Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS Policy for

Privacy Act Implementation & Breach Notification

July 23, 2007

Document Number: CMS-CIO-POL-PRIV01-01

TABLE OF CONTENTS

1. PURPOSE

This document establishes the policy for implementation at the Centers for Medicare & Medicaid Services (CMS) of the Privacy Act of 1974, as amended at 5 U.S.C. 552a, the Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503), and the Department of Health and Human Services (HHS) Privacy Act Regulations at 45.C.F.R. Part 5b. This document also establishes the policy by which CMS shall safeguard against and respond to the breach of personally identifiable information (PII).

This policy incorporates and supersedes the *CMS Policy for "Minimum Necessary" Data Dissemination & Use* that was previously issued on March 2, 2007 to ensure that CMS is in compliance with the "minimum necessary" requirements set forth in the Privacy Act of 1974 (as amended) and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR Parts 160 and 164) regarding use of PII.

2. BACKGROUND

Broadly stated, the Privacy Act of 1974 was established to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them.

The Privacy Act of 1974 focuses on four basic policy objectives:

(1) To restrict disclosure of personally identifiable records maintained by agencies;

(2) To grant individuals increased rights of access to agency records maintained on them;

(3) To grant individuals the right to seek amendment of agency records maintained on them upon a showing that the records are not accurate, relevant, timely, or complete; and

(4) To establish a code of "fair information practices" that requires agencies to comply with statutory norms for the collection, maintenance, and dissemination of personally identifiable records.

Due to the steady automation of government programs, automated records play a significant and pervasive role in Federal recordkeeping. The Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503) is the first amendment to the Privacy Act of 1974 to attempt to deal with the issue of automated records and their use. This amendment adds certain protections for individuals whose Privacy Act records are used in automated matching programs. These mandated protections ensure procedural uniformity in carrying out matching programs; due process for individuals in order to protect their rights, and oversight of matching programs through the establishment of Data Integrity Boards at each agency that engages in matching in order to monitor the agency's matching activities.

Safeguarding PII in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Office of Management and Budget (OMB) requires all government agencies to safeguard against and respond to the breach of PII, which is also a function of applicable laws, such as the Privacy Act of 1974 and the Federal Information Security Management Act (FISMA) of 2002. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." FISMA requires government agencies to implement procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done.

Privacy breaches are generally specific and context dependant. External notification of a breach is not always necessary or desired. Breaches, however, can implicate a broad range of harms to individuals, including but not limited to the potential for identity theft or fraud, breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information that could result in fear or uncertainty, or unwarranted exposure leading to humiliation or loss of self-esteem.

The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. A Federal agency's ability to respond quickly and effectively in the event of a breach of Federal data is critical to its efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

3. SCOPE

The Privacy Act binds only Federal agencies, and covers only records in the possession and control of Federal agencies. The Privacy Act and CMS' data use policies protect information about individuals (e.g., beneficiaries, individual health care providers, CMS employees and contractor staff), but do not cover institutional providers (e.g., hospitals, home health agencies, etc.).

This policy applies to all CMS data dissemination and use of PII, including but not limited to health care operations, payment and oversight, coordination of benefits, research, and/or any other purpose authorized under a CMS Privacy Act System of Records or the Privacy Rule. Breaches subject to notification requirements include electronic systems, as well as paper documents or any other format.

All employees of CMS, as well as CMS contractor staff, are required to comply with this Agency policy. Any Agency employee or contractor that does not comply with this policy will be subject to the maximum penalties allowed by law.

This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

4. POLICY

4.A. Collection and Maintenance of Personal Information

4.A.1. The collection and maintenance of information that is protected by the Privacy Act shall be limited to only that which is relevant and necessary to accomplish the mission of the Agency. Only the minimal amount of information that is necessary to meet the identifiable needs at hand shall be collected. Without exception, the collection of information from and/or about individuals must be based on legitimate institutional needs directly related to statutory mandates.

4.A.2. All information technology (IT) projects that involve the collection, maintenance, use, or disclosure of information about individuals, or transmit or maintain electronically any PII, are required to have a System of Records (SOR). Each CMS SOR shall have its own system notice, which contains routine uses specific to that SOR. These routine uses must be compatible with the purpose(s) for which the data are collected. A routine use shall also be included that specifically applies to the disclosure of information in connection with response and remedial efforts in the event of a data breach.

4.A.3. All new and existing CMS systems shall be evaluated during development and/or modification to determine whether a Computer Match Agreement (CMA) applies to the information being collected.

4.A.4. Accurate, relevant, timely, and complete data shall be maintained. Quality and oversight activities shall be performed to ensure this requirement is met. In many instances, CMS is not the source of the collected data (e.g., enrollment data, claims data), and therefore, relies on the source of the data for accuracy. In the event that CMS determines data to be inaccurate, the source organization shall be notified. CMS shall work with the source organization to develop a plan to rectify the discrepancy and correct the data.

4.A.5. Unnecessary collection and use of social security numbers shall be eliminated from CMS information systems and programs. CMS shall participate in government-wide efforts to explore alternatives to use of social security numbers as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

4.B. Disclosure and Use of Personal Information

4.B.1. The disclosure and use of PII shall be limited to that which is necessary to accomplish the intended purpose of an Agency activity. CMS shall disclose PII consistent with the routine uses identified in the Privacy Act SOR notices that are published in the *Federal Register* and the limitations on uses and disclosures that are set out in the HIPAA Privacy Rule and other

applicable rules. Thus, CMS shall limit the disclosure of PII to no greater amount of information than is reasonably necessary to achieve the specific purpose of the disclosure.

