07-16. This is true whether a particular name is unique, such as Glenn Schlarman, or if the name is relatively common, such as John Smith, and additional PII is necessary to successfully distinguish one individual from another. Whether information falls within the definition of PII is a separate evaluation than the sensitivity of that information.

[15] OMB M-10-23, clarifies the definition of PII in the *Definitions* section. ("The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an organization to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.")

[16] *Re-identification* refers to the use of a combination of data in a record that has been previously anonymized by the removal of PII to re-establish the identity of the individual.

[17] See Department of Health and Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, available online at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html (accessed 28 March 2015).

adjustment to the PII confidentiality impact level for that system, possibly invoking use of the Privacy Overlays and other applicable privacy requirements.

(iii) Non-PII becomes PII when combined with a unique identifier or when combined with data elements that have aggregated to become PII

When information that is not otherwise attributed to one individual is associated with PII, then the non-attributable information becomes PII by association. For example, information contained in a financial record of an unidentified individual is not PII, e.g., purchasing history without any other identifying information. However, if the financial record subsequently is linked or linkable to a name or other unique identifier for a particular individual, e.g., credit card number or account number, then the entire financial record becomes PII, i.e., the buying habits of an individual.

2.3.2 PHI

PHI is a specific subset of PII that is defined by HIPAA. It is important to note that HIPAA and the guidance in the PHI Privacy Overlay only apply to covered entities[18] and business associates.[19] For clarification and discussion of the scope and applicability of HIPAA and the PHI Privacy Overlay, see definition of PHI in Section 7. The Privacy Overlays distinguish between PII and PHI to clearly document the supplemental guidance, control extensions, and regulatory and statutory references that apply specifically to PHI (i.e., the HIPAA Privacy, Security, and Breach Rules). [20]

The PHI Privacy Overlay identifies minimum security and privacy control requirements designed to meet HIPAA Security Rule requirements, as well as the HIPAA Privacy and Breach Rule requirements, where appropriate. Covered entities and business associates must conduct a risk analysis to determine which controls are reasonable and appropriate for their environment and business practices, to include consideration of the probability and criticality of potential risks to PHI.[21]

The concept of "addressable controls" (referred to as "addressable implementation specifications" in the HIPAA Security Rule) provides covered entities additional flexibility with respect to compliance with the HIPAA Security Rule standards. With respect to controls that are identified as "addressable" in the PHI Privacy Overlay, a covered entity or business associate must do one of the following: (i) implement the addressable control; (ii) implement one or more alternative security measures to accomplish the same purpose; or (iii) not implement either an

[18] 45 C.F.R. §160.103 (defining *covered entities* as health plans, health care clearing houses, and health care providers that electronically transmit PHI in connection with any transactions set forth in the regulations).
[19] 45 C.F.R. §160.103 (defining *business associates* as people or entities that perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provide services to, a covered entity).
[20] 45 C.F.R. Parts 160 and 164.
[21] See Department of Health and Human Services, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*, available online at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf (accessed 28 March 2015). See also 45 C.F.R. §164.308(a)(1)(ii)(A).

addressable control or an alternative. The covered entity or business associate must decide whether a given addressable control is a reasonable and appropriate security measure to apply within its particular security framework. For example, a covered entity or business associate must implement an addressable control if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable control is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, security measures already in place, and the cost of implementation. The decisions that a covered entity or business associate makes regarding addressable controls must be documented in writing. The written documentation of the organization's risks decisions, as required by HIPAA, should include the factors considered as well as the results of the risk assessment on which the decision was based. Before tailoring these "addressable" controls, the organization should consult with the office or individual responsible for HIPAA compliance within their organization. For more information about tailoring, see "Tailoring Considerations" in Section 6 of this document.

2.4 Exception of Business Rolodex Information

OMB M-07-16, Footnote 6, establishes the flexibility for an organization to determine the sensitivity of its PII in context using a best judgment standard. The example provided in footnote 6 addresses an office rolodex and recognizes the low sensitivity of business contact information used in the limited context of contacting an individual through the normal course of a business interaction. The Privacy Overlays refers to this example from OMB M-07-16, Footnote 6, as the "Rolodex Exception." PII meeting the "Rolodex Exception" typically presents a very low risk to privacy for the individual or the organization and will not trigger implementation of the low, moderate, or high Privacy Overlays for a system containing only this type of information. Consistent with NIST and CNSS tailoring guidance, the "Rolodex Exception" is a scoping decision that, when applicable, helps organizations avoid unnecessary expenditures of resources based on a risk determination for this limited subset of PII.

For the purposes of implementing the low, moderate, and high Privacy Overlays, PII that may be included in this "Rolodex Exception" is limited to the following business contact information:

- Name (full or partial)
- Business street address
- Business phone numbers, including fax
- Business e-mail addresses
- Business organization

An example of an information system which may meet the parameters of the Rolodex Exception include office rosters that contain only business contact information.

Before choosing to apply the Rolodex Exception, an organization must consider the sensitivity of the PII based on the complete context in which it appears. Business contact information alone can be sensitive under certain circumstances, such as in association with a tax return or on a list of individuals under investigation for fraud, waste, and abuse. Consider, also, whether the contact information includes a blend of business and personal information (e.g., a business phone

number may be a personal device, or a business address may be a residential address of a home office). If, after exploring contextual considerations, the organization determines that a system's use of the business contact information is limited to business contact purposes, then the organization may apply the Rolodex Exception.

This analysis must include an evaluation of related operational security issues, which are distinct from privacy considerations and may require additional protective measures. Application of this Rolodex Exception is limited to the Privacy Overlays and does not affect applicability of any other statute, regulation, or standard which may require consideration and protection of this type of information in other contexts. For example, consider business contact information which both meets the terms of the Rolodex Exception and appears in a context that has increased classification or operational security sensitivities; the Rolodex Exception may obviate the organization from implementing the Privacy Overlays, but the organization must still meet requirements that are applicable to protect classified information and resolve operational security concerns.

2.5 Categorization of PII Using NIST SP 800-122

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, provides guidance on how to categorize the sensitivity of PII resulting in selection of a **PII confidentiality impact level.** The PII confidentiality impact levels in NIST SP 800-122 — low, moderate, or high — are based on a combination of the FIPS 199 impact values and six factors for determining the harm[22] (*see* Table 2 below) that could result to the subject individuals, the organization, or both, if PII were inappropriately accessed, used, or disclosed.[23] The FIPS 199 impact value definitions are written for information (information types) and information systems and NIST SP 800-122 adopts the "low, moderate, or high" framework for the risk to the PII information type.[24]

[22] NIST SP 800-122, Section 3.1, "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 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."

[23] NIST SP 800-122, Section 3.2, discusses the use of six factors to determine impact levels and the freedom of agencies to determine the most relevant factors, including extending the six factors when appropriate. The six factors include identifiability, quantity of PII, data field sensitivity, context of use, obligation to protect confidentiality, and access to and location of PII (see Table 2 of the Privacy Overlays for illustrative examples of these six factors for each PII confidentiality impact level). NIST SP 800-122 leaves it to the organization's discretion to determine whether additional factors should be considered beyond the six defined by NIST. NIST also notes the importance of considering the relevant factors together as the impact levels of each factor may differ.

[24] FIPS 199, Footnote 1, "Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation." When identifying information types, some data elements may be more easily recognized as PII than others, e.g., social security numbers. NIST SP 800-60, Volume II contains detailed descriptions of information types, including a discussion of which information types are likely to have privacy

The Best Judgment Standard from OMB M-07-16 supports a two-step approach to first identify PII in the system and then determine the sensitivity of that PII (alone and then in context) and implement protections commensurate with its sensitivity. Table 1, below, provides the impact values defined in FIPS 199, as incorporated in NIST SP 800-122, which are based on the potential impact of a security breach involving a particular system. *Table 1 should be used in concert with Table 2. Use Table 1 to gain an understanding of the potential adverse effects on individuals, organizational assets, or organizations based on the listed impact value. Use Table 2 to identify the applicable PII confidentiality impact levels based on the factors and illustrative examples of impact descriptions listed.*

Table 1: FIPS 199 Potential Impact Values as Incorporated in NIST SP 800-122

Potential Impact Value	Type of adverse effect on organizational operations, organizational assets, or individuals	Expected adverse effect of the loss of confidentiality, integrity, or availability on organizational operations, organizational assets, or individuals
LOW	Limited	(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.
MODERATE	Serious	(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.
HIGH	Severe or catastrophic	(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.

Table 2 provides six factors described in NIST SP 800-122, with illustrative examples aligned to the three PII confidentiality impact levels.

implications. Some examples of those information types with privacy implications include: Program Evaluation, Travel, Intelligence Operations, Space Operations, and Health Care Administration.

Table 2: Illustrative Examples of the Six Factors Described in NIST SP 800-122 as Used in Determining PII Confidentiality Impact Levels[25]

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact Level[26]		
	Low	**Moderate**	**High**
Identifiability	Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.	Combined data elements uniquely and directly identify individuals.	Individual data elements directly identifying unique individuals.
Quantity of PII	A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.	A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a serious or substantial amount of data.	A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a significantly large amount of data, e.g., "Big Data."
Data Field Sensitivity	Data fields, alone or in combination, have little relevance outside the context.	Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.	Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
Obligation to Protect Confidentiality[27]	Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.	Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide	Organization or Mission-specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government-wide or industry-specific

[25] These examples are for illustrative purposes and provided to clarify the six factors from NIST SP 800-122; each instance of PII is different, and each organization has a unique set of requirements and different missions to consider.

[26] NIST SP 800-122, p. ES-2, "PII should be evaluated to determine its PII confidentiality impact level, which is different from the Federal Information Processing Standard (FIPS) Publication 199 confidentiality impact [value], so that appropriate safeguards can be applied to the PII. 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."

[27] NIST SP 800-122, p. ES-3, "An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance). For example, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII." NIST 800-122, Section 3.2.5, advises that "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."

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact Level[26]		
	Low	Moderate	High
		requirements. Violations may result in serious civil or criminal penalties.	requirements. Violations may result in severe civil or criminal penalties.
Access to and Location of PII	Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.	Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization-owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at contractor-owned facilities.	Located on computers and other devices on a network not controlled by the organization or on mobile devices or storage media. Access open to the organization's entire workforce. Remote access allowed by equipment owned by others (e.g., personal mobile devices). Information can be stored on equipment owned by others (e.g., personal USB drive).
Context of Use	Disclosure of the act of collecting, and using the PII, *or* the PII itself is unlikely to result in limited harm to the individual or organization such as name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.	Disclosure of the act of collecting, and using the PII, *or* the PII itself may result in serious harm to the individual or organization such as name, address, and phone numbers of a list of people who have filed for retirement benefits.	Disclosure of the act of collecting, and using the PII, *or* the PII itself is likely to result in severe or catastrophic harm to the individual or organization such as name, address, and phone numbers of a list of people who work undercover in law enforcement.

2.6 Additional Assumptions

The Privacy Overlays are based on the following assumptions:

- The information system maintains, collects, uses, stores, archives, or disseminates (hereafter "maintains") PII, possibly including PHI, throughout the information lifecycle.
- The information system's inclusion of PII may not be immediately apparent.[28]
- The sensitivity of PII is a separate analysis from both dissemination control, e.g., "NOFORN" and classification, e.g., "Secret."

[28] Examples of where PII may be identified for a system include the data dictionary, the architecture for the data store(s), or the data store(s) themselves. For existing systems, current privacy documentation, such as PIAs and SORNs, may provide insight into the types of PII in a system. However, these may be documented at a higher level of categories or types than is necessary for the categorization of system information and determining privacy risk for the purposes of implementing the Privacy Overlays.

- The requirement to implement the Privacy Overlays is separate and distinct from the requirement to conduct a Privacy Impact Assessment (PIA).[29] The Privacy Overlays are required by CNSSI 1253 for all NSS that maintain PII as described in this Section regardless of whether the requirement to conduct a PIA applies.
- The information system implements the applicable Privacy Overlay(s) to ensure that the PII in the information system is protected from security threats.

There are also some possible situations that are specifically not addressed in the Privacy Overlays. These include:

- Applicability of privacy documentation requirements for information systems containing PII or PHI, e.g., PIA, system of records notice, etc.;[30] and
- Ensuring that the functionality of the system is free from privacy risks.[31]

3. Applicability

Use the questions below and the appropriate PII confidentiality impact level — low, moderate, or high — to identify the applicable Privacy Overlays. For example, if the PII confidentiality impact level is high, then the privacy and security controls marked as high in Table 3 of this document are applicable for the information system. For assistance in answering these questions, consult with your organization's Privacy Office, General Counsel, and/or Cybersecurity Office.

1) *Does the information system contain PII?*

   Identify if your system contains PII by using Section 2.3.1, "PII." If the answer to this question is no, the Privacy Overlays do not apply. If the answer is yes, continue through the

[29] A PIA is a risk analysis process implemented during the development or acquisition phase of an information system to identify, evaluate, mitigate, and document privacy risks to individuals and agencies. The Privacy Overlays present a subset of security and privacy controls applicable to information systems that contain PII and/or PHI and are selected from the NIST SP 800-53 security, information security programs, and privacy control catalogs, per CNSSI 1253 at Appendix F. One does not obviate the need for the other. The information and evaluation process of a PIA will inform the successful implementation of these Privacy Overlays, and vice versa. For example, the PIA facilitates analysis of the sensitivity of the PII in a system which supports an evaluation of the appropriate PII confidentiality impact level for the system while the security controls implemented via the Privacy Overlays support a discussion within the PIA about how the organization has protected the PII in the system.

[30] The E-Government Act of 2002, which requires PIAs for federal information systems under Section 208, provides a limited exception under Section 202(i) for information systems that meet the statutory definition of NSS which must be determined through a case-by-case analysis of the information system and not a blanket assumption based on the organization. While not required by law, however, identifying and addressing privacy risks in federal NSS through the PIA process may be required by organizational policy.

[31] An information system could be protected by the controls in the Privacy Overlays and successfully perform its required data action as intended by the purpose of the system, while the data action itself may result in privacy risks to individuals, i.e., the PII in a system is protected from security threats, but the intended data action of the system itself presents privacy risks. Such data actions have been referred to by NIST as "problematic data actions." Anticipation and prevention of those problematic data actions and the associated privacy risks to individuals and organizations are outside the scope of the Privacy Overlays. See generally, NIST, *Privacy Engineering Objectives and Risk Model*, available online at http://csrc.nist.gov/projects/privacy_engineering/documents.html (accessed 28 March 2015).

additional questions below.

2) *Does Exception of the Business Rolodex Information apply?*

   Determine if the exception for business Rolodex information applies by using Section 2.4, "Exception of the Business Rolodex Information." If the answer to this question is yes, the overlays do not apply. If the answer is no, continue through the additional questions below.

3) *Is the PII confidentiality impact level low, moderate, or high?*

   Determine the PII confidentiality impact level by using Section 2.5, "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. Continue to question 4.

4) *Is your organization a covered entity or business associate under HIPAA?*

   Determine if: a) your organization is a covered entity or business associate under HIPAA, and b) the PII in the information system is PHI, by using Section 2.3.2, "PHI." If the answers to both a) and b) are yes then the information system contains PHI, and the organization must apply the PHI Privacy Overlay. If the answer to either a) or b) is no, then the organization should not apply the PHI Privacy Overlay. Application of the PHI Privacy Overlay is in addition to the low, moderate, or high Privacy Overlay selected in response to question 3.

4. Overlays Summary

The table below contains a summary of the security and privacy control specifications as they apply in the Privacy Overlays. The detailed specifications and tailoring considerations for each control can be found in the sections that follow. The symbols used in the table are as follows:

- A plus sign ("+") indicates the control should be selected.
- Two "dashes" ("--") indicates the control should not be selected.[32]
- The letter "E" indicates there is a control extension.[33]
- The letter "G" indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter "V" indicates this overlay defines a value for an organizational-defined parameter for the control.
- The letter "R" indicates there is at least one regulatory/statutory reference that affects the control selection or that the control helps to meet the regulatory/statutory requirements.

Controls that include an E, G, V, or R specification without a "+" or a "--" are not required, but they do have privacy implications when implemented for other reasons. Please see the Tailoring Considerations section for more information regarding these specifications.

[32] AC-2(8) includes regulatory/statutory references that prohibit its selection of this control for systems that maintain PII with a PII Confidentiality Impact Level of Moderate or High and for PHI.
[33] Control extensions will be submitted to NIST for consideration when updating the NIST SP 800-53 catalog.

Table 3: Privacy Overlays Security and Privacy Controls

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
AC-1	+GR	+GR	+GR	+ER
AC-2	+EGVR	+EGVR	+EGVR	+EGR
AC-2(8)		--R	--R	
AC-2(9)	GVR	GVR	GVR	R
AC-2(13)	+R	+R	+R	+R
AC-3	+EGR	+EGR	+EGR	+GR
AC-3(9)		+EVR	+EVR	+R
AC-3(10)	GVR	GVR	GVR	
AC-4		+GR	+GR	+R
AC-4(8)			+VR	
AC-4(12)				+GR
AC-4(15)		+GR	+GR	+R
AC-4(17)		+GVR	+GVR	
AC-4(18)		+GR	+GR	+R
AC-5		+GR	+GR	+GR
AC-6		+GR	+GR	+GR
AC-6(1)			+GR	+R
AC-6(2)		+GR	+GR	+R
AC-6(3)			GR	
AC-6(5)			+R	+R
AC-6(7)	+VR	+VR	+VR	+VR
AC-6(9)		+R	+R	+R
AC-6(10)		+R	+R	
AC-8	GR	GR	GR	GR
AC-11	+EVR	+EVR	+EVR	+GR
AC-12				+GR
AC-14		GR	GR	GR
AC-16	+GVR	+GVR	+GVR	+GVR
AC-16(3)	+GVR	+GVR	+GVR	+GVR
AC-17	+GR	+GR	+GR	+GR
AC-17(1)	+GR	+GR	+GR	+R
AC-17(2)	+R	+R	+R	+GR
AC-18(1)	+GR	+GR	+GR	
AC-19	+ER	+ER	+ER	+GR

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
AC-19(5)	+EVR	+EVR	+EVR	+GVR
AC-20	+EGR	+EGR	+EGR	+R
AC-20(1)	+R	+R	+R	+R
AC-20(3)	+EGVR	+EGVR	+EGVR	
AC-21	+GR	+GR	+GR	+GR
AC-22	+GR	+GR	+GR	+R
AC-23	EGR	EGR	EGR	
AT-1	+GR	+GR	+GR	+R
AT-2	+ER	+ER	+ER	+GR
AT-3	+ER	+ER	+ER	+R
AT-4	+GR	+GR	+GR	+R
AU-1	+GVR	+GVR	+GVR	+R
AU-2	+GVR	+GVR	+GVR	+GR
AU-3	+GR	+GR	+GR	+R
AU-4		+GR	+GR	+R
AU-4(1)		GR	GR	R
AU-6		+GR	+GR	+R
AU-6(3)		+R	+R	
AU-6(10)		+GR	+GR	
AU-7	+R	+R	+R	+R
AU-7(1)		+R	+R	+R
AU-7(2)		+R	+R	+R
AU-9	+GR	+GR	+GR	+R
AU-9(3)		+GR	+GR	+GR
AU-9(4)		GR	GR	
AU-10		+GR	+GR	+R
AU-10(1)		+GR	+GR	+R
AU-11(1)		GR	GR	
AU-12		+R	+R	+R
AU-12(3)		+VR	+VR	+VR
AU-14		GR	GR	
AU-14(2)		GR	GR	
AU-14(3)		GR	GR	
AU-16(2)				+GVR
CA-1	+GR	+GR	+GR	+R

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
CA-2	+GR	+GR	+GR	+VR
CA-3		+R	+R	+GVR
CA-3(3)	+VR	+VR	+VR	+R
CA-3(5)	+VR	+VR	+VR	+R
CA-6	+EGR	+EGR	+EGR	+GR
CA-7		+GR	+GR	+GR
CA-8			+GVR	
CA-9		+GVR	+GVR	+VR
CA-9(1)		+GR	+GR	+R
CM-3(6)	+GVR	+GVR	+GVR	+GVR
CM-4	+GR	+GR	+GR	+R
CM-4(1)		+GR	+GR	
CM-4(2)		+R	+R	+R
CM-8(1)				+R
CP-1	+R	+R	+R	+R
CP-2	+R	+R	+R	+GR
CP-2(5)				+R
CP-2(8)				+GR
CP-4				+GR
CP-7		GR	GR	GVR
CP-9		+ER	+ER	+ER
CP-10		+R	+R	+R
IA-2	+R	+R	+R	+R
IA-2(6)		+GR	+GR	
IA-2(7)		+GR	+GR	
IA-2(11)		+GR	+GR	
IA-3				+R
IA-4	+ER	+ER	+ER	+GR
IA-4(3)		+GR	+GR	
IA-5		+R	+R	+GR
IA-6				+GR
IA-7	+GR	+GR	+GR	+GR
IA-8		+R	+R	+R
IR-1	+GVR	+GVR	+GVR	+GR
IR-2	+GR	+GR	+GR	+GR

