UNIVERSITY OF PITTSBURGH POLICY 10-02-08

CATEGORY: SUPPORT SERVICES
SECTION: Computing, Information, and Data
SUBJECT: Use and Management of Social Security Numbers and University Primary ID ("UPI") Numbers
EFFECTIVE DATE: January 26, 2018 Revised
PAGE(S): 8

I. POLICY

The University of Pittsburgh is committed to maintaining the privacy and confidentiality of Social Security numbers (SSNs). The University is cognizant of the risk the improper disclosure of SSNs can have on individuals who have entrusted this information to the University, including the risk of identity theft. Therefore, it is the University's policy that the collection, management, and display of SSNs be controlled and that the use of a SSN as an identification number is limited.

SSNs may only be requested in certain cases (e.g., when required by law or for business purposes with certain third-party providers) and with appropriate disclosure of its use. Online and offline systems that maintain SSN data must have adequate security controls implemented to protect its confidentiality and integrity.

The University Primary ID (UPI) number will serve as the primary identification number for University students, faculty, and staff. A UPI is assigned to all persons affiliated with the University, and is displayed on the University's Panther Card as part of this ID card's "2P" value.

Violations of this policy are to be reported to the University's Privacy Officer (abuse@pitt.edu).

II. SCOPE

This policy sets forth the framework for the University's collection, management, and use of Social Security numbers (SSNs) and is applicable to all University units.

This policy will not apply to clinical and patient systems maintained by the University that are required to use the SSN for billing and healthcare coordination purposes.

SSNs are considered an identifier under the Health Insurance Portability and Accountability Act (HIPAA).

III. REQUIREMENTS FOR APPROPRIATE USE AND MANAGEMENT OF SOCIAL SECURITY NUMBERS (SSNs)

Collection of SSNs for University records

SSNs may be collected and recorded when needed by federal or state governmental agencies or by outside third parties who are mandated to collect SSN information (example: healthcare providers). Other reasons for collecting SSNs must be within the scope of this policy or approved by the University's Privacy Officer.

University employees authorized to collect SSNs may request a SSN during the execution of their duties if a primary means of identification, such as the UPI number, is not known or available.

University employees may not collect SSNs, except for those purposes noted below. Exceptions will require approval from the University's Privacy Officer.

- **Enrollment:** Those wishing to enroll in academic offerings at the University— both credit and non-credit—may be required to provide a SSN for secondary identification purposes. IRS regulations require the University to request a SSN as a taxpayer ID number for use in tax reporting. In addition, any student applying for financial aid must provide a SSN to the University.

- If a person enrolling in a University academic offering—credit or non-credit—cannot provide a SSN, certain services (e.g., transcripts, enrollment verification, tax reporting, and financial aid) may not be available to the individual, and the University cannot guarantee a complete academic record for the individual.

- **Immigration Law:** A SSN may be collected as necessitated by immigration law or regulations as determined by OHR International Scholars and Faculty Visa Services or the Office of International Students.

- **Certification Exams/Cooperative Experiences/Internships**: A SSN is required to be collected and reported for students who are taking certification exams if mandated by the certifying agency. Employers participating in co-ops and internships may also require the student to provide a SSN.

- **Employment:** Any person employed by the University must provide a SSN as the taxpayer ID number as directed by the IRS. This includes all employees, including part-time and student employees. Providing the SSN is a condition of employment. Applicants for employment must also provide a SSN, if requested, for mandatory background checks.

- **Employee Benefits:** If required by a benefits' provider, the SSNs of dependents may be collected to receive service. The University may also release an employee's SSN to benefit providers.

- **Payment for Personal or Professional Services:** Any person providing services to the University as an independent contractor, invited speaker (honorarium), or research subject for which payment will be made, must provide a SSN as the taxpayer ID number per IRS regulations. These taxpayer ID numbers will be stored in the accounts payable system as part of the vendor record.

- **Planned Giving Donors:** Donors participating in planned giving programs must provide a SSN as the taxpayer ID per IRS regulations.

- **Campus Police:** Because the SSN is, and will continue to be, a primary identifier for law enforcement and criminal justice records, Campus Police has access to SSN information in all University systems. Suspects and defendants will be asked for their SSN because it is used as a personal identifier in criminal justice databases (e.g. FBI NCIC, criminal history records, etc.), on citation forms, on criminal complaints, and in local police databases.

- **Other Entities:** The SSN may be released to entities outside the University where required by federal or state law, regulation or procedure, or if the individual grants permission.

Collection of an individual's SSN may have additional privacy considerations. These cases must be reviewed with the University's Privacy Officer and the Office of General Counsel to determine appropriate handling.

<u>Maintaining the Security and Privacy of SSNs</u>

All records containing SSNs, whether online or offline, will be considered confidential information and should be maintained appropriately to protect the confidentiality and integrity of this information.

The University will take reasonable precautions to protect SSNs for all individuals who provide it.

A SSN may not be used as a primary identifier in a University system, including indexing systems for imaged documents, unless the University's Privacy Officer has approved an exception.

If and when records including SSNs are no longer needed, disposal of the records must follow University information retention and destruction policies and procedures.

SSNs are considered to be confidential data and may not be used for purposes of data mining.