4.B.2. CMS employees can obtain access to individual-specific data on a 'need-to-know' basis (i.e., role-based access only in those situations in which the data are integral to the completion of official duties as an employee of the Department of Health and Human Services (DHHS)). CMS employees are to limit their use of PII to only that information which is specifically needed to carry out their duties and are obligated to protect individual-specific data from wrongful disclosure.

4.B.3. Information that is protected by the Privacy Act shall not be published on the Internet.

4.B.4. For each information request, CMS shall determine if legal authorization exists for disclosure of the data and what data are needed to accomplish the task or project.

4.B.5. CMS shall assist research organizations by determining exactly what data are needed to accomplish a particular project/study, and provide only the data necessary for the given project/study. Requests for PII for research purposes must be submitted to and approved by the CMS Privacy Board. If the CMS Privacy Board determines that PII is not required to accomplish the purpose of the project/study, the request for PII will be denied and a recommendation made that the requestor obtain a limited data set or public use file when appropriate.

4.B.6. A requestor who already obtained CMS data for a specific purpose may use the data for another project if the second project meets the requirements of the Privacy Act and the CMS data use policies and procedures. The requestor must apply for written permission from CMS for the additional use by submitting a complete data request package in accordance with CMS procedures. A letter of support is required from the original requestor when the data being requested for reuse were acquired through either a Federal/State funded project and conducted by another private organization. If the initial data was obtained under a CMS contract, a letter of support from the prior project officer is required.

4.B.7. A record of disclosures shall be maintained for all required Privacy Act disclosure provisions. Additionally, CMS shall maintain a record of disclosures for all data disclosed to other agencies within the DHHS.

4.B.8. Statistical, aggregate or summarized information created as a result of analysis conducted using identifiable CMS data obtained under CMS-approved projects/studies may only be disclosed if the data are not individual-specific and the data are aggregated to a level where no data cells contain 10 or fewer individuals. CMS must review all reports, manuscripts, files, etc. to be re-released. This review pertains to all forms of publication, including information to be posted to the Internet. This review ensures that the reports, manuscripts, files, websites, etc. contain no data elements or combinations of data elements that by themselves or in addition to other data files and/or sources, could allow for the deduction of the identity of an individual and that the level of cell size aggregation meets the stated requirement. Only after such review has

occurred and CMS has provided written approval for the re-release of the reformatted CMS information (includes e-mail correspondence) is the data requestor legally authorized to re-release the data.

4.B.9. Processing fees may be charged when data are provided to other DHHS organizations, Federal agencies outside of DHHS, non-CMS Federal contractors/grantees, state agencies, and private organizations/individuals. Processing fees shall not be charged when data are provided to CMS employees or contractors/grantees performing duties/tasks of the Agency, the Government Accountability Office, Congress, or congressional committees. Due to legislative requirements, CMS does not grant requests for waivers of processing fees.

4.B.10. Requests from non-CMS organizations for the disclosure of beneficiary names and addresses for the purpose of contacting a target population in order to conduct interviews/surveys with the beneficiary or to initiate other activities involving the beneficiary's direct participation, must be approved by the CMS Privacy Board and meet all legal and Agency privacy policy and procedures. Internal CMS requests do not require Privacy Board approval, but must be reviewed and approved by the business owner. To obtain names and addresses of Medicare beneficiaries and/or physicians, the requestor is required to show that the data are absolutely necessary to conduct their study/project. The requestor must provide a rigorous and detailed explanation of how alternative sources of information (e.g., Department of Motor Vehicles driver's license lists, State voter registration lists, and random digit dialing) cannot be used to obtain survey participants. The relative resource intensity (e.g., money, staff time, etc.) of obtaining survey participants from other sources versus CMS is not considered a sufficient justification for use.

4.B.11. A beneficiary notification letter is required whenever a beneficiary is going to be contacted using data disclosed by CMS. The beneficiary notification letter must be signed by the CMS Privacy Officer. It must briefly describe the project/survey and explain that there will be no adverse affect on Medicare benefits whether or not the beneficiary chooses to participate. The letter shall contain a name and collect or toll-free telephone number (study contact) that beneficiaries may call with any questions. Additionally, a 2-3 page brochure explaining the project should be included with the letter to help the beneficiary make an informed decision on their participation in the study. Similarly, a provider notification letter is required whenever a physician or institution is going to be contacted using data disclosed by CMS. The same basic requirements apply for these letters as well.

4.B.12. Reasonable efforts shall be made to notify an individual when any record on that individual is made available to any person under a compulsory legal process, when such process becomes a matter of public record. Most disclosures of PII for legal purposes are made to other Federal agencies (e.g., Office of the Inspector General, Department of Justice, etc.). As Federal organizations, these entities must also comply with this notification requirement. Therefore, when CMS discloses the data to other Federal Agencies for legal purposes, the notification requirement becomes the responsibility of the other organization. An individual is not required to be notified when the disclosure is made with the consent or authorization of the individual.

4.B.13. Individuals or other agencies shall be informed about any correction or notation of dispute made by CMS, as requested by the individual, if the corrected or disputed record was disclosed outside of CMS under a required accounting of disclosure provision. This notification only occurs when CMS corrects, changes, or makes a notation of dispute. Any changes or corrections made by the source agency (e.g., SSA or FI/Carriers), are not communicated to the individuals or agencies for which the disclosure was made.