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
IR-4	+GR	+GR	+GR	+GR
IR-4(3)				+EVR
IR-5	+GR	+GR	+GR	+R
IR-6	+GVR	+GVR	+GVR	+R
IR-7	+GR	+GR	+GR	+R
IR-8	+GR	+GR	+GR	+GR
IR-10	+GR	+GR	+GR	
MA-1		+ER	+ER	+GR
MA-2				+GR
MA-4(6)	+R	+R	+R	+R
MA-5	+GR	+GR	+GR	+GR
MP-1	+VR	+VR	+VR	+VR
MP-2	+VR	+VR	+VR	+VR
MP-3	+GR	+GR	+GR	+GR
MP-4	+VR	+VR	+VR	+R
MP-5	+VR	+VR	+VR	+VR
MP-5(4)	+R	+R	+R	+GR
MP-6		+GVR	+GVR	+VR
MP-6(1)	+GR	+GR	+GR	+GR
MP-6(8)		+GR	+GR	
MP-7		+GVR	+GVR	
MP-7(1)		+R	+R	
MP-8(3)		+VR	+VR	+GVR
PE-1				+R
PE-2	+R	+R	+R	+GR
PE-2(1)				+GR
PE-3	+R	+R	+R	+R
PE-4				+GR
PE-5	+GR	+GR	+GR	+GR
PE-6				+GR
PE-8				+GR
PE-17	+GR	+GR	+GR	
PE-18			+GR	+GR
PL-1				+ER
PL-2	+EGR	+EGR	+EGR	+R

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
PL-4	+ EGR	+EGR	+EGR	
PL-8	+GR	+GR	+GR	
PS-1	+ER	+ER	+ER	+R
PS-2	+ER	+ER	+ER	+GR
PS-3	+ER	+ER	+ER	+GR
PS-3(3)	+GVR	+GVR	+GVR	+GR
PS-4	+GR	+GR	+GR	+GR
PS-5	+ER	+ER	+ER	+GR
PS-6	+GR	+GR	+GR	+R
PS-7	+GR	+GR	+GR	+R
PS-8	+EGR	+EGR	+EGR	+R
RA-1	+EGR	+EGR	+EGR	+R
RA-2	+ER	+ER	+ER	+R
RA-3	+EGVR	+EGVR	+EGVR	+GVR
SA-2	+ER	+ER	+ER	
SA-3	+GR	+GR	+GR	
SA-4	+EGR	+EGR	+EGR	+ER
SA-8	+GR	+GR	+GR	
SA-9				+ER
SA-9(5)	+EGR	+EGR	+EGR	
SA-11		+EGR	+EGR	
SA-11(5)			+ER	
SA-15(9)		+EGR	+EGR	
SA-17	+EGR	+EGR	+EGR	
SA-21	+GVR	+GVR	+GVR	+GR
SC-2		+ER	+ER	+ER
SC-4	+GR	+GR	+GR	+R
SC-7(14)				+GVR
SC-8	+GVR	+GVR	+GVR	+VR
SC-8(1)	+EVR	+EVR	+EVR	+GR
SC-8(2)		+GVR	+GVR	
SC-12	+VR	+VR	+VR	+GR
SC-13	+VR	+VR	+VR	+GR
SC-28	+GVR	+GVR	+GVR	+R
SC-28(1)	+EGR	+EGR	+EGR	+GR

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
SI-1	+R	+R	+R	+R
SI-3				+GR
SI-4	+GR	+GR	+GR	+R
SI-5				+GR
SI-7	+VR	+VR	+VR	+VR
SI-7(6)	+ER	+ ER	+ ER	+ GR
SI-8				+ GR
SI-10		+VR	+ VR	
SI-11	+VR	+ VR	+ VR	+ VR
SI-12	+EGR	+EGR	+EGR	+EGR
PM-1	+GR	+GR	+GR	+R
PM-2	GR	GR	GR	+ER
PM-3	+R	+R	+R	
PM-5	+GR	+GR	+GR	+GR
PM-7	+GR	+GR	+GR	+R
PM-9	+ER	+ER	+ER	+ER
PM-10	+EGR	+EGR	+EGR	+ER
PM-11	+EGR	+EGR	+EGR	+R
PM-12	+ER	+ER	+ER	
PM-13	GR	GR	GR	R
PM-14	+EGR	+EGR	+EGR	
PM-15	+EGR	+EGR	+EGR	
AP-1	+GR	+GR	+GR	
AP-2	+GR	+GR	+GR	
AR-1	+EGR	+EGR	+EGR	+GR
AR-2	+GR	+GR	+GR	+R
AR-3	+ER	+ER	+ER	+ER
AR-4	+GVR	+GVR	+GVR	+R
AR-5	+EGR	+EGR	+EGR	+R
AR-6	+R	+R	+R	+GR
AR-7	+GR	+GR	+GR	+R
AR-8	+R	+R	+R	+GR
DI-1	+GR	+GR	+GR	
DI-1(1)		+GR	+GR	
DI-1(2)		+VR	+VR	

CONTROL	PRIVACY OVERLAYS			
	PII Confidentiality Impact Level			
	LOW	MODERATE	HIGH	PHI
DI-2	GR	GR	GR	
DI-2(1)	GR	GR	GR	
DM-1	+GR	+GR	+GR	+R
DM-2	+VR	+VR	+VR	+VR
DM-2(1)				+R
DM-3	+GR	+GR	+GR	+GR
DM-3(1)	GR	GR	GR	+GR
IP-1	+GR	+GR	+GR	+GR
IP-1(1)				+R
IP-2	+GR	+GR	+GR	+ER
IP-3	+GR	+GR	+GR	+R
IP-4	+R	+R	+R	+R
IP-4(1)	GR	GR	GR	+R
SE-1	+GR	+GR	+GR	+ R
SE-2	+GR	+GR	+GR	+R
TR-1	+GR	+GR	+GR	+GR
TR-1(1)	G	G	G	GR
TR-2	+GR	+GR	+GR	
TR-2(1)	+GR	+GR	+GR	
TR-3	+R	+R	+R	
UL-1	+EGR	+ EGR	+ EGR	+R
UL-2	+ EGR	+ EGR	+ EGR	+ GR

5. Detailed Overlays Control Specifications

This section is a comprehensive view of the security and privacy controls as they apply to the Privacy Overlays. The guidance provided in this section elaborates on the guidance given in NIST SP 800-53, Rev. 4. For controls that should either be selected ("+") or not selected ("--"), a justification is given based on the defined overlay characteristics. In addition to justification, a security or privacy control may have other specifications that include control extensions "("E"), supplemental guidance ("G", including specific tailoring guidance), parameter values ("V"), and regulatory/statutory references ("R").

Some controls discussed in the Privacy Overlays may not be selected for any overlay, yet may include supplemental guidance — when systems containing PII employ these controls (e.g., selected as part of a baseline or another overlay), the supplemental guidance should be followed to ensure privacy considerations related to that control are addressed. These controls can be found in Section 6, Tailoring Considerations.

On occasion, a security or privacy control may only include a selection or supplemental guidance without a reference — in these instances applicability of the control is not absolute but should be considered as a common practice (see as an example TR-1(1)).

AC-1, ACCESS CONTROL POLICY AND PROCEDURES

Justification to Select: Access Control policies and procedures form the foundation that allows privacy protections to be implemented for the identified uses of PII and PHI.

PHI Control Extension: The organization develops, disseminates, and reviews/updates the access control policies and procedures complying with the HIPAA Minimum Necessary Rule and permitted or required uses and disclosures, to limit unnecessary or inappropriate access to PHI.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Privacy requirements commonly use the terms "adequate security" and "confidentiality" when referring to access controls and other security safeguards for PII. Applied together, these terms signify the need to make risk-based decisions based on the magnitude of harm (to both organizations and individuals) when determining applicable restrictions for PII. For the purpose of this overlay, refer to the definitions of "adequate security" in OMB Circular A-130, Appendix III, and "confidentiality" in NIST SP 800-37, Rev. 1, Appendix B. These definitions are consistent with CNSSI No. 4009. Related Controls: AR-4; AR-7.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b), (e)(9)-(10); OMB M-07-16, Att. 4; OMB Circular A-130, 7.g. and Appendix III; OMB M-06-16; NIST SP 800-37, Rev. 1, Appendix B; NIST SP 800-122

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.514(d)(1)-(5)

AC-2, ACCOUNT MANAGEMENT

Justification to Select: Account management is a critical function for developing and implementing an access control framework that is appropriate for the information contained in systems and applications. When implemented effectively, the access control framework provides the necessary constructs for controlling access to PII, limiting disclosure of records about individuals to only those system and application users that have a need for the information to perform their job functions. The purpose of this guidance is to establish requirements for user access to PHI and PII.

Low PII Confidentiality Impact Level Control Extension: Prohibit use of guest, anonymous, and shared accounts for providing access to PII. Notify account managers

within an *organization-defined timeframe* when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes. Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties.

Moderate and High PII Confidentiality Impact Level Control Extension: Apply the Low PII confidentiality impact level Control Extension. Implement access controls within the information system based on users' or user group's need for access to PII in the performance of their duties. Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AC-16, AC-3

PHI Control Extension: Apply the High PII confidentiality impact level Control Extension.

PHI Supplemental Guidance: The identification of authorized users and access privileges include considerations of whether the user will need access to PHI and whether such access may be permitted or required under HIPAA. The purpose of this guidance is to establish requirements for user access to PHI. Organizations should establish procedures for obtaining necessary electronic protected health information, to include during an emergency. Related Controls: AC-16, AC-3

Low and Moderate PII Confidentiality Impact Level Parameter Value:
f.… the requirement for each user to complete annual privacy training, or otherwise the account would be disabled.
j.… at least annually.

High PII Confidentiality Impact Level Parameter Value:
f.… the requirement for each user to complete privacy training annually, otherwise the account would be disabled.
j.… at least quarterly for privileged accounts, at least annually for general user's accounts

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b), (e)(9)-(10); OMB M-07-16, Att. 1

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.312(a)(2)(ii); 45 C.F.R. §164.502

Control Enhancement: 8

Justification to Not Select: Access to PII may not be granted to entities who are previously unknown, only to officers and employees who have a need for the information

in performance of their duties. Dynamic account creation (DAC) is an automated process that may not support independent verification of a need for access to PII.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b)(1); OMB Circular A-130, 7.g.

Control Enhancement: 13

Justification to Select: Disabling accounts for high-risk individuals is a minimum requirement for the organization's rules of behavior as a consequence for abusing access privileges to access PII, including information protected under the Privacy Act of 1974.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(1)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(C)

AC-3, ACCESS ENFORCEMENT

Justification to Select: Access to PII is more effectively controlled when access controls are considered during system design and built-into or enforced by the system (i.e. automated controls). Well-designed, automated access controls (e.g., mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), or attribute-based access control (ABAC)) limit user access to information according to defined access policies, which helps ensure the security and confidentiality of the PII contained in the system.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Organizations shall control access to PII through access enforcement mechanisms. For example, implement role-based access controls and configure access controls so that each user can access only the pieces of information necessary for the user's role or only permit users to access PII through an application that restricts their access to the PII the users require, instead of allowing users direct access to a database or files containing PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AC-16, AC-2

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB M-06-16

PHI Supplemental Guidance: Related Controls: AC-16, AC-2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(a)(2)(i)

Control Enhancement: 9

Justification to Select: PII released outside a system boundary may be at increased risk of unauthorized access and use. Release could include a formal process or an informal activity, such as a spreadsheet receiving data extracted from an information system.

Moderate and High PII Confidentiality Impact Level Control Extension: Applicable policy mandates establishing policy regarding access to PII, including PHI, are the Privacy Act of 1974,E-Government Act of 2002 (Section 208), and HIPAA. PII may only be released when authorized, there is a need to know, and adequate assurances of protection have been provided. Related Controls: AC-21, UL-1, UL-2.

Moderate and High PII Confidentiality Impact Level Parameter Value:
(a) … organization or information system…
… privacy and security controls commensurate with the PII confidentiality impact level of the PII being received…
(b) … Appendix J, Controls UL-1 and UL-2…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(a)(7), (b), (c), (e)(3)(c), (o); Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment, Overview

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(4)(i)

AC-4, INFORMATION FLOW ENFORCEMENT

Justification to Select: The information flow enforcement controls provide a technical means of implementing disclosure requirements by minimizing information shared between networks, devices, and individuals within information systems and between interconnected systems. This control can also limit information transfers between organizations based on data structures and content.

Moderate and High PII Confidentiality Impact Level Supplementary Guidance: Related Control: AC-16

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b); OMB M-06-19; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.310(b)

Control Enhancement: 8

Justification to Select: Security policy filters, or like technology, such as data loss prevention (DLP), can provide a form of continuous monitoring for compliance with

privacy laws and regulations. Implementation of this security control reduces the potential for unauthorized transfer of PII.

High PII Confidentiality Impact Level Parameter Value:
…… best available security policy filters, or like technology to filter on selected PII values …… prevention of unauthorized transfer of PII across information system boundaries or domains.

High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b); OMB M-06-19; OMB M-07-16; NIST SP 800-37, Rev. 1, Appendix G

Control Enhancement: 12

Justification to Select: The confidentiality of PHI is better protected when a system can automatically detect data types and usage when being transferred from one security domain to another. This includes, for example, transfers between systems having different access controls with only a limited set of users allowed access to the PHI.

PHI Supplemental Guidance: Ensure that the minimum security controls identified in this overlay for PHI are in place to protect the data before transferring data between security domains.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312

Control Enhancement: 15

Justification to Select: To provide the ability for an organization to monitor and prevent transfer of PII across different security domains, a system needs to have mechanisms to automatically detect, and where appropriate, prohibit the unauthorized transfer of PII across different security domains. Typical implementations of such controls will detect particular data types or metadata tagging and take action to prevent the transfer of the information beyond the intended boundaries.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: The organization ensures systems containing moderate and high PII confidentiality impact level information include the capability for the organization to centrally monitor for and detect unauthorized transfer of such PII across different security domains. Some technologies that would facilitate this include data-loss prevention, data-rights management, and key-word detection to prevent the unauthorized export of information from a network or to render such information unusable in the event of the unauthorized export of such information between security domains. Related Control: AC-16

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b), (e)(9)-(10)

PHI Regulatory/Statutory References: 45 C.F.R. §164.306(a); 45 C.F.R. §164.308(a)(5)(ii)(B)

Control Enhancement: 17

Justification to Select: The ability to identify source and destination points for PII flow within information systems is necessary for attribution and compliance with need to know requirements.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Implement a higher level of granularity for identification and authentication based on sensitivity of the PII. This is not to determine permissibility of the transfer but to enable an audit capability.

Moderate and High PII Confidentiality Impact Level Parameter Value: … the applicable organization, system, application, or individual…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(c) and (e)(10); OMB M-06-16

Control Enhancement: 18

Justification to Select: To have a high level of trust in the information flow of PII, this control ensures the security attributes selected in AC-16 are bound to the information.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: To ensure the protection of PII throughout its information flow, this control should be used to protect PII as it travels within and among information systems and information system components, such as database servers, application servers, shared storage environments, document repositories, and file folders. Related Control: AC-16.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB Circular A-130, 7.g. and Section 8 and Appendix III; OMB M-07-16; OMB M-06-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.306(a)

AC-5, SEPARATION OF DUTIES

Justification to Select: Separation of duties aligns privileges with appropriate roles with the idea that duties are split between roles in such a way as to reduce the risk of malevolent or inappropriate behaviors based on access. Implementing this control helps reduce the risk of inappropriate access to PII (e.g., separating employees that perform security investigations from mission and business functions).

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Separation of duties is implemented by designating a selected set of administrators the capability to set user permissions to PII and PHI information, while those administrators do not themselves have access to the PII and PHI. The principle of separation of duties is significant for developers as well as for operational system administrators. Related Control: AC-6

PHI Supplemental Guidance: HIPAA requires the separation of duties to ensure that checks and balances are designed into the system to limit the effect of any given end user to control the entire process. Roles and responsibilities should be divided so that a single end user cannot subvert a critical process. This practice divides the tasks related to maintaining system security among different personnel such that no single individual could compromise PHI. Related Control: AC-6.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(e)(10)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(c)(1)

AC-6, LEAST PRIVILEGE

Justification to Select: The concept of least privilege aligns with the notion of only allowing access to PII when a particular individual has a need-to-know in performance of their job duties.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: The organization enforces the most restrictive set of rights/privileges or access needed by users (or processes acting on behalf of users) for the performance of specified tasks — increasing the level of restriction as PII confidentiality impact level rises. The organization ensures 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) necessary to perform their assigned tasks.

PHI Supplemental Guidance: HIPAA requires least privilege to satisfy both the Minimum Necessary Rule and access control safeguards. Related Control: AC-5.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b); OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.502(b)

Control Enhancement: 1

Justification to Select: Limiting access to security functions to authorized personnel reduces the number of users able to perform certain security functions, such as configuring access permissions, setting audit logs, performing system management functions. Examples of authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. These types of security functions can provide a level of access to PII, and capabilities to manipulate it, in ways that other users roles typically could not.

High PII Confidentiality Impact Level Supplemental Guidance: The organization identifies the security relevant functions that require authorized access for all information systems that contain moderate or high PII confidentiality impact level information.

High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b)(1); OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.502(b)

Control Enhancement: 2

Justification to Select: This control requires system users with elevated privileges to use their non-privileged accounts when performing non-security functions. Requiring system users to use their non-privileged accounts when working with PII for purposes other than security functions limits inadvertent access to or disclosure of PII and protects the integrity of PII.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Any access involving PII that is non-administrative in nature should require the user to use their non-privileged accounts to perform that function.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b); OMB M-06-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.502(b)

Control Enhancement: 5

Justification to Select: This control limits who is authorized to administrative accounts, such as those who can perform security functions, which include configuring access permissions, setting audit logs and performing system management functions. These types of system and network management personnel typically have a level of access that is capable of circumventing other access controls. Limiting access to these accounts

further protects PII by limiting the number of individuals that have the "keys to the kingdom" on a network or system.

High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b)(1); OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.312(a)(1)

Control Enhancement: 7

Justification to Select: Review of user privileges is necessary in order to ensure privileges are revoked for those who no longer require access to PII or PHI. Implementation of this control reduces the risk of unauthorized access to PII by users who no longer need access to perform their job functions.

Low and Moderate PII Confidentiality Impact Level Parameter Value:

(a) … at least annually…
… individuals with access to low or moderate confidentiality impact level PII……

High PII Confidentiality Impact Level Parameter Value:

(a) … at least quarterly…
…… individuals with access to privileged accounts…

AND

(a) … at least annually…
… individuals with access to high confidentiality impact level PII……

PHI Parameter Value:

(a) … at least quarterly…
…… individuals with access to privileged accounts…

AND

(a) … at least annually…
… individuals with access to PHI……

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) , (e)(9)-(10); OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R.

§164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.312(a)(2)(ii); 45 C.F.R. §164.312(b)

Control Enhancement: 9

Justification to Select: Privileged functions have elevated permissions to access, and grant access, to PII. Accountability requires the ability to detect, trace, and audit a privileged function whenever it is executed.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g. and Appendix III

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)

Control Enhancement: 10

Justification to Select: Non-privileged users may not have the same level of trust as privileged users. Privileged functions have access beyond that of the typical user, and as such may have greater ability to access PII. Individual accountability requires the ability to trace (audit) the actions of the user who initiated them.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g. and Appendix III

AC-11, SESSION LOCK

Justification to Select: This control protects PII from unauthorized access when system users are away from their workstation. Since 2007, OMB has required session lock for remote and mobile devices, a standard which is neither technically nor financially burdensome. Based on risk, many agencies have adopted 15-minute session locks by policy as a best practice.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Period of inactivity shall be no more than 30 minutes before session lock occurs for remote and mobile devices and requires user re-authentication. As agencies continue to migrate to laptops and docking stations making clients increasingly mobile, this is a logical extension of that requirement.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control, therefore the decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:
a. … no more than 30 minutes…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB M-06-16; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(a)(2)(iii)

AC-12, SESSION TERMINATION

Justification to Select: The session termination control requires implementing functionality to prevent unauthorized use of an established user session. This control protects PHI from unauthorized access when system users have initiated a session.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(2)(iii); 45 C.F.R. §164.308(a)(3)(ii)(C)

AC-16, SECURITY ATTRIBUTES

Justification to Select: Implementation of this control provides a technical means to enforce security and privacy policies, e.g., access controls and encryption. Parameter values specified by the Privacy Overlays for this control include meta-data that supports privacy.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Using the security attributes listed in this control's parameter values section enables cross system functionality and reciprocity through consistent security attribute interpretation. This control supports privacy protections by assigning security attributes that characterize information, devices, or processes (i.e., an "object") as containing PII or associate an organization's mandatory security/privacy training requirement with a user (i.e., a "subject") of an information system containing PII. The terms "Subject" and "Object" are defined in NIST SP 800-53, Rev. 4, Appendix B, *Glossary*. Security attributes are meta-data about either a subject or an object. Other security attributes may exist for other requirements beyond privacy. If an organization creates security attributes they should be cognizant of the risk associated with including PII in that meta-data. However, PII is not included in the security attributes for the parameter values specified below. Related Controls: AC-2, AC-3, AC-4, AC-4(15), AC-4(18)

PHI Supplemental Guidance: The parameter values below for PHI enable policies, procedures, and data classification schemas that specify the application of administrative, technical, physical controls of a specific workstation or class of workstation that maintains electronic PHI. Related Controls: AC-2, AC-3, AC-4, AC-4(15), AC-4(18)

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:
a. … a security attribute to demonstrate the user (subject) has completed privacy training in the last year…
… for data structures that are known or plan to contain PII, a security attribute of "Contains PII" [having] value of "yes" or "no"…

PHI Parameter Value:
a. … for data structures that are known or plan to contain PHI, a security attribute of "Contains PHI" [having] value of "yes" or "no"…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b), (e)(9)-(10); OMB Circular A-130, 7.g. and Appendix III

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.310(b)

Control Enhancement: 3

Justification to Select: In an effort to use automated systems controls for PII and PHI objects, such as intrusion detection and key-word detection tools, maintaining the association and integrity of security attributes to subjects and objects can be used as the basis of automated policy actions.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance:
Related Controls: AC-4, AC-4(15), AC-4(18)

PHI Supplemental Guidance: Implement policies, procedures, and data classification schemas that specify the manner in which the physical, technical, and security attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:
… the user attribute of "Annual PII Training" [to] individuals with access to PII……
… the information attribute of "Contains PII" [to] applicable information…

PHI Parameter Value:
… the information attribute of "Contains PHI" [to] applicable information……

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and Appendix III

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.310(b)

AC-17, REMOTE ACCESS

Justification to Select: Limiting access to PII from remote networks and/or restricting activities that can be conducted with PII remotely reduces the risk of intentional and unintentional disclosures of PII that may not exist on an internal network.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Allow remote access to PII only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

PHI Supplemental Guidance: Implement technical security measures to guard against unauthorized remote access to electronic PHI that is being transmitted over an electronic communications network.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-06-16; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(e)(1)

Control Enhancement: 1

Justification to Select: Auditing remote access ensures unauthorized connections to information systems containing PII can be detected across all information system platforms (e.g., servers, mobile devices, work stations).

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Audit all remote access to, and actions on, resources containing PII. Related Control: AU-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-06-16; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(e)(1);

Control Enhancement: 2

Justification to Select: Encrypting remote sessions protects the confidentiality and integrity of PII.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-06-16, Step 3

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii);

AC-18, WIRELESS ACCESS

Control Enhancement: 1

Justification to Select: Communications over wireless networks, unless properly secured, have greater risk of interception than hard-wired networks. Implementing encryption of wireless network communications containing PII renders any intercepted data unreadable.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: If wireless networks permit access to organization information systems containing PII, then encryption of content and authentication of users or devices is required. Organizations should ensure that all WLAN components use Federal Information Processing Standards (FIPS)-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications. Related Controls: AC-3, IA-2, IA-3, IA-8.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: NIST SP 800-97, NIST SP 800-153

AC-19, ACCESS CONTROL FOR MOBILE DEVICES

Justification to Select: Limiting access to PII from mobile devices reduces the risk of intentional and unintentional disclosures of PII that may not exist on an internal network.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Encrypt information on all mobile devices that contains low, moderate, and high PII confidentiality impact level information.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-06-16; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(2)(ii)

Control Enhancement: 5

Justification to Select: Mobile devices are more likely to be lost or stolen and as a result PII is more vulnerable. Encryption reduces this vulnerability.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Encrypt information on all mobile devices that contains low, moderate, and high PII confidentiality impact level information.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:
… full-device encryption or container encryption…
… on any type of mobile device permitted by the organization to access PII…

PHI Parameter Value:
… full device encryption or container encryption…
… on any type of mobile device permitted by the organization to access PHI…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-06-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(iv)

AC-20, USE OF EXTERNAL INFORMATION SYSTEMS

Justification to Select: Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is reinforced by a binding agreement to terms and conditions of the organization's privacy requirements to ensure awareness and accountability of both parties.

Low, Moderate, and High PII Confidentiality Impact Level Control Enhancement: Privacy requirements shall be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage PII. Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is limited to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements which protect the PII.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Such agreements may include memoranda of understanding (MOUs), terms of service, or contracts.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); FAR Part 24, 39.105; OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(i)

Control Enhancement: 1

Justification to Select: An external information system which processes, stores, or transmits PII needs to have its security controls verified to meet the organization's security control requirements for information systems processing PII.
Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); FAR Part 24, 39.105; OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.314(a)

Control Enhancement: 3

Justification to Select: Mobile devices are more vulnerable to loss or theft than other types of computing media (e.g., desktops and servers) due to their portability and widespread use inside and outside of government facilities. PII stored on mobile devices is more vulnerable as a result. This security control implements protections for PII contained on any mobile device not owned by the organization, including personal mobile devices, commonly referred to as "bring your own device" (BYOD).

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: At a minimum controls must include implementation of either full-device or virtual container encryption to reduce the vulnerability of PII contained on mobile devices. Prior to being provided access to PII on remote devices, device users must acknowledge through a binding agreement their responsibilities to safeguard the PII accessible from the device and that they are aware of and agree to the organization's capabilities to manage the organization's PII on the device, including confiscation, in consultation with the organization's counsel, if necessary to remove the PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The organization should include in its mobile strategy a method to ensure both the device's access to PII can be revoked and the device's PII contents can be remotely removed. Related Control: AC-19(5).

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:
… restricts for PII…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB M-07-16; OMB M-06-16

AC-21, INFORMATION SHARING

Justification to Select: When PII is shared it is necessary to ensure the PII is being shared in accordance with statutory and regulatory requirements, including any restrictions on how the PII may be shared and the requirements for security of the receiving partner.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: This control addresses the sharing of information in a general sense (i.e. disclosure). It is

not "information sharing" as defined by the Information Sharing Environment (ISE) Privacy Guidelines. All sharing partners, processes, and information systems must comply with applicable system of records notice (SORN), Privacy Impact Assessment (PIA), or other forms of notice or public statements. Examples of actions that may be required to implement privacy requirements in information sharing activities include: addressing privacy requirements in information sharing agreements; ensuring sharing partners have a mutual understanding of the PII confidentiality impact level (as NIST SP 800-122 is a risk based analysis and accepts variation in organizational implementation); developing processes and supporting mechanisms to ensure/enforce compliance; and implementing technical capabilities that enforce privacy requirements for PII stored or processed by a sharing partner. Program managers and system owners should work with their privacy office to ensure information sharing activities are compliant with privacy requirements. Related Controls: TR-1, UL-2.

PHI Supplemental Guidance: The privacy officer may permit a business associate to create, receive, maintain, or transmit PHI on behalf of the organization to the extent the business associate is required by law to perform such function or activity, without meeting the requirements of a business associate contract, provided that the privacy officer attempts in good faith to obtain satisfactory assurances required in the business associate contracts, and documents the attempt and the reasons that these assurances cannot be obtained. This control helps covered entities to enforce the Minimum Necessary Rule. Related Control: SA-9.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e); Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.314(a)

AC-22, PUBLICLY ACCESSIBLE CONTENT

Justification to Select: PII that is maintained in a system of records or not approved for release under the Freedom of Information Act (FOIA) is nonpublic information. When agencies consider sharing or posting PII, they must do so in a way that fully protects individual privacy. Under HIPAA, a covered entity or business associate may not use or disclose protected health information except as provided by the HIPAA Privacy Rule. This control implements procedures to protect information, including PII, from being posted publicly improperly.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: PII that is nonpublic information shall not be posted onto a publicly accessible information system.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552(b)(6), OMB M-11-02

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.502(a)

AT-1, SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Justification to Select: Security awareness and training complements privacy awareness and training efforts, particularly where the two disciplines overlap in the areas of use, confidentiality, access, integrity and protection of PII. Coordination between the security and privacy office on the proper use and protections to be afforded to PII within security awareness and training policies addresses the purpose, roles and responsibilities surrounding PII compliance.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AR-5, AR-6.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; OMB M-03-22; OMB M-07-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(5)(i)

AT-2, SECURITY AWARENESS TRAINING

Justification to Select: Security awareness and training complements privacy awareness and training efforts, particularly where the two disciplines overlap in the areas of use, confidentiality, access, and integrity.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Provide privacy training for all systems with PII, commensurate with the PII confidentiality impact level. Integrate privacy training with general Information Assurance (IA) training. Related Controls: AR-5, AR-6.

PHI Supplemental Guidance: The following elements of security training are addressable under HIPAA. The decision to implement the following is dependent on a risk analysis to determine if or to what extent these elements should be included in Security Awareness Training: (i) periodic security updates; (ii) procedures for guarding against, detecting, and reporting malicious software; (iii) procedures for monitoring log-in attempts and reporting discrepancies; and (iv) procedures for creating, changing, and safeguarding passwords.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; OMB M-03-22; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(5)(i)-(ii)

AT-3, ROLE-BASED SECURITY TRAINING

Justification to Select: Role-based training further supports protection of PII by focusing training content on requirements that are specific to an individual's job responsibilities.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Provide role-based privacy training for all systems with PII, commensurate with the PII confidentiality impact level. Related Controls: AR-5, AR-6.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; OMB M-03-22; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(i)

AT-4, SECURITY TRAINING RECORDS

Justification to Select: Maintaining security training records provides the capability for organizations to track compliance with privacy-related training requirements. Under HIPAA, a covered entity must document that the training as described within the regulation has been provided as required.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AR-5, AR-6.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; OMB M-03-22; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(ii)

AU-1, AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Justification to Select: Security audit and accountability policies and procedures directly support privacy audit and accountability procedures.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AU-2, AR-4.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: b.1. … in accordance with organizational policy but not less than annually…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16; OMB Circular A-130, 7.g. and 8.b(2)(c)

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D)

AU-2, AUDIT EVENTS

Justification to Select: This control identifies privacy-relevant security auditable events using a risk-based approach. Examples of privacy-relevant auditable events include logging access to or modification of PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The parameter values for this control do not provide an exhaustive list of all auditable events, but instead list the auditable events required by OMB privacy policy. The organization should manage the length of time that a log file is maintained to the period necessary to comply with the organization's security and privacy policies. Related Control: AR-4.

PHI Supplemental Guidance: The HIPAA Security Rule requires the auditing of activity in information systems that contain PHI but does not identify the specific audit events. Follow PII Supplemental Guidance. Related Control: AR-4.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:
a. … monitor system access, including unsuccessful and successful login attempts, to information systems containing PII…
… successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository…
… privileged activities or system level access to PII…
… concurrent logons from different workstations…
… all program, e.g., executable file, initiations…

d. … monitor system access, including unsuccessful and successful login attempts, to information systems containing PII…
… successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository…
… privileged activities or system level access to PII…
… concurrent logons from different workstations…
… all program, e.g., executable file, initiations…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-06-16; OMB M-07-16; OMB Circular A-130, 7.g., 8.b(2)(c)(iii) and Appendix I.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(5)(ii)(C)

AU-3, CONTENT OF AUDIT RECORDS

Justification to Select: Audit records that are commensurate with the privacy risk they address are an effective tool for identifying whether, when, and how issues have occurred related to data quality and privacy breaches.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-4.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-06-16; OMB M-07-16, Att. 1; OMB Circular A-130, 7.g. and 8.b(2)(c)(iii)

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C)

AU-4, AUDIT STORAGE CAPACITY

Justification to Select: Adequate storage capacity for logs used to audit privacy-related controls reduces the likelihood of the logs exceeding available storage space and potentially losing log information or reducing auditing capability. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act, and providing adequate storage capacity allows for preserving complete audit information for these purposes.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AR-4, AU-5(1), AU-9, AU-9(2), AU-11.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(i); OMB M-07-16; OMB Circular A-130, 7.g. and Appendix II

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D)

AU-6, AUDIT REVIEW, ANALYSIS, AND REPORTING

Justification to Select: Periodic reviews and analysis of privacy logs are important for identifying indications of inappropriate or unusual activity that may signify a privacy incident or breach.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-4.

Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(g)(1)(D), OMB M-7-16.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b)

Control Enhancement: 3

Justification to Select: Correlating and analyzing privacy audit logs across different log repositories and systems provides greater awareness of privacy incidents and breaches across the organization.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(g)(1)(D), OMB M-7-16.

Control Enhancement: 10

Justification to Select: When there is a potential breach of PII, audit levels may need to be adjusted to determine scope and/or magnitude of breach.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Change of risk includes situations involving a potential breach of PII. Related Control: AR-4.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16

AU-7, AUDIT REDUCTION AND REPORT GENERATION

Justification to Select: To meet the deadlines associated with reporting breaches of PII, it is necessary to have the ability to summarize audit information and generate customized audit reports.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)

Control Enhancement: 1

Justification to Select: To conduct efficient and effective remediation of breaches of PII, it may be necessary to tailor the audit fields provided in audit reports. For example, it may be necessary to include the identities of individuals and the system resources involved to determine scope of access to an information system containing PII.

Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)

Control Enhancement: 2

Justification to Select: To conduct efficient and effective remediation of breaches of PII, it may be necessary to tailor the organization of the audit report or to provide search functionality with audit reports that are generated. For example, if the PII breach involves only one or two users it may be most efficient to sort the audit report by user ID or to provide the ability to search on user ID within the audit report.

Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)

AU-9, PROTECTION OF AUDIT INFORMATION

Justification to Select: When audit information contains PII or PHI, it must be protected commensurate with its PII confidentiality impact level. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act. Protecting audit records from compromise by applying this control enhancement helps ensure their availability when needed.

Low, Moderate, and High PII Confidentiality Impact Level Supplementary Guidance: Related Control: AU-4(1).

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(i); OMB M-07-16; OMB Circular A-130, 7.g. and Appendix II

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.306(a)(1)

Control Enhancement: 3

Justification to Select: Using cryptographic mechanisms protects audit log integrity and the confidentiality of the information in the logs, including information related to privacy incidents and breaches. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: In addition to cryptographic mechanisms to protect integrity, the confidentiality of PII may require the use of encryption.

PHI Supplemental Guidance: Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (74 FR 42740), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. Related Controls: RA-3, SI-12.

Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(i); OMB Circular A-130, 7.g. and Appendix II

PHI Regulatory/Statutory References: 45 C.F.R. §164.306(a)(1); 45 C.F.R. §164.312(a)(2)(iv)

AU-10, NON-REPUDIATION

Justification to Select: Non-repudiation is a critical element of accountability and accuracy of information in system history and logs, and it is important for investigating PII incidents and breaches.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AR-4, AR-8.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (g)(1)(C); OMB Circular A-130, 7.g. and 8.b(2)(c)(iii)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(c)(2); 45 C.F.R. §164.312(e)(2)(i)

Control Enhancement: 1

Justification to Select: Digital signatures support accountability and non-repudiation by assuring data object originator authenticity (provides a reasonable level of certainty regarding who did what), data integrity (data has been manipulated by a verifiable person), and time-stamping for prevention of replay (time-stamping may also useful for gauging timeliness and relevance of PII).

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Digital signatures bind the signer to the information the user signs. Digital signatures support accountability and non-repudiation by assuring data object originator authenticity (provides a reasonable level of certainty regarding who did what), data integrity (data has

been manipulated by a verifiable person), and time stamping for prevention of replay (time-stamping may also useful for gauging timeliness and relevance of PII).

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (i)(3); OMB M-04-04; OMB Circular A-130, 7.g. and Appendix II

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(c)(2); 45 C.F.R. §164.312(e)(2)(i)

AU-12, AUDIT GENERATION

Justification to Select: This control defines the technical aspects of how the privacy auditing requirements identified in controls AU-2 and AU-3 will be selected, generated and reviewed for compliance.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g. and 8.b(2)(c)(iii)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b)

Control Enhancement: 3

Justification to Select: Changes to the audit of information systems containing PII must be limited to a subset of authorized system administrators to ensure integrity of audit logs. This control requires organization to define the individuals or roles that would be able to make changes to audit generation requirements.

Moderate and High PII Confidentiality Impact Level Parameter Value:
… limited subset of authorized system administrators…
… any information system that contains PII …
… change in risk based on law enforcement, intelligence, or other credible sources of information or a security incident…

PHI Parameter Value:
… limited subset of authorized system administrators…
… any information system that contains PHI…
… change in risk based on law enforcement, intelligence, or other credible sources of information or a security incident…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g. and 8.b(2)(c)(iii)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R.

§164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.308(a)(2)

AU-16, CROSS-ORGANIZATIONAL AUDITING

Control Enhancement: 2

Justification to Select: As audit logs may contain PII, when audit information is shared between organizations, either an agreement addressing the handling, protection, and disclosure of PII is required, or the sharing is covered by ICS 500-27 or ICS 700-02.

PHI Supplemental Guidance: MOUs, memoranda of agreement (MOAs), and other data sharing agreements must address both protection of PHI, audit content confidentiality ensuring authorized disclosures, and assurance that sharing agreement define which audit events and results are both captured and shared.

PHI Parameter Value:
… to any organization with whom audit information containing PII or PHI is shared…
… MOUs, MOAs, or other data sharing agreements…

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.314

CA-1, SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Justification to Select: The security assessment and authorization policy, procedures and personnel responsibilities should address the strategy for including applicable privacy requirements (e.g., the planned CNSSI No. 1253 Privacy Overlay and NIST SP 800-53 Rev. 4 Privacy Control Catalog) in the security program and information systems.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The security assessment and authorization policy and procedures should address the strategy for including applicable privacy requirements and controls in the security program and information systems. Related Controls: AR-1, AR-7.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(ii); 45 C.F.R. §164.308(a)(2)

CA-2, SECURITY ASSESSMENTS

Justification to Select: This control addresses the process of planning for and executing security assessments, the scope of which should include assessment of applicable privacy requirements.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Once the final security assessment is completed, update the associated PIA to reflect the results of the security assessment. Related Control: AR-2.

PHI Parameter Value: …at least annually and in response to environmental or operational changes affecting the security of electronic protected health information.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b); OMB M-07-16, Att. 1, A.2.c

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(8)

CA-3, SYSTEM INTERCONNECTIONS

Justification to Select: Interconnection Security Agreements (ISAs) document whether and under what circumstances PII can be shared between information systems in different authorization boundaries (e.g., an interface between systems owned by different agencies) over a dedicated or "always on" connection. ISAs communicate that PII will be communicated via the connection and define the security parameters required to protect it. ISAs also provide a record of agreed upon terms and a document to against which controls can be enforced and audited. Organizational policy dictates whether ISAs are required for internal connections within an organization.

PHI Supplemental Guidance: Consider the need for a MOU/MOA or Business Associate Agreement, and implement as necessary.

PHI Parameter Value: …at least annually and in response to environmental or operational changes affecting the security of electronic protected health information.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(o)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(b)(1); 45 C.F.R. §164.308(b)(3); 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.504(e)(3)

Control Enhancement: 3

Justification to Select: Boundary protection devices protect systems containing PII from unauthorized access by individuals outside the organization. A firewall is such a boundary protection device.
Low, Moderate and High PII Confidentiality Impact Level Parameter Value:
… systems containing PII…

… a firewall or other network boundary protection device approved to prevent unauthorized access to the system…

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB M-07-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(1)

Control Enhancement: 5

Justification to Select: External network connections open up the opportunity for intentional as well as inadvertent disclosure of PII. E-mail and file sharing applications are common points of vulnerability. Organizations require the ability to evaluate external network connections on a case-by-case basis to ensure such connections do not permit unauthorized access or disclosure of PII.

Low, Moderate and High PII Confidentiality Impact Level Parameter Value:
… permit-by-exception…
… information systems containing PII…

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB M-07-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(1)

CA-6, SECURITY AUTHORIZATION

Justification to Select: One of the considerations for the "go/no go" decision when authorizing (or re-authorizing) an information system is whether applicable privacy requirements have been met.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Prior to authorizing an information system containing PII a privacy impact assessment must be completed.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance:
Related Controls: AR-2, AR-4, CA-5.

PHI Supplemental Guidance: The senior-level executive should be one of the following: HIPAA Security Officer, Authorizing Official, Program Manager, Information System Security Manager (ISSM), or Information System Security Officer (ISSO).