4.C. Data Use Agreement (DUA)

4.C.1. CMS' non-operational contractors and other entities external to CMS that use PII are required to enter into a DUA for the purpose of tracking the use of PII. The DUA shall identify the data being used, the specific uses of the data, the requestor/custodian of the data, the length of time the data can be used (i.e., retention date), and the business owner approving the use of the data. The DUA shall be signed by the requesting entity, the custodial entity (responsible for maintenance of the data while being used), CMS, and other Federal agency representatives, if applicable.

4.C.2. CMS' operational contractors are not required to enter into a DUA(s) due to the fact that the contract language for these organizations is very specific and stringent and is more than sufficient to warrant compliance with the requirements of the Privacy Act and HIPAA. These entities are considered an extension of CMS, such that disclosures are made under the 'employee of the agency' disclosure provision of the Privacy Act. Disclosures to operational contractors do not require accounting.

4.C.3. CMS does not require a DUA from a third party that contracts with operational contractors as long as the contract language extends the data use and privacy protections to the third party entities. The only time CMS requires an operational contractor, or their third party contractors, to enter into a DUA is when the organization requests to use CMS data for a purpose that is outside the scope of work specified in the CMS contract.

4.C.4. An established DUA must be closed or extended on or before the retention date identified in the DUA. If the project is completed before the specified retention date, the requestor shall ensure that the DUA is properly closed. A DUA is considered expired when use of the data exceeds the retention date of the existing DUA. Any requestor or custodian with an expired DUA is prohibited from establishing a new DUA with CMS, and must either extend or close the expired DUA(s). A one-time extension for a period of no more than one year may be requested for a DUA that is nearing expiration or has already expired. Additional extensions or extensions longer than one year shall be reviewed and approved on a case-by-case basis.

4.D. Privacy Impact Assessment (PIA)

4.D.1. All current CMS holdings of PII shall be reviewed annually to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. An annual PIA shall be conducted for each CMS SOR and data extract system to ensure there is no collection, storage, access, use or dissemination of PII that is not both needed and permitted. All

PII holdings shall be reduced to the minimum necessary for the proper performance of the documented CMS function.

4.D.2. A PIA shall be prepared at the individual system or application level for each information system or application that is covered by a General Support System (GSS) or Major Application (MA). An initial PIA shall be conducted for all systems or applications (whether currently in existence, undergoing modification, or being newly developed), and annually thereafter.

4.E. Safeguarding Personal Information

4.E.1. Safeguards shall be established to ensure the security and confidentiality of PII and to protect against any anticipated threats or hazards to their security or integrity. CMS shall also contemplate and incorporate best practices to prevent data breaches. For example, employees and contractor staff should include laptop computers in carry-on luggage rather than in checked baggage when traveling.

4.E.2. CMS managers, supervisors, employees, contractor staff, and other data users shall be informed and trained regarding their respective responsibilities relative to safeguarding PII and the consequences and accountability for violation of these responsibilities. CMS employees and contractors that have a User ID to access CMS computer systems are required to complete a mandatory Information Security and Privacy Training session annually. If this training is not completed, the User's access privileges shall be revoked. Additionally, Privacy Awareness and Data Dissemination Training shall be provided to CMS project officers and other CMS employees who may benefit. CMS employees and contractor staff shall be trained on how to prevent security incidents and privacy breaches, and instructed in their roles and responsibilities regarding responding to incidents and breaches should they occur.

4.E.3. All individuals with authorized access to PII and their supervisors shall sign, at least annually, a document clearly describing their responsibilities. Every CMS employee and CMS contractor that is assigned a CMS User ID must complete and sign an 'Application for Access to CMS Computer Systems' form. All access to and use of CMS' computerized information and resources shall be recorded and routine reviews conducted to identify unauthorized access and/or illegal activity.

4.E.4. Any individual with access to CMS computer systems containing sensitive information must abide by the HHS Rules of Behavior, as well as the following:

- Do not disclose or lend their CMS User ID and password to someone else. They are for individual use and serve as an 'electronic signature.' The user will be held responsible for the consequences of unauthorized or illegal transactions.
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create sub-files of such records, remove, or transmit data, unless specific authorization has been provided.

- Do not modify, delete, or otherwise alter CMS data files, unless specific authorization has been provided.
- Do not intentionally cause corruption or disruption of CMS data files.

4.E.5. Electronic information about an individual in an organized set of records shall be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.

4.E.6. Data extract tools that can customize and encrypt data files shall be utilized to ensure minimum disclosure of PII. All dissemination of PII using any portable media (e.g., CDs, DVDs, cartridges, diskettes, laptops, external hard drives, USB memory sticks or thumb drives, etc.) must be encrypted using CMS-approved encryption software.

4.E.7. All PII (whether it is for a CMS employee, a provider, or a beneficiary) shall not be transmitted via e-mail unless it is sent as an attachment that has been appropriately encrypted using CMS-approved encryption software. One exception is for e-mail being sent to internal CMS recipients and to recipients at the Social Security Administration (SSA). Internal e-mail and e-mail to SSA does not need to be encrypted, because CMS routes such transmissions through other secure mechanisms. A second exception is for e-mail transmitted specifically by the Program Safeguard contractors via the secure e-mail system on the Medicare Data Communications Network.

4.E.8. No PII is to be transported from a CMS data center unless it has been encrypted. The encryption requirement may only be waived through written concurrence from the business owner of the data followed by a "wet" signature from the Chief Information Officer (CIO), Deputy CIO, or the Chief Technology Officer. The only exception to this requirement is for tapes destined for off-site storage or for the purpose of data center transitions, and that data must be shipped using proper precautions (i.e., locked in sturdy containers).

4.E.9. All PII that is remotely stored must be encrypted in accordance with NIST Special Publication 800-53 security controls.