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: Pub. L. No. 107-347, §208; 5 U.S.C. §552a(e)(10)
PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii)

CA-7, CONTINUOUS MONITORING

Justification to Select: The state of security controls can directly correlate to privacy risk. Continuous monitoring supports the identification of issues that could result in unauthorized access to PII, data quality issues, and other privacy concerns that are supported by security controls (e.g., the controls in the Privacy Overlays).

Moderate and High PII Confidentiality Impact Level Supplemental Guidance:
Related Control: AR-4.

PHI Supplemental Guidance: Consider using automated tools and mechanisms for system activity review. The effectiveness of continuous monitoring of various activities, for example, failed or successful log-ins, inappropriate file access, detecting and reporting on malicious code/viruses through network transmission, is enhanced through the use of approved automated tools.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.308(a)(8)

CA-8, PENETRATION TESTING

Justification to Select: Penetration testing is one method to ensure that security and privacy controls are operating as intended. The sensitivity of information that is at the high PII confidentiality impact level necessitates testing prior to authorization of the information system and periodically thereafter. The standard rules of engagement for penetration testing should be coordinated with the privacy office to address unintended disclosure of PII.

High PII Confidentiality Impact Level Supplemental Guidance:
When user session information and other PII is captured or recorded during penetration testing, ensure relevant privacy controls are addressed. Related Controls: AP-1, AP-2, TR-1, TR-2.

High PII Confidentiality Impact Level Parameter Value:
… prior to authorization of information system and periodically no less frequently than when a significant change to the information system occurs…
… information systems containing PII at the High PII confidentiality impact level…

High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b(3)

CA-9, INTERNAL SYSTEM CONNECTIONS

Justification to Select: Privacy requirements such as sharing and disclosure apply to internal systems and their connections as well as to external connections.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Include privacy requirements in the Information Connection Document (or equivalent such as an Interconnection Security Agreement or an Authority to Connect package), specifically addressing the collection authority, compatibility of purpose for use, and need for recipient of information to achieve specific business purpose. Documentation must also address responsibilities of the receiving information system for protecting PII. Related Controls: AC-3, UL-1, UL-2.

Moderate and High PII Confidentiality Impact Level Parameter Value: … information systems containing PII…

PHI Parameter Value: … information systems containing PHI…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b(3)(b)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1)

Control Enhancement: 1

Justification to Select: Control is necessary to confirm compliance with CA-9 prior to connection.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Security compliance checks may include an assessment, prior to initial connection, of specific components, e.g., printers, based on sensitivity of PII processed by that component. Any change to the components' security posture would require a re-verification of the configuration settings.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b(3)(b)

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.306(a); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1)

CM-3, CONFIGURATION CHANGE CONTROL

Control Enhancement: 6

Justification to Select: If encryption is used to protect PII or PHI, there must be a management process in place to ensure future access to such information.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: When encrypting PII, there must be management processes in place to ensure future access to such data. Related Controls: SC-8, SC-12, SC-13, SC-28.

PHI Supplemental Guidance: When encrypting PHI, there must be management processes in place to ensure future access to such data. Related Controls: SC-8, SC-12, SC-13, SC-28.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … … encryption of Low, Moderate, and High PII……

PHI Parameter Value: … encryption of PHI…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (e)(10); OMB M-06-16; OMB Circular A-130, Appendix I

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(2)(ii)

CM-4, SECURITY IMPACT ANALYSIS

Justification to Select: Security Impact Analyses examine changes to information systems and any information security ramifications. Any security impacts identified may also impact the implementation of privacy requirements.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: When analyzing changes to the information system, the impacts to privacy are also considered. If necessary, conduct a privacy impact assessment. Related Control: AR-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: E-Government Act of 2002 (Pub. L. No. 107-347), §208; OMB M-03-22

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(A); 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(8)

Control Enhancement: 1

Justification to Select: If the system contains PII, the test environment must have the same security controls as the operating environment.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: If PII is used in the test environment, then the same controls required for systems containing PII

must be applied to the test environment. Simulated PII information should be used to the maximum extent practicable when testing system functionality. Related Controls: SA-15(9), AP-2, AR-3, DM-2, DM-3,UL-1.

Moderate and High PII Confidentiality Impact Level Statutory/Regulatory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.

Control Enhancement: 2

Justification to Select: If a system change is made, verification of Privacy Overlay security control functions is required to ensure continued compliance with privacy-related statutes and regulations.

Moderate and High PII Confidentiality Impact Level Statutory/Regulatory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.

PHI Statutory/Regulatory Reference: 45 C.F.R. §164.308(a)(7)(ii)(D); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii)

CM-8, INFORMATION SYSTEM COMPONENT INVENTORY

Control Enhancement: 1

Justification to Select: Identifying any changes or updates to system inventories allow organizations to accurately track the equipment on which their information systems are run and maintains an accurate inventory of hardware and software used to collect and manage PHI. Maintaining a current inventory supports accountability controls and may also support breach response efforts.

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(iii)

CP-1, CONTINGENCY PLANNING POLICY AND PROCEDURES

Justification to Select: Contingency planning policy and procedures must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g. and 8(a)(1) and 8(b)(3).

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(7)(i)

CP-2, CONTINGENCY PLAN

Justification to Select: Contingency plans must take privacy applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

PHI Supplemental Guidance: The contingency plan for systems containing PHI must include:

1) Data backup plan,
2) Disaster recovery plan,
3) Emergency mode operation plan, and
4) Emergency access procedures.

Additionally, the decision to include the following is dependent on a risk analysis to determine if or to what extent these should be included in the contingency plan:

1) Testing and revision procedures,
2) Applications and data criticality analysis, and
3) Contingency operations (i.e., procedures that allow facility access in support of restoration of lost data.

Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130 7.g.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(7)(i)-(ii); 45 C.F.R. §164.310(a)(2)(i); 45 C.F.R. §164.312(a)(2)(ii)

Control Enhancement: 5

Justification to Select: Pursuant to the emergency mode operations plan and emergency access procedure mandated under HIPAA, this control is required for both provision of emergency services (a mission critical business function), and for protection of the security of PHI while operating in emergency mode.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(7)(ii)(C); 45 C.F.R. §164.312(a)(2)(ii)

Control Enhancement: 8

Justification to Select: This control addresses the HIPAA Security Rule requirement to assess the relative criticality of specific applications and data to facilitate a risk-based contingency plan.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(7)(ii)(E)

CP-4, CONTINGENCY PLAN TESTING

Justification to Select: Contingency plan tests and exercises should include an evaluation of the ability to meet privacy requirements in a contingency scenario as well as corrective measures to address any privacy risks identified.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(7)(ii)(D)

CP-9, INFORMATION SYSTEM BACKUP

Justification to Select: Backup copies of information need to be protected with the same level of security as if that information were being maintained on the original information system. Applicable controls necessary to achieve this and to protect confidentiality include encryption of the backup. Backing up information helps maintain the integrity of the data — a requirement of the Privacy Act and HIPAA.

Moderate and High PII Confidentiality Impact Level Control Extension: Use the encryption methodology specified in SC-13 to encrypt moderate and high PII confidentiality impact level information in backups at the storage location.

PHI Control Extension: Establish procedures that create a retrievable, exact copy of the PHI before any movement of information system equipment.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.; OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(7)(ii)(A) – (C); 45 C.F.R. §164.310(d)(2)(iv); 45 C.F.R. §164.312(c)(1)

CP-10, INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Justification to Select: Information system recovery and reconstitution is an important step to restoring both PII and PHI to an accurate state following execution of a contingency plan.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(5) and (e)(10); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(7)(ii)(B); 45 C.F.R. §164.308(a)(7)(ii)(C)

IA-2, IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Justification to Select: Implementing this control ensures unique identification of individual's account, preventing anonymous access to PII and providing appropriate access (e.g., need for the PII in the performance of the users official duties) for organizational users. HIPAA requires that organizations uniquely identify users and implement procedures to verify user identity.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b(3)(b)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.312(d);

Control Enhancement: 6

Justification to Select: Requiring multi-factor authentication to privileged accounts provides added assurance that a privileged user, who likely has elevated privileges with access to PII, has proven their identity during the authentication process. OMB Policy requires the use of two-factor authentication with one factor being separate from the computer itself. Multi-factor authentication provides heightened assurance of identity during the authentication process. OMB Policy requires the use of two-factor authentication with one factor being separate from the computer itself.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: A separate device would include a Common Access Card (CAC). This control is required when the network access is remote (from outside the organization controlled networks).

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1, §C

Control Enhancement: 7

Justification to Select: Requiring multi-factor authentication to non-privileged accounts provides added assurance that a non-privileged user, who has access to PII, has proven their identity during the authentication process. OMB Policy requires the use of two-factor authentication with one factor being separate from the computer itself. Multi-factor authentication provides heightened assurance of identity during the authentication process.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: This control is required for remote network access to information systems containing PII (from outside the organization controlled networks). A separate device could include a CAC.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1, § C

Control Enhancement: 11

Justification to Select: Required for remote access to PII. Multi-factor authentication provides heightened assurance of identity during the authentication process. OMB Policy requires the use of two-factor authentication with one factor being separate from the computer itself.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: A separate device could include a CAC. This control is required when the network access is remote (from outside the organization controlled networks). Related Control: SC-13.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1, § C

IA-3, DEVICE IDENTIFICATION AND AUTHENTICATION

Justification to Select: Implementing this control ensures that un-authenticated devices, e.g., mobile devices and personal laptop computers, are not able to make a connection to an information system containing PHI. HIPAA requires technical policies and procedures for systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights.

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(d)

IA-4, IDENTIFIER MANAGEMENT

Justification to Select: Identifiers are a critical and necessary function to confirm which people and devices are accessing PII. Using Social Security Numbers (SSNs) as identifiers may create the potential for unauthorized disclosure of the SSN, and linkage of that individual to other PII, as system identifiers are not protected with the same level of security as are database elements or passwords. In addition, collecting an individual's SSN may create notice requirements under the Privacy Act.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: SSNs, and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, PII is attributable to a unique individual.

PHI Supplemental Guidance: Identifier management must ensure that any access to, or action involving, PHI is attributable to a unique individual.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a (note §§7(a)(1)), (b), (e)(10) and (j); 44 U.S.C. §3518(c)(1)

PHI Regulatory/Statutory References: 45 C.F.R. § 164.308(a)(4); 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.312(d)

Control Enhancement: 3

Justification to Select: Identity proofing requirements support agencies in confirming the identity of system users before granting them access to any system that contains PII.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Identity proofing registration process is mandatory for Federal Employees, Contractors, and Service Members.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); Homeland Security Policy Directive (HSPD) No. 12; NIST FIPS 201-1

IA-5, AUTHENTICATOR MANAGEMENT

Justification to Select: Adequate security to insure confidentiality for an information system containing PII is achieved through the management of the authenticators permitting access to that system. Authenticator management includes periodically changing passwords or other identifiers (e.g., certification and signatures) to reinforce identity validation and adherence to administrative security policies as well as enforces a time-based restriction on access, all of which bound access to PII in some way, limiting exposure in the event a user account is compromised.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b) and (e)(10); Federal Information Security Management Act (P.L. No. 107-347, Title III) § 3547; OMB M-06-16; OMB M-07-16 Att. 1.C.
PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3); 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(d)

IA-6, AUTHENTICATOR FEEDBACK

Justification to Select: Restricting feedback from the authentication process limits ability of unauthorized users to compromise the authentication mechanisms for accounts that can access PHI.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(1)

IA-7, CRYPTOGRAPHIC MODULE AUTHENTICATION

Justification to Select: PII requires encryption in certain circumstances. As such, FIPS 140-2 applies, including requirements for authentication to cryptographic modules. FIPS 140-2 is the current standard for validating cryptographic modules or alternatively NSA-certified hardware-based encryption modules. Use of unapproved cryptographic modules potentially allows unauthorized access to the cryptographic module or underlying, encrypted PII. As such, all organizations must either use cryptographic modules which satisfy FIPS 140-2, including requirements for authentication, or NSA-certified hardware-based encryption modules.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Information systems containing PII must use FIPS 140-2 or NSA-approved cryptographic modules.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. If the risk analysis determines that encryption will be used then a FIPS 140-2 or NSA-approved cryptographic module is required. Related Controls: RA-3, SI-12.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16 Att. 1.C.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(2)(iv)

IA-8, IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Justification to Select: Similar to IA-2, this control requires information systems to uniquely identify and authenticate system users that are not part of the organization as well as processes that act on behalf of another organization. This means no one is provided anonymous access to PII and supports managing each user's appropriate access to PII.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References:

5 U.S.C. §552a(b) and (e)(10); Federal Information Security Management Act (P.L. 107-347, Title III) ; OMB Circular A-130, 7.g. and 8.b(2)(c)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(i)

IR-1, INCIDENT RESPONSE POLICY AND PROCEDURES

Justification to Select: Incidents involving PII or PHI have response requirements unique from other types of security incidents. Therefore, a breach notification and response policy for PII and PHI must be developed and implemented. Security incidents may involve PII or PHI and when they do the privacy office must be involved.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving PII. Related Control: SE-2.

PHI Supplemental Guidance: In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving PHI. Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
a. … Incident Response Team as required by OMB M-07-16…

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 2 and Att. 3

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(6)(i)

IR-2, INCIDENT RESPONSE TRAINING

Justification to Select: Those responsible for identifying and responding to a security incident must understand how to recognize when PII or PHI are involved so that they can coordinate with the designated privacy official.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-5.

PHI Supplemental Guidance: Related Control: AR-5.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16, Att. 1 and Att. 2; NIST SP 800-122

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(6)(i); 45 C.F.R. §164.530(b)(1)

IR-4, INCIDENT HANDLING

Justification to Select: A strategic, well-thought-out security incident response program will integrate with privacy incident and breach response where appropriate, with the two processes being mutually supportive.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: SE-2.

PHI Supplemental Guidance: Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-1, Att. 2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D

Control Enhancement: 3

Justification to Select: HIPAA requires administrative, physical and technical safeguards for the protection and access of PHI during an emergency or other occurrence.

PHI Control Extension: Organizations establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain PHI including procedures to enable continuation of critical business processes for the protection of PHI and for obtaining necessary PHI during an emergency. Additionally, HIPAA requires organizations to conduct a risk analysis to determine whether and to what extent they establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan in the event of an emergency.

PHI Parameter Values:
…… emergencies, vandalism, security incidents, or natural disasters……
… … reasonable and appropriate policies and procedures consistent with federal laws and regulations and organizational requirements……

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(7)(i); 45 C.F.R. §164.308(a)(7)(ii)(B); 45 C.F.R. §164.308(a)(7)(ii)(C); 45 C.F.R. §164.312(a)(2)(ii); 45 C.F.R. §164.310(a)(2)(i)

IR-5, INCIDENT MONITORING

Justification to Select: Tracking and documenting security and privacy incidents enables the organization to respond more effectively and evaluate both individual incidents and trends across incidents over time.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 2, A

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D

IR-6, INCIDENT REPORTING

Justification to Select: Security incident reporting for incidents that are also privacy incidents must comply with privacy reporting requirements set forth by OMB M-07-16.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Incidents involving PII must be reported to the appropriate incident response center, e.g., United States Computer Emergency Readiness Team (US-CERT) or Intelligence Community Security Coordination Center (IC SCC). Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
a. … as short a time as is possible, but in no case later than one hour, after discovery or detection for incidents involving PII…

b. … both the Privacy Incident Response Team and the appropriate incident response center, e.g., US-CERT or IC SCC, if the incident involves PII…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16, Att. 2, B.1; ICS 502-01
PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. §164.314(a)(2)(i)(C); 45 C.F.R. Part 164 Subpart D

IR-7, INCIDENT RESPONSE ASSISTANCE

Justification to Select: Security incident response resources and privacy incident and breach response resources must know which resources are available, and how and when to coordinate.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Incident response assistance for incidents involving PII may include use of the forensic, technical, policy, and legal expertise of the organization's Information Assurance Officers/Managers, Privacy Officers, Legal Counsel, external or internal IT help desks, and the organization's Computer Emergency Response Team (CERT), in investigating and remediating incidents. Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 3, B.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(6)(i)

IR-8, INCIDENT RESPONSE PLAN

Justification to Select: A strategic, well-thought-out security incident response program must integrate with privacy incident and breach response planning where appropriate, with the two processes being mutually supportive.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: In developing an incident response plan, ensure it incorporates guidance from the privacy office for the handling of incidents involving PII. Related Control: SE-2.

PHI Supplemental Guidance: In developing an incident response plan, ensure it incorporates guidance from the privacy office for the handling of incidents involving PHI. Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(6)C.F.R.

IR-10, INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Justification to Select: Instances of loss, theft, or compromise of PII may involve an information security related malicious code attack or intrusion. In such cases, the Integrated Information Security Analysis Team is the organization's subject matter experts best able to support the organization's PII incident response team required by OMB M-07-16. In addition to security implementers, developers, and operators; this internal team should also comprise of the Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy among others.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The integrated information security analysis team will support the organization's PII incident response team (as specified in OMB M-07-16) in all aspects of response to a security incident involving PII. Related Control: SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 3, B.

MA-1, SYSTEM MAINTENANCE POLICY AND PROCEDURES

Justification to Select: Privacy considerations should be included in system maintenance policy and procedures especially when the system contains information subject to the Privacy Act and/or HIPAA.

Moderate and High PII Confidentiality Impact Level Control Extension: System maintenance policy and procedures must ensure that contractors having access to records (i.e., files or data) maintained in a system of records are contractually bound to be covered by the Privacy Act.

PHI Supplemental Guidance: Procedures to facilitate the implementation of the system maintenance policy should include access control validation and accountability procedures.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(m); OMB Circular A-130 7.g.; FAR Parts 24.104, 39.105, and 52.224-1&2; 5 U.S.C. §552a(b), (e)(9)-(10), and (m)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.310(d)(2)(iii)

MA-2, CONTROLLED MAINTENANCE

Justification to Select: HIPAA requires organizations to apply reasonable and appropriate safeguards for the protection of PHI, including implementing policies and procedures to document repairs and modifications to the facility which are related to security.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.310(d)(2)(iii)

MA-4, NONLOCAL MAINTENANCE

Control Enhancement: 6

Justification to Select: Encrypting the communications channel when maintenance is performed remotely protects user credentials, PII, and other data as it travels "across the wire."

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-06-16, Action Item 2.2 and Step 3.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(ii)

MA-5, MAINTENANCE PERSONNEL

Justification to Select: This control requires that maintenance personnel and others that have physical access to an information system are properly authorized and/or supervised by someone that is authorized to access the system, protecting PII and other information from unauthorized use and disclosure.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: If maintenance personnel are contractors, then the organizations personnel responsible for contracting (such as the contracting officer (KO or CO), contracting officer representative (COR), or contracting officer technical representative (COTR)) or the program manager (PM) must ensure that contractors having access to records (i.e., files or data) from a system of records are contractually bound to be covered by the Privacy Act. Related Controls: SA-4, AR-3.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b), (e)(9)-(10), and (m); FAR Part 24.104, 39.105, and 52.224-1

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.310(d)(2)(iii)

MP-1, MEDIA PROTECTION POLICY AND PROCEDURES

Justification to Select: All employees and contractors with potential access to PII or PHI must be informed about all policies and procedures that protect the various media types used by an organization to protect any PII or PHI that may reside on the media.

Low, Moderate and High PII Confidentiality Impact Level Parameter Value:
a. … employees and contractors with potential access to PII……

PHI Parameter Value:
a. … employees and contractors with potential access to PHI……

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1 and Att. 4

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.310(d)(1)

MP-2, MEDIA ACCESS

Justification to Select: Restricting access to digital and non-digital media, including mobile devices with storage capabilities, protects PII from unauthorized use and

disclosure. A risk assessment should be conducted to determine what PII, if any, can be stored on certain media types and who is authorized to do so.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
… any digital or non-digital media containing PII……
… authorized individuals with a valid need to know…

PHI Parameter Values:
… any digital or non-digital media containing PHI……
… authorized individuals with a valid need to know…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: E-Government Act of 2002 (Pub. L. No. 107-347) § 208; OMB M-03-226, Att.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(c); 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.312(c)(1)

MP-3, MEDIA MARKING

Justification to Select: To enable individuals to appropriately protect media containing PII or PHI, that media (or its container) must be marked to specify the contents, applicable protections (i.e. distribution limitations, handling caveats, and applicable security markings), or both, for the information therein.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Media containing PII, or the container for the media if labeling the media is not practicable, shall be marked appropriately.

PHI Supplemental Guidance: Media containing PHI, or the container for the media if labeling the media is not practicable, shall be marked appropriately.
Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(c); 45 C.F.R. §164.310(d)(1)

MP-4, MEDIA STORAGE

Justification to Select: Controlling the storage of media containing PII protects the media from theft and promotes accountability.

Low, Moderate and High PII Confidentiality Impact Level Parameter Value:
a. … removable media that contains PII……
… any securable area or in a locked container……

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(c); 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(iv)

MP-5, MEDIA TRANSPORT

Justification to Select: Protecting and controlling media containing PII, commensurate with the sensitivity of the PII contained on the media, during transport outside of controlled areas promotes accountability and limits situations that make the media vulnerable to unauthorized use and disclosure through loss, theft, or other mishandling.

Low, Moderate and High PII Confidentiality Impact Level Parameter Value:
a. … digital media that contains PII……
… NSA-approved or FIPS-validated encryption…

PHI Parameter Value:
a. … digital media that contains PHI……
… NSA-approved or FIPS-validated encryption…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16, Att. 1, C.; OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(iii); 45 C.F.R. §164.312(c)(1)

Control Enhancement: 4

Justification to Select: Encrypting portable media and mobile devices protects confidentiality and integrity of PII stored on those devices.

PHI Supplemental Guidance: Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16, Att. 1, C.; OMB M-06-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(iv)

MP-6, MEDIA SANITIZATION

Justification to Select: Properly sanitizing media that contains PII prior to disposal or release protects PII from unauthorized use and disclosure.

Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: DM-2.

Moderate and High PII Confidentiality Impact Level Parameter Value:
a. … digital media that contains PII……
… NSA-approved or FIPS-validated media sanitization techniques or procedures…

PHI Parameter Value:
a. … digital media that contains PHI……
… NSA-approved or FIPS-validated media sanitization techniques or procedures…

Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g.; OMB M-07-16, Att. 1, C.

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(i);45 C.F.R. §164.312(d)(2)(ii)

Control Enhancement: 1

Justification to Select: Tracking, documenting, and verifying media sanitization and disposal actions for media that contains PII reduces the risk of unauthorized disclosure of PII and PHI, and increases accountability.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: DM-2.

PHI Supplemental Guidance: Related Control: DM-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g.; OMB M-07-16, Att. 1, C.

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.312(d)(2)(ii)

Control Enhancement: 8

Justification to Select: If a smart device containing PII is lost or stolen, most such devices now permit the organization to specify either remote memory and data wipe when the smart device is reported lost or stolen, and/or implementing a limited number of unsuccessful login attempts before the smart device wipes its memory and clears its contents.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Organizations shall consider the use of this control for moderate and high PII confidentiality impact level information on devices such as mobile devices like an iPad or other smart device. If your organization permits use of personal smart devices (for example, BYOD), the organization must evaluate methods to ensure this control is enforced or that compensating controls are in place. Related Controls: DM-2, SE-2.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g.

MP-7, MEDIA USE

Justification to Select: Personally owned mobile devices and other personal media exist outside the boundaries of organization owned information systems, which limits the ability of organizations to control how PII is handled. Therefore controlling what may be placed on a personally owned mobile device reduces organizational risk.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: This control applies to devices containing PII, particularly portable storage and mobile devices. Related Control: SE-2.

Moderate and High PII Confidentiality Impact Level Parameter Value:
… restricts…
… portable storage and mobile devices…
… information systems and networks containing PII, without…
… device ownership, media sanitization and encryption controls…
Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g.

Control Enhancement: 1

Justification to Select: The ability to identify the owner of removable media that stores PII assigns accountability and responsibility managing the media and responding to a privacy breach.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 4

MP-8, MEDIA DOWNGRADING

Control Enhancement: 3

Justification to Select: Prior to public release of any media containing PII or PHI, that media must be reviewed to ensure that the PII and PHI have been appropriately redacted or de-identified and any file containing PII or PHI on that media is appropriately sanitized so that the PII or PHI is not recoverable or re-identifiable.

PHI Supplemental Guidance: Downgrading of media containing PHI must implement HIPAA de-identification procedures to ensure PHI may not be re-identified.

Moderate and High PII Confidentiality Impact Level Parameter Values:
… PII…

PHI Parameter Values:
… PHI…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); 5 U.S.C. §552 (b)(6); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.514

PE-1, PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Justification to Select: Sensitivity of PII may impact the necessary physical and environmental controls. Physical controls are important for protecting PII against unauthorized access, use, and disclosure. Environmental controls can be critical when PII has high availability requirements (e.g., core mission capabilities of an organization rely on consistent and frequent access to PII).

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.310(a)(2)(iii)

PE-2, PHYSICAL ACCESS AUTHORIZATIONS

Justification to Select: Maintaining a current list of personnel that are authorized to access facilities where PII is located protects PII from unauthorized access.

PHI Supplementary Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii)

Control Enhancement: 1

Justification to Select: Implementing role-based access controls for physical access provides a further level of granularity in governing who can access facilities, and even certain parts of facilities, that store and process PHI.

PHI Supplementary Guidance: The authorization of physical access to the facility should include considerations of whether the person needs access to PHI and whether such access is permitted under the HIPAA Privacy Rule.

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(iii)

PE-3, PHYSICAL ACCESS CONTROL

Justification for Selection: Employing physical access controls that limit access to a facility that are commensurate with the level of sensitivity of the PII processed in a facility protect the PII from unauthorized access, use, and disclosure.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g.

PHI References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(c)

PE-4, ACCESS CONTROL FOR TRANSMISSION MEDIUM

Justification for Selection: Protecting physical access to transmission medium protects the confidentiality of PII by protecting it from eavesdropping, the integrity of PII by protecting it from modification (when unencrypted), and protects the availability of PII by helping to prevent accidental or intentional damage or disruption to transmission lines.

PHI Supplementary Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SC-7(14), SI-12.

PHI References: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.310(c)

PE-5, ACCESS CONTROL FOR OUTPUT DEVICES

Justification for Selection: Controlling physical access to output devices, such as monitors, printers, and audio devices, protects PII from unauthorized access.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The access controls applied to output devices should be commensurate with the PII confidentiality impact level. For example, human resource information is only sent to printers located in secured locations such as a locked suite.

PHI Supplemental Guidance: Related Controls: RA-3, SI-12.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.

PHI References: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(c)

PE-6, MONITORING PHYSICAL ACCESS

Justification for Selection: Monitoring physical security incidents could identify PII incidents or breaches.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Reference: 45 C.F.R. §164.308(a)(6)(i); 45 C.F.R. §164.310(a)(2)(iii)

PE-8, VISITOR ACCESS RECORDS

Justification for Selection: Visitor access records provide a history of who had access to facilities in the event of a privacy incident or breach.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. When implemented, records should be retained in accordance with the organization's records retention schedule. Related Controls: RA-3, SI-12.

PHI Reference: 45 C.F.R. §164.310(a)(2)(iii)

PE-17, ALTERNATE WORK SITE

Justification for Selection: PII collected, stored, and processed at alternate worksite is subject to the same laws, regulations, and policies as PII handled at "non-alternate facilities." Adequate security and privacy controls commensurate with the risk to PII at the alternate work site must be implemented.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: PII collected, stored, and processed at alternate worksite is subject to the same laws, regulations, and policies as PII handled at "non-alternate facilities."

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16, Att. 1 and Att. 4; OMB M-11-27

PE-18, LOCATION OF INFORMATION SYSTEM COMPONENTS

Justification for Selection: Organizations must consider the location and placement of information system components that either store or display PII and place components in a manner to decrease the risk of unauthorized disclosure.

High PII Confidentiality Impact Level Supplemental Guidance: This control is required to limit intentional and unintentional disclosures of PII in violation of the Privacy Act. One example of an information system component requiring this control would be monitors and ensuring proper placement of the monitors will prevent unauthorized viewing. Another example of an information system component would be servers and disk arrays and location would include ensuring these are in a secured space.

PHI Supplementary Guidance: This control is required to limit intentional and unintentional disclosures of PHI in violation of the HIPAA Privacy and Security Rules.

High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10)

PHI References: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.310(c)

PL-1, SECURITY PLANNING POLICY AND PROCEDURES

Justification for Selection: Security planning addresses the privacy requirements for confidentiality, availability, and integrity for the organization and individual information system(s).

PHI Control Extension: The organization retains the policies and procedures in written form (which may be electronic) for 6 years from the date of its creation or the date when it was last in effect, whichever is later. The organization makes the documentation available to those persons responsible for implementing the procedures to which the document pertains.

PHI References: 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(i); 45 C.F.R. §164.316(b)(2)(ii)

PL-2, SYSTEM SECURITY PLAN

Justification for Selection: The system security plan (SSP) is necessary for the information system to be authorized. As the security controls section of a privacy impact assessment or other privacy documentation may not provide sufficient details to determine which controls have been implemented, the SSP and plan of action and milestones (POAM, see PM-4) are the best locations to address privacy related security controls.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The system security plan (SSP) must provide the security category and the PII confidentiality impact level of the system (as described in NIST SP 800-122), describe relationships with, and data flows of, PII to other systems, provides an overview of security and privacy requirements for the system, including the security controls within the Privacy Overlays. The SSP must define the boundary within the system where PII is stored, processed, and/or maintained. The person responsible for meeting information system privacy requirements must provide input to the SSP.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: PM-4.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: E-Government Act of 2002 (Pub. L. No. 107-347) § 208; OMB M-03-22; OMB M-07-16 Att. 1, A.2.

PHI References: 45 C.F.R. §164.306(a); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.310; 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii)

PL-4, RULES OF BEHAVIOR

Justification for Selection: Rules of behavior govern expectations of system users for systems that handle PII.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Pursuant to OMB M-07-16, organizational rules of behavior must include a policy outlining the rules of behavior to safeguard personally identifiable information (PII) and identifying consequences and corrective actions for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of PII involved.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-5.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9); OMB M-07-16, Att. 1, A.2. and Att. 4

PL-8, INFORMATION SECURITY ARCHITECTURE

Justification for Selection: The information security architecture identifies security and privacy controls necessary to support privacy requirements. The Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO) are the best resource for identifying privacy requirements and privacy controls.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-7.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. 107-347) § 208; OMB M-03-22

PS-1, PERSONNEL SECURITY POLICY AND PROCEDURES

Justification for Selection: Roles that require access to certain types of PII may require additional personnel security measures beyond those applied to the general workforce of an organization.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The personnel security policies and procedures shall address the different levels of background investigations, or other personnel security requirements, necessary to access different levels of PII.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 4; OMB Circular A-130, 7.g. and 8.a.1(f)

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii)

PS-2, POSITION RISK DESIGNATION

Justification for Selection: Position risk designations, for different levels of access to PII, should be commensurate with the risks associated with the PII confidentiality impact level.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Whether a member of the workforce will be working with PII is a factor in determining the screening criteria for working in the position.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-06-16; OMB M-07-16Att. 4

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(B)

PS-3, PERSONNEL SCREENING

Justification for Selection: Screening individuals who are provided access to PII, and re-screening as deemed appropriate by the organization, reduces risk.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Individuals that work with PII are screened prior to being provided access to the PII and re-screened as determined by the organization.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate. High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 C.F.R. 731.106

PHI Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(B)

Control Enhancement: 3

Justification for Selection: Access to PII and PHI requires both a valid need to know as documented by an access authorization request, and requires a background investigation (or appropriate screening) to ensure the individual being provided access is suitable.
Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-5.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII …

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 C.F.R. §731.106

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(B)

PS-4, PERSONNEL TERMINATION

Justification for Selection: This control governs termination procedures for access to PII and other information

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: PL-4.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b)(1); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(C)

PS-5, PERSONNEL TRANSFER

Justification for Selection: When personnel are reassigned or transferred, their access to PII must be reviewed to determine whether and how their access permissions should change.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Individuals that work with PII are screened prior to being provided access to the PII and re-screened as determined by the organization.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.
Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b)(1) and (e)(10)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(B)

PS-6, ACCESS AGREEMENTS

Justification for Selection: Access agreement documentation notifies users and organizations of their respective responsibilities regarding authorization for access to, rules of behavior, and handling of PII. This documentation provides a legal mechanism for holding individuals accountable for their actions.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Examples of access agreement documents required for access to PII may include access authorization requests, nondisclosure agreements, acceptable use agreements, privacy training and awareness, and rules of behavior. Related Controls: AC-2, PS-3, AR-5,PL-4.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1, A.2. and Att. 4

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(d)(2)(iii); 45 C.F.R. §164.314(a).

PS-7, THIRD-PARTY PERSONNEL SECURITY

Justification for Selection: This control ensures that third-party service providers that will have access to PII are held accountable in the same way the organizational personnel are.

Low, Moderate, High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-3.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(m); OMB Circular A-130, 7.g. and 8.a.1(f), FAR Parts 24.1, 39.105, and 52.224-1&2

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(b)(1); 45 C.F.R. §164.314(a)

PS-8, PERSONNEL SANCTIONS

Justification for Selection: Applying clear and consistent sanctions for mishandling of PII demonstrates a degree of organizational accountability for meeting applicable privacy requirements.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The organization employs a formal sanctions process for individuals failing to comply with established privacy policies and procedures.

Low, Moderate, High PII Confidentiality Impact Level Supplemental Guidance: If the personnel sanctions are associated with the loss, theft, or compromise of PII, additional care must be taken to prevent further privacy breach. When providing notice of sanctions, do not provide the PII involved in the incident to anyone without an explicit need to know. Unless the individual needs the specific PII elements breached to perform their job function, the individual does not need to know the PII. Instead, provide characterization of the type(s) of PII breached, e.g., provide "Full Name" instead of providing "John Doe," or "Blood Type" instead of "A positive."

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9); OMB M-07-16, Att. 2, A.2. and Att. 4

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(1)(ii)(C)

RA-1, RISK ASSESSMENT POLICY AND PROCEDURES

Justification for Selection: Formal risk assessment processes and policies provide the foundation for implementation of the security controls required for protecting PII.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Organization risk assessment policy and procedures shall incorporate the requirements to conduct information system privacy risk management processes across the life cycle of an information system collecting, using, maintaining, and/or disseminating PII. Related Control: AR-2; PM-2.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The privacy office (SAOP/CPO) should be consulted with in developing risk assessment policy and procedures to cover information systems containing PII.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB Circular A-130, 7.g. and 8.b.(3)(b); OMB M-07-16 Att. 1, A.2.; OMB M-05-08

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.316(a)

RA-2, SECURITY CATEGORIZATION

Justification for Selection: A determination of security categorization is based in part on whether the information is PII, or the system contains PII, and is a fundamental determination for implementing security controls. See Section 2.5 above.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Involve the SAOP, the CPO, or their designee when conducting the security categorization process for information systems containing PII or PHI.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16, Att. 1, A.2 ; OMB M-06-16; OMB M-14-04

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(1)(ii)(A); 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(7)(ii)(E)

RA-3, RISK ASSESSMENT

Justification for Selection: A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of PII. Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by enabling the organization to identify, evaluate, and manage the privacy risks for the PII in that system. The content of the privacy risk assessment performed under this

control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing PII.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Include an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PII in the related risk assessment documentation.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance:
Related Control: AR-2

PHI Supplemental Guidance: The Department of Health and Human Services has issued Final Guidance on Risk Analysis (Assessment) under the HIPAA Security Rule (see http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf)

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
b. … an evaluation of risks associated with the potential impact of loss of the PII must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings…

PHI Parameter Values:
b. … a HIPAA Risk Analysis, and associated risks to PHI must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings. All HIPAA Risk Analysis documentation must be maintained for 6 years from the date of creation or date it was last in effect – whichever is later…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB Circular A-130, 7.g. and 8.b.(3)(b); M-07-16, Att. 1, A.2; M-06-16; M-05-08;

PHI References: 45 C.F.R. §164.308(a)(1)(ii)(A); 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.316(a)

SA-2, ALLOCATION OF RESOURCES

Justification for Selection: Resources must be considered for the protection of privacy and confidentiality when budgeting for an information system.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension:
As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of PII in the information system.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References:
E-Government Act of 2002 (Pub. L. No. 107-347), § §208; OMB Circular A-130, 7.g. and 8.b(3)(b)

SA-3, SYSTEM DEVELOPMENT LIFECYCLE

Justification for Selection: Managing an information system through a defined lifecycle process helps to ensure that privacy controls are appropriately considered from the initial system conception and requirements development, to verification of implemented requirements, and through decommissioning.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: To ensure that privacy and security controls are appropriately considered during each phase of the System Development Life Cycle (SDLC), both the security and privacy offices should have a clear understanding of the requirements to protect PII. The privacy office should participate throughout the SDLC.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130

SA-4, ACQUISITION PROCESS

Justification for Selection: Contracts for information systems, components, or services must meet the privacy requirements of the Federal government and it is much easier, and cheaper, to build privacy into a system at the acquisition phase of the life cycle than it is to bolt it on after the system is already acquired.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension:
When acquiring information systems, components, or services used to store, process, or transmit PII, ensure the following, in consultation with the privacy office, are included in the acquisition contract:

h. List of security and privacy controls from the Privacy Overlays necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements.
i. Privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior.
j. Privacy functional requirements, i.e., functional requirements specific to privacy.
k. FAR Clauses per FAR Part 24 and Part 39.105, and any other organization specific privacy clause

PHI Control Extension: When acquiring information systems, components, or services used to store, process, or transmit PHI, in addition to the requirements for PII, ensure the following in consultation with the privacy office:

l. Necessary memorandum of understanding, memorandum of agreement, or other data sharing agreement are obtained.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance:
Related Control: AR-7.

Low, Moderate, High PII Confidentiality Impact Level Regulatory/Statutory References:

5 U.S.C. §552a(m) and (e)(10); OMB Circular A-130, 7.g. and Appendix 1; E-Government Act of 2002 (I; Pub. L. No. 107-347) §208; Federal Information Management Security Act (Pub. L. No. 107-347); FAR Part 24 and 39.105

PHI Reference: 45 C.F.R. §164.314(a)

SA-8, SECURITY ENGINEERING PRINCIPLES

Justification for Selection: Considering the privacy requirements of an information system during the design phase of the life cycle ensures the most cost effective and efficient implementation of security and privacy controls.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: When applying information system security engineering principles in the specification, design, development, implementation, and modification of an information system containing PII, the organization should apply privacy-enhanced system design and development principles described in NIST SP 800-53, Rev. 4, Appendix J.
Related Control: AR-7.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: E-Government Act of 2002 (Pub. L. 107-347) § 208; OMB Circular A-130 7.g.; OMB M-05-08; OMB M-03-22

SA-9, EXTERNAL INFORMATION SYSTEM SERVICES

Justification for Selection: External information system service providers must meet the same privacy requirements as applied to internal services so that PHI has the equivalent level of protection regardless of where it is.

PHI Subset Control Extension: The information security requirements and controls are documented through a written contract, or other arrangement that meets the requirements of 45 C.F.R. §164.314(a). This guidance is not intended to cover the acquisition of services of all third party providers, only those who rise to the level of a business associate of a covered entity.

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(b)(1); 45 C.F.R. §164.314(a)

Control Enhancement: 5

Justification for Selection: Other countries have different requirements for the protection of PII of either their own citizens or for transfer of PII across national borders. When selecting a service provider, the location for storage, maintenance, or processing must be considered. Some organizations, such as European Union member states, have very stringent data transfer restriction requirements and your organization may have a treaty or other agreement for data exchange and/or protection. Consult with your legal counsel or your organization's liaison to the Department of State.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: If the service provider will be maintaining PII outside of the United States the organization must evaluate the legal environment of the country in which the information will be maintained to ensure US equities are protected. If the service provider is located in the US and the PII is about non-US Citizens, then the organization must address the data transfer requirements of the country whose citizens PII is collected or maintained and must ensure that country's privacy/data protection legal requirements are met. Coordinate with your organization's legal counsel, privacy office, and Department of State representative in meeting this requirement.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AP-1, AP-2, UL-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g., 9.b and 9.c.

SA-11, DEVELOPER SECURITY TESTING AND EVALUATION

Justification for Selection: Testing is a key method to ensure privacy controls are implemented. Including privacy controls in the security assessment plan ensures they are tested.

Moderate and High PII Confidentiality Impact Level Control Extension:
For information systems containing PII, the organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan that includes assessment of privacy controls.
b. In testing:
    1. minimize to the use of PII to the maximum extent practicable.
    2. only conduct testing with actual PII if a formal MOA, MOU, or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system including how loss, theft, or compromise (i.e., breach) of PII is to be handled.
    3. de-identify or anonymize PII to the maximum extent practicable.
    4. coordinate use of PII with the privacy office before conducting any testing.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance:
Related Control: AR-7.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References:
5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. No. 107-347), §208, and Title III; OMB Circular A-130, 7.g.; OMB M-03-22

Control Enhancement: 5

Justification for Selection: To implement penetration testing identified in CA-8.

High PII Confidentiality Impact Level Control Extension:
If the system contains PII, then the penetration testing requirements of CA-8, as specified above in this overlay, shall be applied.

High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b.(2)(c)(iii)

SA-15, DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control Enhancement: 9

Justification for Selection: Preproduction environments may not be as formally controlled as production environments. Use of PII in a preproduction environment increases risk to the organization because the preproduction environment may not be as secure as the production environment.