4.E.10. All documents that contain privacy information shall be clearly marked as “FOR OFFICIAL USE ONLY – PRIVACY ACT INFORMATION CONTAINED HEREIN.”

4.F. Rights and Privileges of Individuals

4.F.1. Individuals shall be informed of any records that are collected, maintained, and/or used by CMS from which information is retrieved by a unique identifier (e.g., the name of the individual, symbol, or other identifying particular assigned to the individual). The mechanism for this notification is via the publication of a SOR notice in the *Federal Register* that is available for public comment. Individuals shall also be informed when their records are subject to computer matching. The mechanism for this notification is via the publication of a CMA in the *Federal Register* that is available for public comment. After the required comment period and

review/clearance of all comments, a final SOR notice or CMA shall be published in the *Federal Register*.

4.F.2. An individual shall have access to any record that is maintained on that individual in a CMS SOR when requested, unless the record is maintained in an exempt SOR or meets other Privacy Act criteria for not permitting access.

4.F.3. Information shall be collected directly from a subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges. A majority of the data maintained by CMS is initiated by the individual, but may be provided to CMS by a secondary source (e.g., claims data provided by the Fiscal Intermediaries (FIs) and Carriers and enrollment data provided by the Social Security Administration (SSA)). CMS can only permit correction of data in cases where CMS is the source of the data. CMS cannot make corrections to data provided by a secondary source, but shall instruct the individual to return to the source of the information to request corrections.

4.F.4. Data may be collected directly from an individual to support beneficiary surveys/studies. CMS shall inform the public of collection activities by publishing a notice in the *Federal Register*. All individuals shall have the opportunity to submit comments on the collection notice. CMS shall review and take into account all public comments received.

4.F.5. There are instances when Medicare or Medicaid beneficiaries are contacted directly by an organization to request participation in a study and/or survey (e.g., either by CMS or CMS-approved research organizations). In these instances, CMS requires that the beneficiaries be notified by letter informing them of the study/project, providing them with the option to participate or not participate in the study/project, and informing them that non-participation in the study/project will not impact their Medicare or Medicaid benefits.

4.G. Breach Analysis and Notification

4.G.1. All CMS security incidents involving PII shall be reported to DHHS Secure One and the United States Computer Emergency Readiness Team (US-CERT) in accordance with CMS incident handling procedures within one hour of discovery/detection when: 1) an individual gains logical or physical access without permission to a CMS network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred. Updates are to be provided to DHHS Secure One and US-CERT in accordance with CMS incident handling procedures as further information is obtained during analysis of the incident.

4.G.2. An Agency response team shall be established that includes executive leadership from the business component of the program experiencing the breach, the CIO, the Senior Official for Privacy, Chief Financial Officer, Office of General Counsel, Director of the Office of Beneficiary Information Services, Director of the Office of External Affairs, and the Director of the Office of E-Health Standards and Services. Additional management designees and senior staff (e.g., staff from the Beneficiary Confidentiality Board (BCB), the CMS Privacy Officer,

and the CMS Chief Information Security Officer (CISO)) may also be appointed to assist in analyzing a breach and offering recommendations.

4.G.3. In determining whether external notification of a breach is required, CMS shall first assess the likely risk of harm and then assess the level of impact to determine when, what, how, and to whom notification should be given outside the Agency. Consideration should be given to a wide range of potential harms, including but not limited to the harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach, and the potential for identity theft. In addition, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

4.G.4. Care shall be exercised to avoid unnecessary external notification, concern, and confusion. In addition, the cost to individuals and businesses of responding to notices where the risk of harm may be low should be considered. The benefit of notifying the public of low impact incidents should be carefully evaluated.

4.G.5. The following five factors shall be considered when assessing the likely risk of harm and level of impact for a potential or confirmed privacy breach:

- Nature of the data elements breached in light of their context and the broad range of potential harms that may result from their disclosure to unauthorized individuals;
- Number of individuals affected;
- Likelihood the information is accessible and usable by unauthorized individuals;
- Likelihood the breach may lead to harm (including the broad reach of potential harm and the likelihood the harm will occur); and
- Ability of CMS to mitigate the risk of harm.

4.G.6. Notification shall be provided without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement and national security and any measures necessary for CMS to determine the scope of the breach, and, if applicable, to restore the reasonable integrity of the computerized data system(s) compromised. Any delay of notification should not exacerbate risk or harm to any affected individual(s).

4.G.7. Notice provided to individuals affected by a breach shall be commensurate with the number of people affected and the urgency with which they need to receive notice. Other public and private sector agencies shall also be notified on a need-to-know basis, particularly those that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach.

4.G.8. The best means for providing notification will depend on the number of individuals affected and the contact information that is available about the affected individuals. First-class mail notification to the last known mailing address of the affected individuals shall be the primary means for providing notification. Telephone notification may be appropriate when urgency dictates immediate and personalized notification and/or when a limited number of individuals are affected, and should be contemporaneous with written notification by first-class

mail. Newspapers or other public media outlets may also be used to supplement individual notification as appropriate.

4.G.9. Written notification shall be provided in concise, conspicuous, plain language that includes the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise system security;
- What steps individuals should take to protect themselves from potential harm, if any;
- What CMS is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address, and postal address.

4.G.10. Notification of a breach shall also be posted in a clearly identifiable location on the home page of the CMS and/or Medicare web sites, as appropriate and as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting should provide answers to frequently asked questions and other talking points to assist the public's understanding of the breach and the notification process. The information should also appear on the www.USA.gov web site.