Moderate and High PII Confidentiality Impact Level Control Extension:
Before use of live data containing PII in a preproduction environment, the organization shall:

a. Implement policies and procedures in coordination with the privacy office for evaluating the risk of use of PII in a preproduction environment.
b. Protect, per NIST SP 800-122, the PII within the preproduction environment at the same level as in the production environment.
c. Use anonymized data substitution (See NIST SP 800-122, Section 4.2.4) if possible.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance:
If PII will be provided to a third-party during testing, the organization will need a formal MOA, MOU, or data exchange agreement before providing access to that third-party. Such agreement will at a minimum include how loss, theft, or compromise of PII is to be handled. Related Controls: SA-9, DM-1(1), DM-3, UL-2.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference:
5 U.S.C. §552a(b) and (e)(10); NIST SP 800-122

SA-17, DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Justification for Selection: The security architecture and design identifies security and privacy controls necessary to support privacy requirements. The SAOP or CPO are the best resource for identifying privacy requirements and privacy controls.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension:
The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture

that accurately and completely describes the privacy requirements, and the allocation of security and privacy controls among physical and logical components.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-7.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: E-Government Act of 2002 (Pub. L. No. 107-347) Title III; 5 U.S.C. §552a(e)(10); OMB M-05-08

SA-21, DEVELOPER SCREENING

Justification for Selection: Access to PII and PHI requires both a valid need to know as documented by an access authorization request, and requires a background investigation (or appropriate screening) to ensure the individual being provided access is suitable. These access authorization requirements extend to developers of information systems containing PII and PHI.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-5.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value:

… systems containing PII……

a. … contracting officer and contracting officer representative, in consultation with the organization's privacy office……

b. … … organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 C.F.R. §731.106

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(ii)(B)

SC-2, APPLICATION PARTITIONING

Justification for Selection: It is necessary to store PII on separate logical partitions from applications and software that provide user functionality in order to restrict accidental or unintentional loss of, or access to, PII by both unauthorized users and unauthorized applications.

Moderate and High PII Confidentiality Impact Level Control Extension:

In any situation where PII is present, PII shall be stored on a logical or physical partition separate from the applications and software partition.

PHI Control Extension: Apply the Moderate and High PII Confidentiality Impact Level Control Extension.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g. and 8.b.(3)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(1)

SC-4, INFORMATION IN SHARED RESOURCES

Justification for Selection: Shared system resources include, among other things, memory and disk caches. To protect against unauthorized or unintended access to PII, purging of these shared system resources minimizes the risk of such access. For example, ensuring that the clipboard in Windows(TM) is emptied or restricted when access or using PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Following use of a shared system resource, ensure that shared system resource(s) is purged of PII to prevent unintended users or processes from accessing PII.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b.(3)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(1)

SC-7, BOUNDARY PROTECTION

Control Enhancement: 14

Justification for Selection: System interfaces can provide access to the data flows involving PHI. HIPAA has heightened security requirements to protect these interfaces.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: PE-4, RA-3, SI-12.

PHI Parameter Values:
… those organization-defined managed interfaces necessary to prevent unauthorized physical access, tampering, and theft of PHI……

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(i)

SC-8, TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Justification for Selection: Because of the sensitivity of PII and PHI, the confidentiality and integrity of such information in transit must be assured.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-4.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … confidentiality and integrity…

PHI Parameter Values: … confidentiality and integrity…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (10); OMB Circular A-130, 7.g. and Appendix 1; E-Government Act of 2002 (I; Pub. L. No. 107-347), Title III

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(1)

Control Enhancement: 1

Justification for Selection: Because of the sensitivity of PII, the confidentiality and integrity of such information in transit must be assured with encryption techniques if assurance is not provided by other means.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: PII must be protected by NSA-approved or FIPS-validated encryption to ensure the information's confidentiality and integrity during transmission.

PHI Supplemental Guidance:
Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
… prevent unauthorized disclosure of PII…
… physical safeguard measures to prevent unauthorized access to or alteration of the PII contained therein……

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (10); E-Government Act of 2002 (Pub. L. No. 107-347), Title III; OMB Circular A-130, 7.g. and Appendix 1; OMB M-07-16, Att. 1, C.; OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(c)(2); 45 C.F.R. §164.312(e)(2)(i)

Control Enhancement: 2

Justification for Selection: Because of the sensitivity of PII, the integrity of information in transit must be assured at all points during aggregation, packaging and transformation.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AC-13.

Moderate and High PII Confidentiality Impact Level Parameter Values: … confidentiality and integrity…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (10); OMB Circular A-130, 7.g. and 8.b.(3) and Appendix 1; OMB M-07-16, Att. 1, C.; OMB M-06-16

SC-12, CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Justification for Selection: Because cryptography is required to protect PII and PHI, cryptographic key establishment and management must be performed in such a way that even the loss of keys will not permit access to the PII or PHI.

PHI Supplemental Guidance: Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. Related Controls: RA-3, SI-12.

Low, Moderate, High PII Confidentiality Impact Level Parameter Values: …centralized management of key generation, distribution, storage, access, and destruction in accordance with NIST SP 800-55 and NIST SP 800-57…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); E-Government Act of 2002 (Pub. L. No. 107-347), Title III; OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(e)(2)(ii)

SC-13, CRYPTOGRAPHIC PROTECTION

Justification for Selection: NSA-approved and FIPS-validated cryptographic modules are the government standard for encryption. When PII requires encryption the organization must comply with these standards.

PHI Supplemental Guidance: Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. Related Controls: RA-3, SI-12.

Low, Moderate, High PII Confidentiality Impact Level Parameter Values:
… … either FIPS-validated or NSA-approved cryptography to ensure the confidentiality and integrity of PII in transit or at rest…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-07-16, Att. 1, C; OMB M-06-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii)

SC-28, PROTECTION OF INFORMATION AT REST

Justification for Selection: Because of the sensitivity of PII and PHI, the confidentiality and integrity of such information must be assured for data at rest.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: SC-13.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
… confidentiality and integrity…
… PII…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB M-06-16; OMB M-07-16, Att. 1, C.

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii)

Control Enhancement: 1

Justification for Selection: Because of the sensitivity of PII and PHI, the confidentiality and integrity of such information must be assured for data at rest through the use of encryption technologies if assurance is not provided by other means.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Organizations must:

1. Encrypt data at rest in mobile devices for confidentiality to protect against loss, theft, or compromise.
2. Encrypt data stored in network share drives to insure confidentiality.
3. Encrypt storage/back-up data where physical protection is either not available, not implemented, or not audited.
4. Encrypt PII in a database.
5. Encrypt data stored in the cloud — whether or not the cloud is government or private.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Organizations may use file share scanning (e.g., DLP technology) to ensure compliance with the requirement to encrypt PII/PHI at rest. Related Control: AC-13.

PHI Supplemental Guidance: Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized. Related Controls: RA-3, SI-12.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b) and (e)(10); OMB M-06-16; OMB M-07-16 Att. 1, C.

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii)

SI-1, SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Justification for Selection: Policies that support protecting the integrity of systems and information are necessary to meet the Privacy Act requirements to protect against any anticipated threats or hazards to the security or integrity of records.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b)and (e)(10); OMB M-07-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(c)(1)

SI-3, MALICIOUS CODE PROTECTION

Justification for Selection: Malicious code protections are essential in system with PII because of the sensitivity and desirability of such information.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R. §164.308(a)(6)(ii)

SI-4, INFORMATION SYSTEM MONITORING

Justification for Selection: Monitoring of systems may capture PII transacted during the monitoring period. While information system monitoring is necessary to protect the security of the organization's information and information systems, it must be done in a way that protects the privacy of individuals and the data captured during monitoring.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Intrusion-monitoring tools may collect PII of all types. Notice to users who are monitored should be provided prior to system use. Controls sufficient to protect the type of PII collected must be in place for the technology performing the monitoring, including encryption of monitoring data that may contain PII. When conducting information system monitoring on internal or external networks which may collect PII, the organization should coordinate with the organization's counsel and privacy officer.

Low, Moderate, and High PII confidentiality impact level Regulatory/Statutory References: 5 U.S.C. §552a(b), (e)(10); OMB Circular A-130, 7.g.; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R. §164.308(a)(6)(ii)

SI-5, SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Justification for Selection: Receiving and acting on security alerts from US-CERT, or other appropriate organizations, assists in protecting PHI by protecting information systems against rapidly evolving threats.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(5)(ii)(A)

SI-7, SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Justification for Selection: Detection of unauthorized changes to PII and systems containing PII is fundamental to ensuring integrity as required by the Privacy Act.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values: … PII…

PHI Parameter Values: … PHI…

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) ; OMB M-04-04; OMB Circular A-130, 7.g., and Appendix II

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(c); 45 C.F.R. §164.312(e)(2)(i)

Control Enhancement: 6

Justification for Selection: Detection of unauthorized changes to PII and systems containing PII is fundamental to ensuring data integrity. NSA-approved or FIPS-validated cryptographic modules are the government standard for integrity verification. When PII requires integrity verification the organization must comply with these standards.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Either FIPS-validated or NSA-approved cryptography shall be used to detect unauthorized changes to software, firmware, and information.

PHI Supplemental Guidance: Under HIPAA, encryption is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. Related Controls: RA-3, SI-12.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(10); OMB M-07-16, Att. 1, C; OMB M-04-04; OMB Circular A-130, 7.g. and Appendix II

PHI Regulatory/Statutory References: 45 C.F.R. §164.312(c); 45 C.F.R. §164.312(e)

SI-8, SPAM PROTECTION

Justification for Selection: HIPAA requires organizations to implement procedures for guarding against, detecting and reporting malicious software which can be introduced to the system through spam.

PHI Supplemental Guidance: Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization. Related Controls: RA-3, SI-12.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R. §164.308(a)(6)(ii)

SI-10, INFORMATION INPUT VALIDATION

Justification for Selection: Information input validation serves two important purposes for protecting PII: 1) when PII is entered, validation techniques support data quality measures (e.g., ensuring the PII entered is the expected type and format of data), and 2) it provides the capability to limit or exclude PII from being entered into a field (e.g., recognizing a restricted format, such as an SSN).

Moderate and High PII Confidentiality Impact Level Parameter Values: … PII…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5), (e)(6), and (e)(10)

SI-11, ERROR HANDLING

Justification for Selection: An error in a system may reveal PII or PHI. For example, if there is an error posting a form that contains PII and the system includes the PII entered in the form when it writes to the error log, it will be visible to whoever has access permissions to the error log. Therefore, error handling must be considered in design of the system and access to errors containing PII or PHI should be provided only to those individuals with a need for that information in the performance of their duties.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
b. … authorized individuals with a need for the information in the performance of their duties…

PHI Parameter Values:
b. … authorized individuals with a need for the information in the performance of their duties…

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5) and (10); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(3)(i)

SI-12, INFORMATION HANDLING AND RETENTION

Justification for Selection: PII, even if not considered a "record" by statute, should be handled and retained in accordance with applicable regulatory requirements, organizational policies, industry best practices, and the FIPPs. Retention and handling of PII which meets the definition of a "record" as defined by the Federal Records Act (44 U.S.C. §3301) should be addressed in a records disposition schedule. For PII that meets the definition of a "record" as defined by the Privacy Act, for purposes of providing notice the associated SORN should reflect the retention period from the organization's applicable record retention schedule. PHI must be handled and retained in accordance with the HIPAA Security Rule as it has specific requirements for information handling and record retention.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: For PII maintained in a Privacy Act system of records, the corresponding record management requirements, including retention periods, must be addressed in the system of records notice (SORN).

PHI Control Extension: HIPAA requires that the following actions, activities, and assessments relating to the security of systems containing PHI be documented and retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later:

- Decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question;
- A user's right of access to a workstation, transaction, program, or process;
- Security incidents and their outcomes;
- Satisfactory assurances that a business associate will appropriately safeguard PHI. This documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements. If satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained;
- Repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); and
- Changes to organizational policies and procedures.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AP-2, DM-2,TR-2.

PHI Supplemental Guidance: Related Control: AC-21.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(4)

PHI Regulatory/Statutory References: 44 U.S.C. §3301, 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(i)

PM-1, INFORMATION SECURITY PROGRAM PLAN

Justification for Selection: Many parts of a privacy program rely on the organization having a sound information security program. Similarly, an information security program is informed by the requirements of a privacy program.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The organization's approach to protection of PII should be included in the information security program plan, including defining roles and responsibilities for protecting PII. Related Control: AR-1.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.; Federal Information Security Management Act (Pub. L. No. 107-347)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308 (a)(1)(i)

PM-2, SENIOR INFORMATION SECURITY OFFICER

Justification for Selection: Assigning security responsibilities to a senior official supports the HIPAA Security Rule.

PHI Control Extension: The organization must designate privacy and security officials responsible for the development and implementation of the policies and procedures required by HIPAA (45 C.F.R. parts 160 and 164).

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.530(a)

PM-3, INFORMATION SECURITY RESOURCES

Justification for Selection: Ensuring that information security is adequately resourced supports the implementation of all security-related privacy requirements.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: E-Government Act of 2002 (Pub. L. No. 107-347), §208

PM-5, INFORMATION SYSTEM INVENTORY

Justification for Selection: Maintaining a current information system inventory supports privacy by informing PII inventories, data flows, and generally assists in monitoring the maintenance and use of PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: SE-1.

PHI Supplemental Guidance: Information system inventory should govern the receipt and removal of hardware and electronic media that contains PHI.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: E-Government Act of 2002 (44 U.S.C. §3541); OMB M-07-16 Att. 1, B.1.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.310(d)

PM-7, ENTERPRISE ARCHITECTURE

Justification for Selection: Building privacy and security requirements into the Enterprise Architecture promotes the successful and consistent incorporation of information security and privacy practices into an organization's business activities, processes, and systems.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Reference the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) for additional information. Related Control: AR-7.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g.; Federal Information Management Security Act (Pub. L. No. 107-347)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(1)(i)

PM-9, RISK MANAGEMENT STRATEGY

Justification for Selection: A comprehensive risk management strategy includes privacy as an input where appropriate to ensure privacy risks to individuals and organizations are identified, prioritized, and managed consistently across the organization's business processes, programs, and systems.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The risk management strategy must include a process to evaluate and address privacy risks for individuals and information (data) such as risk to individual, risk to the system, risk to the organization, and risk to the enterprise. In addition to business risks that arise out of

privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

PHI Control Extension: The risk management strategy must include a process to evaluate and address privacy risks for individuals and PHI such as risk to individual, risk to the system, risk to the organization, and risk to the enterprise. In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB Circular A-130, 7.g.; OMB M-03-22; OMB M-06-16; OMB M-07-16, Att. 1, B.1 and Att. 2, A.1

PHI Regulatory/Statutory References: 45 C.F.R. §164.308(a)(1)(ii); 45 C.F.R. §164.316(a)

PM-10, SECURITY AUTHORIZATION PROCESS

Justification for Selection: The security authorization process provides a means for evaluating whether a system/process has met given privacy safeguards and documentation requirements.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements, such PIAs and SORNs when applicable, have been appropriately addressed prior to any security authorization.

PHI Control Extension: The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements have been appropriately addressed prior to any security authorization.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AR-2, AR-7, TR-1,TR-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); Pub. L. No. 107-347, §208; OMB Circular A-130, 7.g. and 8.b.(3)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(2)

PM-11, MISSION/BUSINESS PROCESS DEFINITION

Justification for Selection: The way an organization defines its mission/business processes will have different levels of impact on privacy risks stemming from those processes. Reviewing and revising mission/business processes until achievable privacy protections are obtained is vital to reducing risk.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: When defining mission/business processes for information security and identifying resulting risks, the organization must address the privacy risks stemming from those processes.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals. Related Control: AR-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g. and 8.b.(1)(b), 8.b.(2)(b), and Appendix IV

PHI Regulatory/Statutory References: 45 C.F.R. §164.306(a) and (b)

PM-12, INSIDER THREAT PROGRAM

Justification for Selection: The privacy risks inherent with amalgamating sensitive PII from a myriad of data resources within an organization, such as human resource and background investigation information, and the potential for scope creep require the active participation, review, and concurrence of the Privacy Officer.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: When defining the requirements for and designing an organization's insider threat program, the insider threat team must engage the participation, and obtain concurrence, of the organization's Privacy Officer prior to implementation. For existing insider threat programs, conduct a review of the program with the organization’s Privacy Officer to ensure program meets applicable privacy requirements.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5), (9), (10), ; E-Government Act of 2002 (Pub. L. No. 107-347), §208; OMB Circular A-130, 7.g.; OMB M-07-16

PM-14, TESTING, TRAINING, AND MONITORING

Justification for Selection: It is critical to integrate privacy risk management, compliance monitoring, and testing into the organizational risk management strategy and the associated testing and training requirements otherwise an important aspect of privacy may be overlooked.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Reviews testing, training and monitoring plans for consistency with the organizational privacy risk management strategy.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AR-4, AR-5, DM-3, SE-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; OMB Circular A-130, 7.g.; OMB M-07-16 Att.1, A.2.

PM-15, CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Justification for Selection: To maximize organizational compliance with privacy requirements and best practices, the organization should ensure its privacy professionals engage with both the organization's security community and the Federal privacy community to remain current and to share lessons-learned or other privacy-related information.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The organization establishes and institutionalizes contact for its privacy professionals with both the organization's security community and selected groups and associations within the Federal privacy community:
a. To facilitate ongoing privacy education and training for organizational personnel;
b. To maintain currency with recommended privacy practices, techniques, and technologies; and
c. To share current privacy-related information including threats, vulnerabilities, and incidents.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Ongoing contact with privacy groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Privacy groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of privacy professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
Related Control: AR-1.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; OMB Circular A-130, 7.g.; OMB M-07-16; OMB M-05-08

AP-1, AUTHORITY TO COLLECT

Justification for Selection: An organization identifies the legal authority permitting collection. Additional measures, including design choices, ensure the information system collecting, using, maintaining, or disseminating PII complies with those authorities permitting the collection.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Ensure PII collected, used, maintained, or disseminated by the information system is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; Pub. L. No. 107-347, §208

AP-2, PURPOSE SPECIFICATION

Justification for Selection: An organization identifies the authorized purpose(s) for collection, use, maintenance, or dissemination of PII. Additional measures, including, but not limited to, design choices and auditing, ensure the information system collecting, using, maintaining, or disseminating PII complies with those authorized purposes.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Ensure the PII collected, used, maintained, or disseminated by the information system adheres to the specific purpose(s) described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(3)(A)-(B); Pub. L. No. 107-347, §208(b)(2)(B)(ii) and (c)(1)(B)

AR-1, GOVERNANCE AND PRIVACY PROGRAM

Justification for Selection: Effective implementation of privacy and security controls requires a collaborative partnering of the SAOP (or CPO), Chief Information Officer (CIO), and Chief Information Security Officer (CISO). To maximize organizational compliance with privacy requirements and best practices, the organization should ensure its privacy professionals engage with both its security community and the Federal privacy community to remain current and to share lessons-learned or other privacy-related information.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Development of the strategic organizational privacy plan must be done in consultation with the CIO and CISO. The organization establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community:

a. To facilitate ongoing privacy education and training for organizational personnel;
b. To maintain currency with recommended privacy practices, techniques, and technologies; and
c. To share current privacy-related information including threats, vulnerabilities, and incidents.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Ongoing contact with privacy groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Privacy groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of privacy professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related Control: PM-15.

PHI Supplemental Guidance: HIPAA requires policies, procedures, and personnel designations to be documented and for organizations to monitor changes in law.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; 44 U.S.C. §3506 (a)(3) and (g); Pub. L. No. 107-347, §208; OMB Circular A-130, 7.g.; OMB M-07-16; OMB M-05-08

PHI Regulatory/Statutory References: 45 C.F.R. §164.530(a)(1)(i); 45 C.F.R. §164.530(i)(1), (2), and (3)

AR-2, PRIVACY IMPACT AND RISK ASSESSMENT

Justification for Selection: Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. Privacy Impact Assessments are structured reviews (qualitative and quantitative) of both the risk and effect of how information is handled and maintained as well as the potential impacts or harms to individuals and organizations for loss of control or mishandling of the PII.[34] A PIA-like process, even if not required for a particular information system, benefits an organization and the individuals whose PII is in the information system by enabling the organization to identify, evaluate, and manage the privacy risks for the PII in that system.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Information system privacy risk management processes operate across the life cycle of an information system collecting, using, maintaining, and/or disseminating PII. Such privacy risk management processes include, but are not limited to, design requirements, privacy threshold analysis, privacy impact assessments (PIA), and implementation of secure disposition. While Section 208 of the E-Government Act does not require — or prohibit — a PIA for a national security system (NSS), as defined at 40 U.S.C. §11103 (see Section 202(i) of the E-Government Act), an organization may benefit from conducting a PIA or similar privacy risk evaluation on NSS as part of their internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing PII. Related Controls: RA-3

[34] E-Government Act of 2002, §§. 208, and OMB M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB Circular A-130, 7.g., 8.a.(1), 8.b.(2), and 8.b.(3)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.530(c)

AR-3, PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

Justification for Selection: Contracts and other acquisition-related documents provide an enforceable means to ensure privacy and security controls follow the information, and that contractors and service providers protect PII in the same way the organization does.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: The contract or other acquisition-related documents must flow-down privacy and security clauses to ensure sub-contractors adequately protect PII.

PHI Control Extension: Under HIPAA, a business associate must ensure its contracts or other arrangements with subcontractors meet the requirements of 45 §C.F.R. §164.504(e)

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(m); 48 C.F.R. Part 24.102; 48 C.F.R. Part 39.105; OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.504(e)

AR-4, PRIVACY MONITORING AND AUDITING

Justification for Selection: Monitoring and auditing activities ensure privacy controls are implemented and operating effectively.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: As many of the controls assigned by the Privacy Overlays are security controls, it is most efficient to develop a coordinated organizational process to conduct monitoring and audit. Where security and privacy controls align, in order to achieve the most efficient and effective implementation, the SAOP/CPO and CIO or CISO should coordinate to develop a single organizational process to conduct audit and monitoring.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
… concurrent with the organization's security control review schedule……

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: Pub. L. No. 107-347, §208; Pub. L. No. 107-347, Title III; OMB M-07-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.530(a)(1)(ii)

AR-5, PRIVACY AWARENESS AND TRAINING

Justification for Selection: Privacy Training is an effective means to reduce privacy risk for an organization and is mandated by the Privacy Act of 1974, as amended, and OMB M-07-16.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to organization information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties. Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing telework and other authorized remote access programs, training must also include the rules of such programs.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Privacy training may be integrated with general IA training. Examples of jobs or roles that would require job-specific privacy and security training include: human resource personnel who have greater access to PII; system developers who design, develop and implement information systems containing PII; and system administrators who operate and maintain information systems containing PII. Related Control: AT-2.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9); OMB M-06-16; OMB M-07-16 ,Att. 1, A.2.d.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.530(b)(1)

AR-6, PRIVACY REPORTING

Justification for Selection: Privacy reporting helps organizations to determine progress in meeting privacy compliance requirements and to ensure organizational accountability.

PHI Supplemental Guidance: HIPAA covered entities have specific reporting requirements to the Secretary, Health and Human Services.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; 44 U.S.C. §3541(4); OMB Circular A-130, 7.g.; Pub. L. No. 107-347, §208; OMB M-08-09

PHI Regulatory/Statutory Reference: 45 C.F.R. § 160.310(a); 45 C.F.R. §164.408

AR-7, PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT

Justification for Selection: Automating privacy controls provides a concrete way of ensuring information systems are behaving in a way that is intended to achieve privacy objectives. Implementation of this Privacy Overlay enables organizations to automate application of privacy controls. One simple example, which many organizations have already implemented, is TR-1, "Privacy Notice." This concept is one part of the most commonly recognized approach to "building privacy in" which is "Privacy by Design." Privacy by Design is an internationally accepted privacy best practice endorsed by the Federal Trade Commission in their March 2012 Final Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, and embodies the same principles of the Privacy Act and Section 208 of the E-Government Act requiring privacy protections and safeguards before establishing or operating a system that may contain PII. Privacy by Design calls for considering privacy risks in the design and management of information systems. In addition to building in security and privacy controls discussed throughout this overlay, this control considers additional privacy-specific system characteristics and controls that must be built into the system to address privacy risks.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Regardless of the systems engineering lifecycle used, privacy requirements should be considered during system design and development and validated and verified along with other system requirements. Validation ensures the correct requirements were identified. Verification ensures the requirements were implemented correctly.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; OMB M-03-22, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Federal Trade Commission Final Report (March 2012)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.530(c)

AR-8, ACCOUNTING OF DISCLOSURES

Justification for Selection: Both the Privacy Act and HIPAA require accounting of disclosures in certain circumstances. There are differences in the requirements to account for disclosures under the Privacy Act and under the HIPAA.

PHI Supplemental Guidance: HIPAA covered entities have specific accounting of disclosure requirements. An accounting of disclosure documents the disclosures of PHI made by the organization to third parties. Not all disclosures are required to be reported, for specific accounting disclosure requirements see 45 C.F.R. §164.528.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(c), (j), and (k)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.528

DI-1, DATA QUALITY

Justification for Selection: When a record is used to make a determination of a right, benefit, or privilege for an individual, the Privacy Act of 1974, as amended, requires the information used be accurate, relevant, timely, and complete to assure fairness to the individual in the determination. Agencies should ensure the quality of all of its PII, even if it is not protected by the Privacy Act. Organization's data quality assurance process should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), organizations should incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be confirmed accurate, relevant, timely, and complete. Frequency of confirmation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5;); OMB Circular A-130, 7.g. and 8.a.9

Control Enhancement: 1

Justification for Selection: Validating PII, used to determine a right, benefit, or privilege for an individual, ensures the determination is based on accurate, timely, and relevant information. Procedures for validating PII should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), organizations incorporate mechanisms into information systems and develop corresponding procedures and methods to validate the PII is accurate, relevant, timely, and complete.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(5;); OMB Circular A-130, 7.g. and 8.a.9.

Control Enhancement: 2

Justification for Selection: Re-validation of PII used to determine a right, benefit, or privilege for an individual, is necessary to ensure the determination is based on the most

accurate, timely, and relevant information. Frequency of revalidation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Moderate and High PII Confidentiality Impact Level Parameter Values:
… as frequently as is necessary to ensure the PII is accurate, relevant, timely, and complete; commensurate with the impact of the determination to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References:
5 U.S.C. §552a(e)(5;); OMB Circular A-130, 7.g. and 8.a.9.

DM-1, MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

Justification for Selection: Coordinating review of the organization's holdings of PII with existing system review processes maximizes the efficient use of organization resources and will ensure all PII retained, even if the PII is not maintained in a Privacy Act system of records, is relevant and accurate. Reducing PII to the minimum required to accomplish the legally authorized purpose of collection and retaining PII for the minimum necessary period of time reduces the risk of PII breaches and will reduce the risk of the organization making decisions based on inaccurate PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance:
Organizations should coordinate the PII holdings reviews with the systems' annual information security reviews schedule to the maximum extent practicable.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(1); OMB M-07-16; OMB Circular A-130, 7.g. and 8.a.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.502(b)

DM-2, DATA RETENTION AND DISPOSAL

Justification for Selection: Both the Privacy Act and the Federal Records Act require records to be maintained and disposed of in accordance with a published Records Schedule. Disposal and destruction of PII must be done securely so that it may not be reconstructed.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Values:
a. … the time period specified by the National Archives and Records Association (NARA)-approved Records Schedule and the Privacy Act SORN…
c. … NSA-approved or FIPS-validated techniques or methods…

PHI Parameter Values:

a. … a minimum of 6 years from the date of its creation or the date when it was last in effect, whichever is later…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(4)(E); NIST SP 800-88

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.316(b)(2)(i); 45 C.F.R. §164.530(j)(2)

Control Enhancement: 1

Justification for Selection: HIPAA requires the organization to follow specific procedures for de-identification and to implement policies and procedures to address the final disposition of PHI and/or the hardware or electronic media on which it is stored.
PHI Regulatory/Statutory Reference: 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.514

DM-3, MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH

Justification for Selection: When developing and testing information systems, PII is at a heightened risk for accidental loss, theft, or compromise. Therefore the organization needs to take measures to reduce that risk.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: When PII is of a sufficiently sensitive nature, to the greatest extent possible, PII should not be used when testing or developing an information system.

PHI Supplemental Guidance: HIPAA has specific requirements for the use of PHI in training or research. Under the Health care operations definition, covered entities may use PHI for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities. For additional information on the use of PHI in research, see 45 C.F.R. §164.512(i).

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: NIST SP 800-122; OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. §164.501; 45 C.F.R. §164.512(i)

Control Enhancement: 1

Justification for Selection: Anonymizing PII is one technique to reduce risk and decreases the potential impact if the PII is compromised.

PHI Supplemental Guidance: Under HIPAA, there are three requirements that minimize the risk to privacy of using PHI for research, testing or training. The first is the de-

identification of information that results in that information no longer being classified as PHI. There are only two methods for de-identification permitted by HIPAA. For specific details on those two methods see 45 C.F.R. §164.514(a). The second requirement is commonly referred to as the "Minimum Necessary Rule" which limits the amount of PHI used or disclosed to that which is reasonably necessary to accomplish the purpose for which the request for information is made. See 45 §C.F.R. §164.514(d). The third requirement allows covered entities to use or disclose a limited data set, which excludes certain direct identifiers. Unlike de-identified data, a limited data set is PHI and any use or disclosure must meet the requirements of HIPAA. See 45 C.F.R. §164.514(e).

PHI Regulatory/Statutory References: 45 C.F.R. §164.501; 45 C.F.R. §164.512(i); 45 C.F.R. §164.514(a), (d), (e)

IP-1, CONSENT

Justification for Selection: Individual participation and agreement to provide information is fundamental to an individual making an informed decision regarding the collection, use, and safeguarding of their PII.

Low, Moderate, and High PII Confidentiality Impact Level Supplementary Guidance: Whenever feasible, opt-in is the preferred method to obtain consent.

PHI Supplemental Guidance: Consent is a term under HIPAA with specific meaning not equivalent to a HIPAA authorization. For example, see: Uses and disclosures to carry out treatment, payment, or health care operations (45 C.F.R. §164.506); Uses and Disclosures for Which an Authorization is Required (45 C.F.R. §164.508); Uses and Disclosures Requiring an Opportunity to Agree/Object (45 C.F.R. §164.510); Right to Request Privacy Protection for Protected Health Information (45 C.F.R. §164.522).

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(3)-(4)

PHI Regulatory/Statutory References: 45 C.F.R. §164.506(b); 45 C.F.R. §164.508; 45 C.F.R. §164.510; 45 C.F.R. §164.522

Control Enhancement: 1

Justification for Selection: Individual consent or authorization is required under the HIPAA Privacy Rule for uses and/or disclosures of an individual's PHI.

PHI Regulatory/Statutory References: 45 C.F.R. §164.506(b); 45 C.F.R. §164.508

IP-2, INDIVIDUAL ACCESS

Justification for Selection: The Individual Participation FIPP requires organizations to provide mechanisms for individuals to gain access to their PII when appropriate. The

Privacy Act of 1974, as amended, requires organizations to provide mechanisms for individuals to gain access to their PII when that PII meets the definition of a "record." Access is also an important aspect of supporting correction of PII and redress against alleged violations and misuse of their PII. In addition to access requirements under the Privacy Act of 1974, as amended, HIPAA has statutory requirements to provide access to PHI.

PHI Control Extension: Implement policies and procedures to comply with the regulatory requirements governing an individual's right to access copies of their PHI, including electronic copies.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Organizations must provide for public access to records, including PII not included in a Privacy Act System of Records, where required or appropriate. While the language of this control is specific to the Privacy Act's requirements for access, FIPPs encourage organizations to use available authorities to provide access when the Privacy Act does not apply. For example, some organizations use the Freedom of Information Act as another tool to provide access to PII for an affected individual.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(c)(3), (c)(4), (d), and (h); OMB Circular A-130, 7.g. and 8.a.1.(l)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.524

IP-3, REDRESS

Justification for Selection: Redress supports data integrity requirements for PII by providing a process for individuals to request correction of, or amendment to, their PII maintained by an organization.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: DI-1.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(c)(4), (d), and (h)

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.526

IP-4, COMPLAINT MANAGEMENT

Justification for Selection: Establishing a complaint management process ensures complaints are addressed in a timely manner and provides an avenue for individuals to participate in government activities that may impact privacy. Information received from complaints provides external input regarding organizational privacy and security

practices which may improve processes and systems involved in collection, use, and maintenance of PII.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB Circular A-130, 7.g.; OMB M-07-16; OMB M-08-09

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.530 (d)

Control Enhancement: 1

Justification for Selection: Timely communications and resolution of complaints from individuals demonstrates responsiveness by the organization and reduces the organization's risk of reputational damage and potential lawsuits under HIPAA.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.520(b)(1)(vi)

SE-1, INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Justification for Selection: The PII inventory identifies the organization's information assets and identifies those assets collecting, using, maintaining, or sharing PII. The PII inventory identifies those assets most likely to impact privacy; provides a starting point for organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII; and to mitigate risks of PII exposure.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: CM-8.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(10); Pub. L. No. 107-347, §208(b)(2); OMB M-07-16, Att. 1, B.1.a

PHI Regulatory/Statutory References: 45 C.F.R. §164.530(c); 45 C.F.R. §164.310(d)

SE-2, PRIVACY INCIDENT RESPONSE

Justification for Selection: Developing and implementing a risk-based analysis for privacy breaches using a "Best Judgment Standard" as described in this control's supplemental guidance ensures consistency in, and avoids over-reporting of, privacy breach notifications.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The Best Judgment Standard, explained in OMB M-07-16, Footnote 6, imposes a requirement for organizations to develop and implement a risk-based analysis for privacy breaches to determine whether the breach needs to be reported. The Best Judgment Standard gives organizations responsibility for their own data in two important ways. First, the organization must determine the sensitivity of its PII, based on the information and the

context in which the information appears. Second, the organization must determine whether a privacy breach should be reported, based on the resultant privacy risk to the organization and to affected individuals. The Best Judgment Standard effectively imposes a requirement on organizations to develop and implement a risk-based analysis for privacy breaches to determine whether the breach needs to be reported. In the context of breach reporting, the purpose of the Best Judgment Standard is to limit reporting to those privacy breaches which meet the organization's risk threshold.

Conversely, under the Best Judgment Standard, organizations are not required to report privacy breaches that do not meet their risk threshold. The policy provides an example of implementing the Best Judgment Standard as discarding a document with the author's name on the front and no other PII into an office trashcan, positing that this probably would fall below and organization's risk threshold and would not need to be reported.

OMB M-07-16 does not provide bright line rules to define what is considered "sensitive PII" using the common dictionary definition approach to the language in the memo – and under what circumstances a privacy breach should be reported, both because it would be a futile effort to attempt to delineate or predict the myriad potential contexts and situations, and agencies are in the best position to know and understand the relevant circumstances of their PII to determine which PII is sensitive and which breaches create risk.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-07-16

PHI Regulatory/Statutory References: 45 C.F.R. Part 164 Subpart D; 45 C.F.R. §164.308(a)(6)

TR-1, PRIVACY NOTICE

Justification for Selection: Providing the appropriate notification of privacy practices to the individual enables the individual to make an informed decision when they provide their consent.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The Privacy Notice described by OMB M-99-18, *Privacy Policies on Federal Web Sites*, frequently referred to on organization websites as a "Privacy Policy" or "Privacy and Security Notice," is intended as a broad notice of website privacy policies and general website use and does not meet the requirement for specific notice when collecting PII. When PII is maintained (including collection) in a system of records that is covered by the Privacy Act, the organization must provide a "Privacy Act Statement" (PAS) to the individual at the time of collection that meets the requirements of the Privacy Act of 1974, 5 U.S.C. §552a(e)(3), unless the organization has published a rule exempting that system of records from the (e)(3) notice provision in accordance with subsection (j) of the Privacy Act. If the PII is not maintained in a system of records under the Privacy Act, a privacy notice should be provided which describes the privacy practices associated with

that PII, including, but not limited to, the way the PII is protected, how it is used, and whether it is shared. This type of privacy notice must not be labeled as a "Privacy Act Statement." For example, several organizations refer to this notice type as a "Privacy Advisory."

PHI Supplemental Guidance: The HIPAA Privacy Rule also requires a privacy notice referred to as a "Notice of Privacy Practices." For specific rules on this notice please refer to 45 C.F.R. §164.520.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: OMB M-99-18; OMB M-10-22, Att. 2

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.520

TR-2, SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS

Justification for Selection: SORNs and Privacy Act Statements, i.e., (e)(3) notices, provide transparency, in advance of collection, use, maintenance, or sharing of PII when in a system that meets the statutory definition of a "system of records" under the Privacy Act. The Privacy Act defines "maintain" as "maintain, collect, use or disseminate." These requirements impact decisions made during planning, design, development, and operation of programs and systems.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The Privacy Act and OMB guidance set forth specific requirements regarding when and how notices are provided. In addition to any internal organization review process, the publication of a SORN in the Federal Register requires a mandatory review and comment period of a minimum of 40 days.

Regarding TR-2, paragraph a, the publication of a SORN is required only when the PII is maintained in a system that meets the statutory definition of a "system of records" under the Privacy Act. Not all systems containing PII may meet the definition of a "system of records." However, all PII maintained by an organization must be protected irrespective of whether the PII is subject to the Privacy Act.

Regarding TR-2, paragraph c, the PAS, when required, should be provided in the same format as the information is collected. For example, an electronic statement on a website, a written statement on a paper form, and a verbal statement provided for information that is collected verbally.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(3)-(e)(4)

Control Enhancement: 1

Justification for Selection: Publishing SORNs on organization websites improves transparency by providing individuals easier access to information about how their PII will be collected, used, maintained, or shared; and centralizing the information regarding to whom an individual should submit a request for access or amendment to their information covered by the SORN.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The organization may establish a centralized website for publication of their SORNs.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(4;); OMB Circular A-130, 7.g. and Appendix I

TR-3, DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Justification for Selection: Making information about an organization's privacy program readily available to the public reduces the burden on individuals wanting to better understand an organization's privacy practices; and reduces burden on privacy offices and program officials by providing answers to common privacy questions through an easily accessible forum.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(4); Pub. L. No. 107-347, §208(b)(1)(B)(iii); OMB M-03-22, I.A.; OMB M-10-23, Section 4

UL-1, INTERNAL USE

Justification for Selection: Consistent with the Privacy Act, the organization's internal use of PII contained in a SORN is limited to the purposes identified in one of the 12 exceptions to Section b of the Privacy Act and as described in the SORN. Consistent with the FIPPs and Section 208 of the E-Government Act, the organization's internal use of PII not contained in a SORN should be compatible with the purpose for which it was originally collected and as described in the PIA or other public notice.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: All PII must be used for an official government purpose only. The officers and employees of the organization must have a need for the PII in the performance of their official duties. These requirements apply to all PII regardless of its coverage by the Privacy Act.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Controls: AC-2, AC-3, AC-5, AC-6, AC-8, AC-21, AU-2, AU-3, AU-10, AU-14, IA-2, PS-1, PS-2, PS-3

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; OMB Circular A-130, 7.g.

PHI Regulatory/Statutory References: 45 C.F.R. §164.502; 45 C.F.R. §164.504; 45 C.F.R. §164.506; 45 C.F.R. §164.508; 45 C.F.R. §164.510; 45 C.F.R. §164.512; 45 C.F.R. §164.514

UL-2, INFORMATION SHARING WITH THIRD PARTIES

Justification for Selection: Sharing PII with third parties introduces new risks to the individual which, as applicable, requires organizations to establish formal agreements with the third party and ensure the sharing is compatible with the purposes described in notice to, and consent from, the individual. Consideration of privacy risks for sharing PII apply regardless of the method used or whether the information remains stored in the system of records. Data removed from an information system covered by a system of records notice (e.g., an HR database) and shared in another format (e.g., an Excel spreadsheet) must still meet purpose and use requirements of the associated notice. PII not in a system of records that is shared with a third party still must meet the Purpose Specification and, relatedly, Use Limitation FIPPs. For example, data extracts of PII shared via an Excel spreadsheet or database archive.

Low, Moderate, and High PII Confidentiality Impact Level Control Extension: Consistent with the Purpose Specification and Use Limitation FIPPs, sharing of PII must be compatible with the purpose for which it was collected. Consistent with the Transparency FIPP, any subsequent sharing that is not compatible may not be done until additional notice is provided to the individual, their consent is obtained, and relevant documents are updated or published; e.g., when applicable and appropriate publish an updated SORN to cover the additional incompatible sharing and obtain consent from the affected individuals.

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The reference in Appendix J, UL-2, to "ISE Privacy Guidelines," is to the Information Sharing Environment (ISE) established by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). In accordance with Section 1016(d) of the IRTPA and in furtherance of Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," the President of the United States approved for issuance and implementation the Information Sharing Environment Privacy Guidelines. In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (Pub. L. No. 110-53), the ISE facilitates the sharing of "terrorism information" and "homeland security information," as defined, respectively, in Section 1016(a)(5) of the IRTPA and Section 892(f)(1) of the Homeland Security Act (Pub. L. No. 107–296). The ISE Privacy Guidelines provide a framework to enable information sharing while protecting privacy, civil liberties, and other legal rights.