4.H. Criminal Penalties and Sanctions for Non-Compliance

4.H.1. Criminal penalties and/or other sanctions shall be imposed on CMS employees and non-employees, including contractors and researchers, for non-compliance with the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, and the policies and procedures established by CMS for the protection of PII, as well as for failure to take required steps to prevent a breach from occurring or for failure to take appropriate action upon discovering a breach.

4.H.2. All applicable criminal penalties and/or sanctions shall be expressly stated in all CMS DUAs with non-CMS employees, contractors, and/or researchers.

4.H.3. Rules of behavior and corrective actions shall address the following:

- Failure to implement and maintain security controls for PII, for which an individual is responsible and aware, regardless of whether such action results in the loss of control or unauthorized disclosure of PII;
- Exceeding authorized access to, or disclosure to unauthorized persons of, PII;
- Failure to report any known or suspected loss of control or unauthorized disclosure of PII; and

- For managers, failure to adequately instruct, train, or supervise employees in their responsibilities.

4.H.4. As with any disciplinary action, the particular facts and circumstances, including whether the breach was intentional, shall be considered in taking appropriate action. The minimum consequence considered should be prompt removal of authority to access information and/or information systems from any individual who demonstrates egregious disregard or a pattern of error in safeguarding PII. Additional consequences may include reprimand, suspension, removal, or other appropriate action(s). Any action taken must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement or Agency policy.

4.H.5. In accordance with provisions in the Privacy Act of 1974, the following criminal penalties may be imposed on CMS employees:

- Any officer or employee of CMS, who by virtue of his employment or official position, has possession of, or access to, Agency records which contain PII, the disclosure of which is prohibited, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
- Any officer or employee of CMS who willfully maintains a SOR without meeting the notice requirements shall be guilty of a misdemeanor and fined not more than $5,000.
- Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this policy:

5.A. CMS Employees, Contractors, and Other Data Users

CMS employees, contractors, and other users of CMS Privacy-protected data are responsible for:

- Adhering to the policy statements set forth in Section 4 of this policy document;
- Adhering to additional CMS operational policies and procedures that augment this policy (see Attachments Section below); and
- Seeking guidance from CMS management when in doubt about the implementation of this policy.

5.B. CMS Business Owners

CMS Group Directors or Deputy Group Directors who have the primary business needs that are or will be addressed by CMS IT investments/projects are referred to as CMS Business Owners, and are responsible for the following activities:

- Documenting and certifying that the data being collected and maintained are relevant and necessary to CMS' mission;
- Owning the information stored, processed, or transmitted in CMS' information systems, and determining who has access to the data/information;
- Approving all use and disclosure of data from CMS systems/applications that are covered by a SOR through the DUA vehicle by reviewing DUAs and authorizing or denying the release of PII;
- Establishing DUAs in accordance with the appropriate procedures (see Attachments Section below) to govern the disclosure of data from CMS' systems/applications that include an addendum that lists the categories of data to be released and a justification demonstrating the need for the categories of data (e.g., demographics, payment, diagnostic/procedure, etc.);
- Verifying that CMS' systems/applications are only disclosing data that is minimally necessary;
- Ensuring that CMS' systems/applications are disseminating data in compliance with the "minimum necessary" requirements;
- Determining and certifying whether the security controls that protect CMS' systems are adequate enough for operation;
- Establishing/revising SORs and CMAs in accordance with the appropriate procedures (see Attachments Section below);
- Preparing PIAs for systems or applications in accordance with the direction provided by the Privacy Specialists in the Office of Information Services (OIS) / Enterprise Architecture & Strategy Group (EASG) / Division of Privacy Compliance (DPC); and
- Leads the analysis of security incidents involving PII and the determination of the appropriate action to be taken regarding external notification of privacy breaches, as well as the reporting, monitoring, tracking, and closure of PII incidents.

5.C. CMS Project Officers

CMS Project Officers are responsible for the following activities:

- Ensuring that CMS contractors follow all required CMS security and privacy policies and procedures, as specified in established contracts and DUAs;
- Ensuring that CMS contractors follow all required procedures and provide all required documentation when requesting/gaining access to PII;

- Ensuring that CMS contractors only use the data required to perform the approved task(s);
- Ensuring that CMS contractors return or destroy the data covered by a DUA at the end of the contract/task; and
- Ensuring that appropriate notification and corrective actions are taken when a privacy breach involves a contractor or a public-private partnership operating a SOR on behalf of CMS.

5.D. CMS System Developers/Maintainers

CMS System Developers/Maintainers are responsible for the following activities:

- Ensuring that CMS information systems meet all established requirements and are developed/maintained in accordance with this and other CMS data policies, procedures, and standards;
- Enabling authorized access to information within CMS information systems in accordance with this and other CMS policies, procedures, and standards;
- Implementing required controls for CMS information systems and attesting to the successful completion of the appropriate technical certification evaluations;
- Supporting CMS business owners in the fulfillment of security certification and accreditation activities and the development of required security documentation;
- Improving on or correcting information security deficiencies and assisting CMS business owners in developing appropriate corrective action plans;
- Verifying that CMS systems/applications are only disclosing data that is minimally necessary;
- Ensuring CMS systems/applications that currently disseminate data for any purpose are capable of extracting by pre-approved categories of data; and
- Providing extracts of data from CMS systems/applications in accordance with the "minimum necessary" requirements.