PHI Supplemental Guidance: Under the HIPAA, a covered entity may not use, disclose or request a medical record, except when the medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. The disclosure and sharing of PHI is governed by the HIPAA regulations. For

details consult the HIPAA Privacy and Security rules at http://www.hhs.gov/ocr/privacy/index.html.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a; Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment

PHI Regulatory/Statutory References: 45 C.F.R. §164.502(e)(1); 45 C.F.R. §164.514(e)(1)

6. Tailoring Considerations

Information system owners should coordinate with their SAOP or designated Privacy Officer to ensure security and privacy controls selected using the Privacy Overlays meet the organization's privacy requirements. The Privacy Overlays are not intended to be, nor should they be construed or relied upon as, legal advice. Statutes, regulations, and guidance are linked to security controls, as identified in Table 3, to aid system owners, program managers, developers, privacy programs, and those who maintain information systems to protect information systems containing PII, including PHI. As organizations evaluate the PII confidentiality impact level and applicability of HIPAA, they may choose to apply more stringent controls than those identified in the Privacy Overlays.

The specifications presented here were developed by subject matter experts on information privacy and information assurance/cyber security based on the requirements established by federal laws and regulations, federal standards, and industry best practices for protecting PII, including PHI.

Failure to adequately safeguard PII or PHI pursuant to federal laws and regulations may result in organizationally-governed administrative sanctions (up to and including adverse personnel actions) and, under certain circumstances, civil and/or criminal penalties for responsible individuals or organizations. Tailoring of control specifications in the Privacy Overlays may have unintended adverse effects beyond the individual or organization. When there is compelling operational necessity, conduct a risk-based analysis evaluating the effect of tailoring out the particular control(s) or parameter value(s), document the risk-based analysis as an artifact in the authorization package, and obtain approval from the cognizant authorizing official before tailoring or otherwise revising the security and privacy controls identified in the Privacy Overlays. Organizations are strongly encouraged to seek legal counsel when considering tailoring.

Additionally, some controls did not warrant selection or exclusion for any PII confidentiality impact level, but may require further consideration when systems containing PII employ these controls (e.g., selected as part of a baseline or another overlay) to ensure privacy considerations related to that control are addressed. For example, AC-3(10), which discusses override of automated access control mechanisms, is neither mandatory nor must it be excluded for systems containing PII. However, when AC-3(10) is implemented for systems that contain PII, organizations must consider how to implement this control in a way that prevents users from

circumventing access controls that protect PII. Organizations should consider the following specific control guidance when tailoring information systems that are used to store, process, or transmit PII in addition to using the general tailoring guidance in CNSSI 1253.

AC-2, ACCOUNT MANAGEMENT

Control Enhancement: 9

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Shared/group accounts that do not allow for uniquely attributing user activities should not be used for information systems that contain PII or PHI. Shared/group accounts do not allow for the necessary accountability (such as non-repudiation) required to log and monitor access to PII and PHI nor do they permit identification of individuals who have a need for access. Shared/group accounts do not permit audit trails to associate a user with an action — eliminating the ability to establish non-repudiation. Non-repudiation is a critical element of accountability and accuracy of information in systems, database or system history, and related logs and is important for investigating privacy incidents and breaches. Related Controls: AC-14, AR-4.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … the requirement to uniquely attribute user activity to an account……

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b)(1); 5 U.S.C. §552a(c)(1); OMB Circular A-130, 7.g. and 8.a.1, 8.b.(2)(c).

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(i);

AC-3, ACCESS ENFORCEMENT

Control Enhancement: 10

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: For systems covered by the Privacy Act, this type of action must be audited. Under the Privacy Act, only individuals with a need for those records in the performance of their duties may gain access. When access control mechanisms are overridden, the override must be auditable or audited.

Low, Moderate, and High PII Confidentiality Impact Level Parameter Value: … situations where access control mechanisms are overridden for information systems containing PII under the Privacy Act…

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b)

AC-6, LEAST PRIVILEGE

Control Enhancement: 3

High PII Confidentiality Impact Level Supplemental Guidance: This controls restricts network access (i.e. access across a network connection as opposed to local access, such as being physically present at a device to access) to perform privileged commands.

High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b)(1); OMB M-06-16

AC-8, SYSTEM USE NOTIFICATION

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: System use notification (e.g., logon banner) does not satisfy the requirement for Privacy Act Statements or Privacy Act system of records notice, when applicable – see TR-1 and TR-2. System use notifications are the primary, interactive vehicle for notifying system users prior to accessing a system of the organization's monitoring practices and reminding users that unauthorized use is both prohibited and subject to criminal and civil penalties. The system use notification requires explicit action from the system user to acknowledge the notice before they can enter the system. While system use notices are principally intended to convey information regarding consent to monitor (and other security-relevant information), they may also be, in some instances, an appropriate means to remind system users that the system being accessed contains sensitive PII and requires due care (e.g., a logon banner on an employee management system). Related Controls: TR-1, TR-2.

PHI Supplemental Guidance: System Use Notification does not satisfy the requirement for privacy notice under the HIPAA Privacy Rule.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(3) and (e)(4); OMB Circular A-130, 7.g.

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.520(1)(i)

AC-14, PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Individual accountability requires the ability to trace (audit) the actions of the user who initiated them when accessing PII. Therefore, un-identified and un-authenticated users shall not access PII. Related Control: AC-2(9)

PHI Supplemental Guidance: Individual accountability requires the ability to trace (audit) the actions of the user who initiated them when accessing PHI. Therefore, un-identified and un-authenticated users shall not access PHI. Related Control: AC-2(9)

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(b); OMB Circular A-130, 7.g. and Appendix III

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(a)(2)(i)

AC-23, DATA MINING PROTECTION

Low, Moderate and High PII Confidentiality Impact Level Control Extension: When conducting data mining (as defined in the Federal Agency Data Mining Reporting Act of 2007, see Section 7, "Definitions," below) ensure the following are addressed for each data mining relationship in support of a Data Mining Impact Analysis (DMIA):

- An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.
- A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.
- A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to protect the privacy and applicable due process rights of individuals, such as redress procedures; and ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

Low, Moderate and High PII Confidentiality Impact Level Supplemental Guidance: Data Mining should only be conducted when a DMIA has been completed that examines, mitigates and justifies any acceptance of privacy risks.

Low, Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: Federal Agency Data Mining Reporting Act of 2007, §804(c)(2); 42 U.S.C. §2000ee–3.

AU-4, AUDIT STORAGE CAPACITY

Control Enhancement: 1

Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: For audit logs containing PII, regardless of location stored (including portable media or storage devices), implement safeguards commensurate with privacy risk. Transferring audit logs containing PII creates the potential for an increased risk of loss, theft or compromise of the PII. When audit information contains PII or PHI, it must be protected commensurate with its confidentiality impact level with regard to PII, or in accordance with a risk analysis with regard to PHI. Audit information could be necessary to enforce

criminal or civil penalties under the Privacy Act. Maintaining the integrity of audit records by applying this control enhancement facilitates this purpose. Related Controls: AR-4, AU-9, and AU-9(2).

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(i), OMB M-07-16, OMB Circular A-130, 7.g. and Appendix II

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.312(b)

AU-9, PROTECTION OF AUDIT INFORMATION

Control Enhancement: 4

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: When audit information contains PII, the requirement for access to that audit information is the same as for access to PII generally. As such, access to PII in audit logs requires a need-to-know and privacy training commensurate with level of responsibility and access. Privileged users must be evaluated to determine if they have such a need-to-know as part of his or her security function. Related Control: AR-5.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(b)(1)

AU-11, AUDIT RECORD RETENTION

Control Enhancement: 1

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: When audit information contains PII, ensure long-term retrieval systems adequately address necessary safeguards to protect that PII.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a(e)(10)

AU-14, SESSION AUDIT

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: The capture or recording of user sessions may involve the collection of the user's own PII, e.g., bank account information or e-mail to clergy or psychiatrist. Some session audit collections may be exempt from the specific notice requirements of the Privacy Act. However, in such cases where the compilation is exempt, consider alternative methods to provide a general notice, e.g., system usage notification. Consult with your counsel to determine adequacy of notice. Related Controls: AP-1, AP-2, TR-1,TR-2.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(7) and (i)(3)

Control Enhancement: 2

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: When user session information is captured or recorded, ensure relevant privacy controls are addressed. The capture or recording of user sessions may involve the collection of the user's own PII, e.g., bank account information or e-mail to clergy or psychiatrist. Such PII may not be collected without prior publication of a Privacy Act SORN. Investigatory material compiled for law enforcement purposes may be exempt from the specific notice requirements of the Privacy Act. However, in such cases where the compilation is exempt, consider alternative methods to provide a general notice, e.g., system usage notification. Consult with your counsel to determine adequacy of notice. Related Controls: AP-1, AP-2, TR-1, TR-2.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(7) and (i)(3)

Control Enhancement: 3

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: When user session information is captured or recorded, ensure relevant privacy controls are addressed. The capture or recording of user sessions may involve the collection of the user's own PII, e.g., bank account information or e-mail to clergy or psychiatrist. Such PII may not be collected without prior publication of a Privacy Act SORN. Investigatory material compiled for law enforcement purposes may be exempt from the specific notice requirements of the Privacy Act. However, in such cases where the compilation is exempt, consider alternative methods to provide a general notice, e.g., system usage notification. Consult with your counsel to determine adequacy of notice. Related Controls: AP-1, AP-2, TR-1, TR-2.

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(7) and (i)(3)

CP-7, ALTERNATE PROCESSING SITE

Moderate and High PII Confidentiality Impact Level Supplemental Guidance: When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect PII in accordance with the privacy risks identified.

PHI Supplemental Guidance: When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect PHI in accordance with the organization's risk analysis.

PHI Parameter Value: … critical business processes for protection of the security of PHI…

Moderate and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9), (e)(10), and (m)(1)

PHI Regulatory/Statutory References: 45 C.F.R. §164.310(a)(2)(i); 45 C.F.R. §164.308(7)(ii)(C)

PM-2, SENIOR INFORMATION SECURITY OFFICER

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Related Control: AR-1

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: OMB M-05-08

PM-13, INFORMATION SECURITY WORKFORCE

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: In order to implement adequate security controls, the organization's information security and privacy workforce should be knowledgeable of the applicable privacy and security requirements commensurate with the level of access or responsibility for applying appropriate safeguards. The information security workforce should receive role-based training for the privacy requirements commensurate with the level of access or responsibility for applying safeguards to PII.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(e)(9)-(10); OMB Circular A-130, 7.g.; OMB M-07-16

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.308(a)(2)

DI-2, DATA INTEGRITY AND DATA INTEGRITY BOARD

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The Privacy Act of 1974 has specific requirements for organizations who participate in Computer Matching. These controls are applicable when the organization is such a participant. If the organization is a participant in a matching program, as defined by the Privacy Act of 1974, then this control is applicable.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(a)(8), (o), and (u)

Control Enhancement: 1

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: The Privacy Act of 1974 has specific requirements for organizations who participate in Computer Matching. These controls are applicable when the organization is such a participant. If the organization is a participant in a matching program, as defined by the Privacy Act of 1974, then this control is applicable.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: 5 U.S.C. §552a(a)(8), (o), and (u)

DM-3, MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH

Control Enhancement: 1

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: When PII is of a sufficiently sensitive nature, to the maximum extent possible, PII should be anonymized in accordance with NIST SP 800-122 prior to its use in development or testing.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory References: NIST SP 800-122; OMB M-07-16

IP-4, COMPLAINT MANAGEMENT

Control Enhancement: 1

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Timely communications and resolution of complaints from individuals demonstrates responsiveness by the organization and reduces the organization's risk of reputational damage and potential lawsuits under the Privacy Act. Organizations should establish a complaint management process which ensures complaints are resolved within a reasonable amount of time.

Low, Moderate, and High PII Confidentiality Impact Level Regulatory/Statutory Reference: 5 U.S.C. §552a; OMB Circular A-130, 7.g.

TR-1, PRIVACY NOTICE

Control Enhancement: 1

Low, Moderate, and High PII Confidentiality Impact Level Supplemental Guidance: Real-time notice facilitates informed consent and promotes trust from the individual when collecting sensitive PII. Real-time notice used in conjunction with a Privacy Act Statement or Privacy Advisory, based on the sensitivity of the PII provided or collected, ensures the individual provides informed consent.

PHI Supplemental Guidance: The HIPAA Privacy Rule provides the option of layered notice to allow for simplified up-front notification with greater detail following. The Department of Health and Human Services has provided both guidance and model notices of privacy practices (see http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html for details).

PHI Regulatory/Statutory Reference: 45 C.F.R. §164.520

7. Definitions

This Overlay uses terms in NIST SP 800-53, Rev. 4, and CNSSI4009, *National Information Assurance (IA) Glossary*, and provides clarification for terms which appear in Federal policy but may not be consistently applied.

Best Judgment Standard [OMB M-07-16]	The Best Judgment Standard, explained in OMB M-07-16, Footnote 6, gives organizations responsibility for their own data in two important ways. First, the organization must determine the sensitivity of its PII, based on the particular information and the specific context in which the information appears. Second, the organization must determine whether a privacy breach should be reported, based on the resultant privacy risk to the organization and to affected individuals. Effective execution of the Best Judgment Standard requires organizations to develop and implement a risk-based approach to analysis of a privacy breach and limit reporting to only those privacy breaches which meet the organization's risk threshold. Conversely, organizations are not required to report privacy breaches that do not meet its risk threshold. For example, under the Best Judgment Standard an organization could determine that discarding a document with the author's name on the front, and no other PII, into a trashcan would fall below the risk threshold and would not need to be reported. The Best Judgment Standard applies to external reporting of privacy breaches, although an organization may choose to implement this approach for reporting privacy breaches internally, as well. OMB M-07-16 does not provide bright line rules to define what is considered "sensitive PII" – using the common dictionary definition approach to the language in the memo – and under what circumstances a privacy breach should be reported, both because it would be a futile effort to attempt to delineate or predict the myriad potential contexts and situations, and agencies are in the best position to know and understand the relevant circumstances of their PII to determine which PII is sensitive and which breaches create risk.
Chief Privacy Officer (CPO)	CPO is a title generally referring to the individual that has operational privacy responsibilities for an organization. This role may be assumed by the SAOP or another individual within the organization. Organizations may choose other titles to refer to this function (e.g., Privacy Program Manager).
Data Mining [Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. §2000ee–3]	The term "data mining" means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where— (A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
(C) the purpose of the queries, searches, or other analyses is not solely—
(i) the detection of fraud, waste, or abuse in a Government agency or program; or
(ii) the security of a Government computer system.

Personally Identifiable Information (PII) [OMB M-07-16, M-10-22]	OMB M-07-16 defines PII as information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB M-10-22 further clarifies that "the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. In performing this assessment, it is important for agencies to recognize that non-PII can become PII, whenever additional information is made publicly available, in any medium and from any source that, when combined with other available information, could be used to identify an individual." OMB M-07-16, Footnote 6, recommends an organization use its best judgment to determine the sensitivity of PII by evaluating the context in which it appears.
PII Confidentiality Impact Level [NIST SP 800-122]	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.
Protected Health Information (PHI) [45 C.F.R. §160.103, 45 C.F.R. §165.514]	PHI is a subset or smaller grouping of PII and is defined as individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by a covered entity in its role as an employer. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. <u>Limited Data Set (LDS)</u> is a small grouping or subset of PHI that excludes specific data elements created for the purposes of research, public health, or health care operations as set forth in the HIPAA Privacy Rule at 45 C.F.R. §164.514(e)(2).). <u>De-identified data</u> is information that does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual. The two methods for de-identifying PHI are set forth in the HIPAA Privacy Rule at 45 C.F.R. §164.514(b). PHI and LDS are equally protected under HIPAA and the misuse or unauthorized

	disclosure of this information is a violation of HIPAA, which could result in criminal or civil penalties to individuals or organizations. Data that is de-identified in accordance with the HIPAA standards is not considered PHI and is therefore not subject to HIPAA. For PHI, the HIPAA Security Rule requires covered entities and business associates to "reasonably and appropriately implement the standards and implementation specifications"[35] taking into account several factors, including "the probability and criticality of potential risks to electronic protected health information."[36] This risk-based approach requires covered entities and business associates to have an understanding of their technical capabilities, internal and external sources of PHI, and known or potential threats and vulnerabilities in their environments.
Senior Agency Official for Privacy (SAOP) [OMB M-05-08]	The senior organizational official with overall organization-wide responsibility for information privacy issues. This role is defined in OMB M-05-08, Designation of Senior Agency Officials for Privacy.

Annex

Relationship Between the Privacy Overlays and the Risk Management Framework (RMF)[37]

The CNSS adopts the RMF as defined by NIST SP 800-37 and provides additional instructions in CNSSI No. 1253. CNSSI No. 1253 provides guidance on the first two steps of the RMF, Categorize and Select, for all NSS. The Privacy Overlays were developed following the guidance in CNSSI No. 1253. The security and privacy controls of the Privacy Overlays can be applied to any security control baseline selected during the RMF process, protecting PII as an asset of the individual as well as an asset of the organization. The Privacy Overlays inform all steps in the RMF.

From CNSSI No. 1253, categorization (RMF Step 1) is a two-step process: (i) determine the impact values for each information type and for the information system; and (ii) identify overlays that apply to the information system and its environment of operation. The PII confidentiality impact level is used to determine the confidentiality impact value for the privacy information type(s) as well as the applicability of the Privacy Overlays. The initial set of security controls are selected (RMF Step 2) by integrating the baseline security controls with the security controls from the Privacy Overlays, plus any other applicable overlays (e.g., the Classified Information Overlay). To complete the selection process, the initial set of security controls is tailored following the guidance in NIST SP 800-53, CNSSI No. 1253, and the Privacy Overlays. Figure

[35] See 45 C.F.R. §164.306(b)(1)
[36] See 45 C.F.R. §164.306(b)(2)(iv)
[37] The RMF provides a disciplined and structured approach to integrate information security and risk management activities into the enterprise architecture and system development life cycle, providing an emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems. The RMF links risk management processes at the information system level to risk management processes at the organization level.

1 illustrates the relationship between the Privacy Overlays, NIST SP 800-122, and Steps 1 and 2 of the RMF in greater detail.

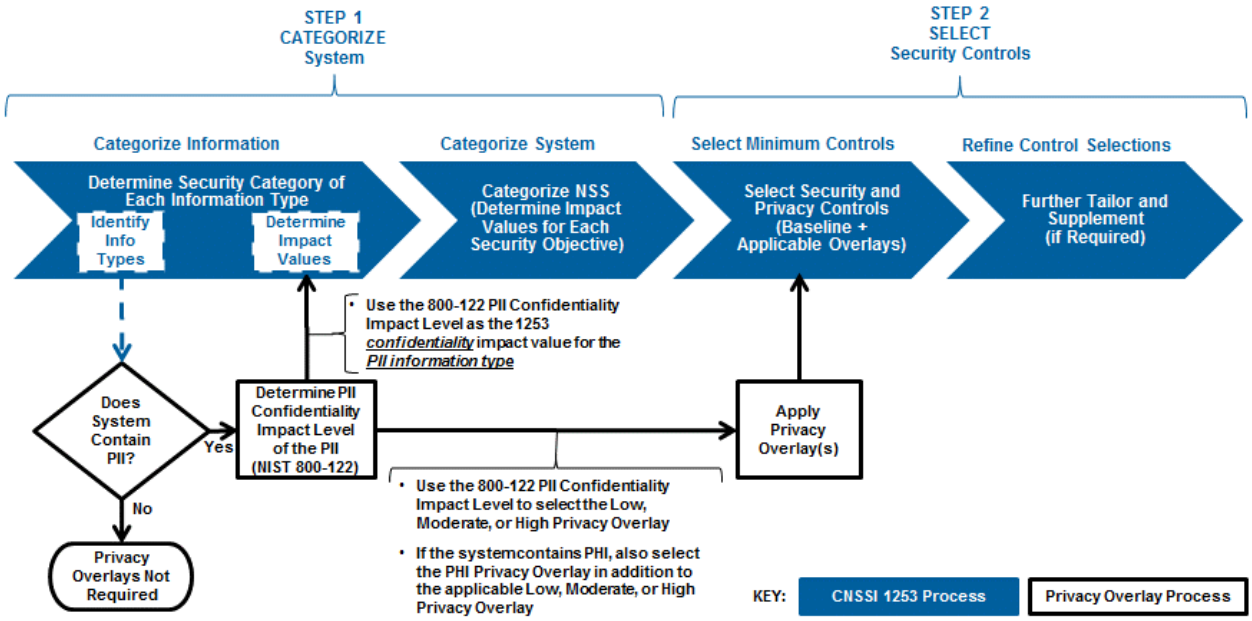

Figure 1. Relationship Among the Privacy Overlays, NIST SP 800-122, and Steps 1 & 2 of the RMF[38]

[38] For definitions of terminology in the diagram, see NIST SP 800-53, CNSSI No. 4009, and NIST SP 800-122.