5.E. CMS Privacy Officer

The CMS Privacy Officer is responsible for the following activities:

- Reviewing requests for the use and/or disclosure of PII to determine if there is legal authorization for the use/disclosure per the request;
- Reviewing and analyzing the purpose of any disclosure of information from a CMS SOR to determine if matching activities apply that require a CMA;
- Reviewing and approving SORs and CMAs;
- Providing information to DHHS, as requested, for inclusion in the President's Biennial Report on Privacy; and

- Assisting in the implementation of CMS incident handling procedures for PII incidents.

5.F. CMS Privacy Specialists

CMS Privacy Specialists in OIS/EASG/DPC are responsible for the following activities:

- Providing guidance and ongoing support to CMS employees, contractors, business owners, project officers, and system developers/maintainers in the implementation of this policy;
- Developing and implementing operational procedures to ensure compliance with this policy (see Attachment Section below);
- Ensuring that approval is obtained from the appropriate Business Owner prior to dissemination of PII data from a SOR;
- Ensuring that established DUAs include an addendum that lists the categories of data to be released and a justification demonstrating the need for the categories of data (e.g., demographics, payment, diagnostic/procedure, etc.);
- Ensuring that the CMS Data Agreement and Data Shipping Tracking System (DADSS) captures the specific categories of data associated with a given DUA;
- Monitoring the status of established DUAs to ensure that they are appropriately closed or extended;
- Facilitating the review and approval of research protocols associated with the use of PII;
- Conducting assessments of CMS' automated systems/applications and data dissemination requests (internal and external to CMS) to ensure that data are being disseminated in accordance with the "minimum necessary" requirements; and
- Developing a remediation plan for ensuring compliance of CMS' systems/applications and data dissemination requests that do not meet the "minimum necessary" requirements.

5.G. Beneficiary Confidentiality Board (BCB)

The BCB is comprised of executive leadership from CMS components that have a direct and substantial programmatic stake in privacy and confidentiality matters. The core responsibilities of the BCB include the following:

- Establishing strategic goals, overarching policies, and objectives related to the protection of confidential beneficiary information from the perspectives of the beneficiary and the institution and coordinating same with the DHHS;
- Establishing and coordinating all CMS policy decisions with regard to privacy and confidentiality, including issuance of policy memoranda to implement and operationalize such policy;
- Developing and assuring the implementation and enforcement of guiding principles for Agency-wide strategic goals and objectives regarding CMS management and oversight of privacy and confidentiality;

- Providing executive oversight of compliance with all privacy and confidentiality statutory and regulatory requirements, and assuring that beneficiary protections are enforced;
- Reviewing all current operations with regard to SORs and beneficiary protections to assure that strategic goals and objectives and guiding principles are effectively in place and operational, including those protections in place regarding downstream sharing of confidential information by contractors to sub-contractors;
- Evaluating legislative proposals involving the collection, use, and disclosure of personal information by any entity, public or private, for consistency with legal standards and guiding principles and recommending CMS positions with regard to such legislation;
- Assuring that CMS' use of new information technologies sustain, and do not erode, the protections provided in all statutes relating to Agency use, collection, and disclosure of personal information. These protections include data that directly identify an individual and information from which an individual's identity can be deduced;
- Assuring that personal information contained in Privacy Act SORs are handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- Serving as a principals-level forum for the discussion and resolution of key strategic issues affecting CMS privacy and confidentiality policies and implementation strategies, including resolving inter-component disputes;
- Reporting to the CMS Office of the Administrator (OA) on all issues related to privacy and confidentiality, and providing full and immediate support to OA on such matters; and
- Assessing the need for a Federal Advisory Committee with regard to confidentiality and privacy issues, and making recommendations to the CMS OA.

5.H. CMS Privacy Board

The CMS Privacy Board safeguards PII, assures that there is minimal privacy risk to an individual when PII is released to a researcher, and ensures compliance with the Privacy Act of 1974 and the HIPAA Privacy Rule. The core responsibilities of the CMS Privacy Board include the following:

- Determining whether the requestor meets the data disclosure provisions contained in the Privacy Act of 1974 and the provisions of the HIPAA Privacy Rule;
- Determining whether the research needs identifiable data and whether the scope of the study could potentially benefit Medicare beneficiaries or help administer CMS programs;
- Examining the soundness of the research design, the expertise and experience of the investigators, and the adequacy of measures to safeguard the data;
- Applying the existing criteria for data release procedures that are posted on CMS' website;
- Certifying that the researcher's use of PII involves no more than a minimal risk to the privacy of the research subjects, that the research cannot practically be conducted without waiving individual beneficiary authorization, and that the research cannot practicably be conducted without access and use of PII;

- Recommending to the BCB improvements to CMS' data release policies, criteria for releasing PII, and the development of new research databases; and
- Developing procedures that will permit an expedited review process (i.e., review by sub-committee). The HIPAA Privacy Rule allows the Privacy Board to conduct their reviews of data requests by a sub-committee rather than a full board member review.

5.I. CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the overall implementation and administration of the CMS Information Security Program, and provides overall direction for high-priority incident handling, which includes all PII incidents.

5.J. CMS Chief Information Security Officer (CISO)

The CMS CISO assists the CIO in the implementation and administration of the CMS Information Security Program, including fulfillment of the CIO's incident handling responsibilities. The CMS CISO maintains coordination and communication with the DHHS CISO and DHHS Secure One for incident reporting, tracking, and closure.

5.K. CMS Senior Official for Privacy

The CMS Senior Official for Privacy is the individual designated within CMS to protect the information privacy rights of CMS employees and beneficiaries of Agency programs, and to ensure CMS has effective information privacy management processes to accomplish this important function. The CMS Senior Official for Privacy provides overall direction on individual notifications for PII incidents.

5.L. CMS Administrator

The CMS Administrator is responsible for making final decisions regarding external breach notification, and issuing written notification to individuals affected by a privacy breach.

6. APPLICABLE LAWS/GUIDANCE

6.1. LAWS

The following laws are applicable to this policy:

- **Privacy Act of 1974, as amended (5 U.S.C. 552a)** requires that agencies balance their need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal

agencies' collection, maintenance, use, and disclosure of personal information about them.

- **Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503), as amended,** establishes procedural safeguards affecting agencies' use of Privacy Act records in performing certain types of computerized matching programs.
- **Paperwork Reduction Act of 1995 (PRA)** requires agencies to perform information resource management activities in an efficient, effective, and economical manner.
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191)** is designed to protect confidential healthcare information through improved security standards and Federal privacy legislation.
- **Government Paperwork Elimination Act of 1998** develops procedures for the use and acceptance of electronic signatures by executive agencies.
- **Federal Information Security Management Act (FISMA) of 2002** requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to OMB.
- **E-Government Act of 2002 (P.L. 107-347)** requires agencies to develop performance measures for implementing E-Government. The Act also requires agencies to support Government-wide E-Government initiatives and to leverage cross-agency opportunities to further E-Government. In addition, the Act requires agencies to conduct and submit to OMB, Privacy Impact Assessments for all new IT investments administering information in identifiable form collected from or about members of the public.

6.2. REGULATIONS AND GUIDANCE

The following regulations and guidance are applicable to this policy:

- **President's Management Agenda** addresses Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, Expanded Electronic Government, Budget, and Performance Integration.
- **OMB Circular A-123, Management's Responsibility for Internal Control,** and the statute it implements, the **Federal Managers' Financial Integrity Act of 1982, revised December 21, 2004,** provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.
- **Circular A-130, Management of Federal Information Resources, November 30, 2000,** establishes policies for the management of Federal information resources to include procedural and analytical guidelines for implementing specific aspects of the Circular.
- **OMB Circular A–130, Appendix III – Security of Federal Automated Information Resources**, establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and

agency management control systems established in accordance with OMB Circular A-123.

- **OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, February 28, 2000,** reminds agencies of OMB's principles for incorporating and funding security as part of agency IT systems and architectures and of the decision criteria that will be used to evaluate security for information systems investments.
- **OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003,** provides guidance on implementing the privacy provisions of the E-Government Act of 2002.
- **OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, August 23, 2004,** describes the integration of security and capital planning through the plan of action and milestone (POA&M) weakness mitigation process.
- **OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006,** requires all government agencies to implement the appropriate safeguards for the protection of sensitive information.
- **OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006,** provides recommendations for planning and responding to data breaches which could result in identify theft.
- **OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007**, requires agencies to develop and implement a breach notification policy while ensuring proper safeguards are in place to protect the information.
- **Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004,** establishes standards for categorizing information and information systems.
- **NIST Special Publication 800-53 Rev. 1, Recommended Security Controls for Federal Information Systems, December 2006,** provides guidance and recommendations for implementing security controls for enforcing encrypted remote access and storage of PII.
- **HIPAA Privacy Rule (45 CFR Parts 160 and 164)** provides guidance regarding the use of PII.
- **HHS Privacy Act Regulations, 45.C.F.R. Part 5b**, establishes policies and procedures for the establishment of, maintenance of, notification of and/or access to, correction of and/or amendment of individual records relevant or necessary to accomplish a function of the Department of Health and Human Services.
- **HHS Memorandum ISP-2007-005, Departmental Standard for the Definition of Sensitive Information, June 11, 2007,** establishes a Departmental definition of sensitive information based on OMB Memorandum M-06-16.
- **HHS Rules of Behavior for Use of Program Support Center Enterprise Support Service Systems,** provides the rules that are to be followed by all users (contractors and

employees) that use any networked or standalone Enterprise Support Service (ESS) System that supports the mission and functions of the ESS and any sub-organizations.

- **CMS Information Security Policy, CMS-OA-POL-SEC01, September 10, 2003,** establishes the high-level policy for the CMS Information Security Program as required by the FISMA.
- **CMS Policy for the Information Security Program, CMS-CIO-POL-SEC02, May 2005, as amended,** provides the details of the CMS Information Security Program.
- **CMS System Security Levels by Information Type, Version 2.0, July 7, 2006,** establishes criteria for classifying CMS information and information systems as a basis for assessing the risks to CMS operations and assets and in selecting appropriate security controls and techniques.
- **CMS Information Security Acceptable Risk Safeguards, Version 2.0, March 13, 2006, as amended,** provides technical guidance to CMS and its contractors as to the minimum level of security controls that must be implemented to protect CMS' information and information systems.
- **CMS Integrated IT Investment & System Life Cycle Framework, March 2005, as amended,** provides a comprehensive set of policies, processes, procedures, artifacts, reviews, resources, and standards that prescribe CMS' requirements and guidance for IT investment and system life cycle management.

7. INFORMATION AND ASSISTANCE

Contact the Director of the OIS/EASG/DPC for further information regarding this policy.

8. EFFECTIVE DATE/IMPLEMENTATION

This policy becomes effective on the date that CMS' CIO signs it and remains in effect until officially superseded or cancelled by the CIO.

9. APPROVED

/s/ 7/23/2007

Julie C. Boughn
CMS Chief Information Officer and
Director, Office of Information Services

Date of Issuance

10. ATTACHMENTS

The following documents augment this policy:

- Procedure: Establishment/Revision of a System of Records (SOR)
- Procedure: Establishment/Revision of a Computer Match Agreement (CMA)
- Procedure: Establishment/Revision of a Data Use Agreement (DUA)
- Procedure: Request for Privacy-Protected Data
- CMS Information Security Incident Handling and Breach Analysis/Notification Procedure
- CMS Beneficiary Confidentiality Board Charter
- CMS Privacy Board Charter

GLOSSARY

Computer Match Agreement (CMA)

A written agreement that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data where there is a computerized comparison of two or more automated SORs. In conjunction with a CMA, an Inter/Intra-agency Agreement (IA) or Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) is also prepared when the SOR(s) involved in the comparison are the responsibility of another Federal agency.

Data Use Agreement (DUA)

A legal binding agreement between a Federal agency and an external entity (e.g., contractor, private industry, academic institution, other Federal government agency, or state agency), when an external entity requests the use of PII that is covered by the Privacy Act of 1974. The agreement delineates the confidentiality requirements of the Privacy Act, security safeguards, and the Federal agency's data use policies and procedures. The DUA serves as both a means of informing data users of these requirements and a means of obtaining their agreement to abide by these requirements. Additionally, the DUA serves as a control mechanism through which the Federal agency can track the location of its data and the reason for the release of the data. A DUA requires that a SOR be in effect, which allows for the disclosure of the data being used.

Federal Register

The official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents, that is published by the Office of the Federal Register, National Archives and Records Administration (NARA) for review by the public. [U.S. Government Printing Office]

General Support System (GSS)

The physical platform and infrastructure upon which applications run (e.g. Mainframe systems, web servers, communications equipment). A GSS consists of interconnected information resources under the same direct management control which shares common functionality.

Information System

A discrete set of information technology, data, and related resources, such as personnel, hardware, software, and associated information technology services organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. [OMB Circular No. A-11]

Information Technology (IT)

Equipment or interconnected systems that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. [OMB Circular A-130]

Inter/Intra-agency Agreement (IA)

A written agreement between an HHS component(s) and another Federal agency(s) (Inter-Agency), or between two or more HHS components (Intra-Agency) to provide to, purchase from, or exchange services, supplies, or equipment. The legal authorities to enter into an IA are numerous, with the primary authority being the Economy Act -31 U.S.C. 1535 and other authorities such as the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), the Medicare Modernization Act of 2003 (MMA), etc., used when the nature of the IA requires a specific authority. An IA is classified as either "Reimbursable" or an "Exchange of Goods and Services" when there is no cost reimbursement to an agency or agencies. Goods may be such items as computers, computer software, communications equipment, vehicles, etc. Services include such items as the costs associated with the creation of datasets, IT or programmatic consulting services, disaster recovery services, etc.

IT Investment

An expenditure of money and/or resources for IT or IT-related products and services involving managerial, technical, and organizational risk for which there are expected benefits to the organization's performance. These benefits are defined as improvements either in efficiency of operations or effectiveness in services.

Limited Data Sets

Files containing beneficiary and/or physician level information that indirectly identify an individual. These files contain indirect identifiers such as date of birth, diagnosis, State/county, etc. that in combination with other data elements and/or data files, could be used to deduce the identity of the individual. CMS protects these data files under the same manner as identifiable data files requiring review, approval, and a completed and signed DUA.

Major Application (MA)

Systems, usually software applications, which support clearly defined business functions for which there are readily identifiable security considerations and needs (e.g. Eligibility Data Base, Group Health Plans, Financial Accounting and Control System). An MA may also consist of multiple individual applications if all are related to a single major business function.

Memorandum of Understanding (MOU) / Memorandum of Agreement (MOA)

An instrument used when Federal agencies enter into agreements with other Federal agencies, or in some cases non-Federal agencies, for the purpose of establishing a joint project in which they each contribute their own resources and the scope of work is very broad and generally not specific to any one project and there is no exchange of funds between the partners. A MOU/ MOA may provide for trailing IA(s) that will establish a reimbursable agreement between the partners of a MOU/MOA, where it is determined that funds need to be exchanged. The same legal authorities are applied to a MOU/MOA as are applied to the legal authority for an IA.

Non-Operational Contractors

Organizations that assist CMS with specific tasks or perform work for CMS that is not related to the payment of claims or enrollment activities (e.g., organizations tasked to create or maintain a database, conduct analysis of a program, or perform a demonstration).

Operational Contractors

Organizations that are either a covered entity in their own right or have a business associate agreement with CMS. Operational contractors are those that perform the work of CMS by paying claims or processing enrollments on behalf of CMS or Medicare beneficiaries (e.g., Fiscal Intermediaries, Carriers, Medicare Advantage plans, and Prescription Drug Plans).

Personally Identifiable Information (PII)

Information which can be used to distinguish or trace an individual's identity (e.g., 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 (e.g., date and place of birth, mother's maiden name, etc.). PII includes individually identifiable health information as

defined by the HIPAA Privacy Rule (45 CFR Section 164.501). PII is also often referred to as personally identifiable data or individually identifiable information.

Privacy Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any other similar act where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

Privacy Impact Assessment (PIA)

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [OMB Memorandum M-03-22]

Public Use File (PUF)

Files that contain statistical/aggregate information that is approved for dissemination to the public. A PUF does not contain any PII making identification or deduction of an individual impossible.

Record

Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. [Privacy Act of 1974]

Routine Use

The use of a record for a purpose that is compatible with the purpose for which it was collected.

Sensitive Information

Information is considered sensitive if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. [HHS Memorandum ISP-2007-005] By definition, PII is considered to be sensitive information.

System of Records (SOR)

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. [Privacy Act of 1974]