SSNs may not be used, in part or in whole, as a user ID or password for accessing a computer system or for generating any type of identifier.

If a SSN must be displayed on a computer monitor, a computer printout, a mailing, a fax, or another visible medium, all but the last four digits of the SSN must be masked.

SSNs may not be included in emails either as direct text or as part of an email attachment.

SSN data moved from one computer to another over a network interface must be transferred using encryption controls to protect the integrity and confidentiality of this information. Examples of encryption controls include cryptorouters and the use of the Secure File Transfer Protocol (STFP). Data transfer methods using cleartext (such as FTP) or ASCII files are inherently insecure and should be avoided.

SSNs in their entirety or in any portion may not be used nor posted where they can be exposed to the public (e.g., time cards, class rosters, grade rolls, and bulletin board announcements).

SSNs may not be used as an identifier for the collection of data for research or academic purposes, unless the University's Privacy Officer has approved an exception.

University units that collect, manage, and disseminate SSNs must undertake annual audits to demonstrate that processes and controls are in place to maintain the integrity and confidentiality of SSN data.

<u>Security Controls for Computer Systems Maintaining SSNs</u>

University units which require the storage of SSNs within their computer systems must have permission from the University's Privacy Officer.

University systems containing SSNs, whether hosted internally or in the cloud, must maintain a system security plan and undergo an annual system security review. At the discretion of the University's CISO, security reviews may be required when changes are made to the system.

Systems storing SSNs must contain security controls that protect the integrity and confidentiality of this information. Controls must include:

- System access controls must be integrated into the University's single sign-on solution which requires multi-factor authentication where possible. In addition, a user's access to information must only be granted based on job responsibilities.

- Network security controls, in which any system with SSNs must be protected by a network firewall.

- Audit controls, in which access to a system with SSNs is logged. Failed log-in attempts and other information that indicate unauthorized attempts to access SSNs must also be logged. Audit logs must be integrated into the University's centralized logging tool.

- Security monitoring controls, in which viruses, worms, spyware, Trojan horses, computer hackers, and other computer threats can be detected. These controls can include anti-virus and anti-spyware software.

- Physical security controls that restrict access to servers and workstations managing SSN data, as well as that protect electronic storage media (such as disks, backup tapes, and CD ROMS) that store SSN data.

- Any media where SSNs are stored must be encrypted.

- Disposal of media containing SSNs must follow the University's established disposal guidelines.

Files that cross-reference UPI numbers to SSNs are prohibited, unless approved by the University's Privacy Officer.

Suspected breaches involving SSNs must be immediately reported to the University's Help Desk, (412) 624-4357.

SSNs Within Historic Records

SSNs may be a part of historical databases or imaged documents given its past use as the primary identifier at the University. SSNs may not be used as a primary identifier in a University system—including as an indexing system for imaged documents—unless the University's Privacy Officer grants permission. If permission is not granted, the indexes must be changed to use UPI numbers or another key; otherwise the documents must be purged from the system.

Access to imaged or other online documents containing SSNs must be limited to authorized persons and secured using authorization controls, including passwords.

Local departmental databases or spreadsheets containing SSNs, which are available through local servers or PCs, are not permitted.

If faculty or others have email or other electronic correspondence that contains a SSN in the text, this will be considered historical information and does not have to be converted, but must be handled as confidentially as possible and purged if no longer required.

Historical records containing SSNs in offline storage (e.g., paper, tape, cartridge, fiche, microfilm, or magnetic media) may be maintained, but access to these offline records must be limited and secure.

All records that are no longer needed must be purged and disposal of the records must follow University Archives and Records Management policies and procedures.

SSNs Shared with Third Parties

SSNs may not be shared with third parties, with the exceptions of:

- As required or permitted by law.

- With the consent of the individual.

- Where the third party is an agent or contractor for the University and have demonstrated that controls are in place to prevent unauthorized distribution.

- As approved by the University's Privacy Officer.

SSNs shared with a third party that is an agent or contractor for the University must have a written agreement on controls and procedures that will be enacted and sustained to protect the confidentiality of these SSNs. The University should hold the third party accountable for compliance with the provisions of the written agreement through regular monitoring or auditing. The agreement should prohibit the third party from disclosing SSNs except as required by law and require the third party to use adequate administrative, physical, and technical safeguards to protect the confidentiality of records or record systems containing SSNs. The agreement should give the University the right to conduct audits to independently validate that these controls and procedures are in place and properly sustained.

IV. REQUIREMENTS FOR USING UNIVERSITY PRIMARY ID (UPI) NUMBERS

Use of UPI Numbers

The UPI is to be used as the primary identifier in the University's administrative and academic systems.

The UPI is an 11-character value beginning with "2P" and then a nine-digit number using the following format: 2PXXXXXXXXX

The UPI is unique to an individual and is a lifetime assignment used for multiple and changing relationships with the University.

The UPI number is assigned to an individual and is used for all affiliations with the University.

The UPI number for an individual will not be available to the general public, such as through the University Directory Service.

The UPI number may only be used in email or other correspondence within the University among appropriate University personnel and offices in performing their assigned duties, or in email or other correspondence sent directly to that individual. The UPI should never be part of the subject line of an email or printed on the address label of written correspondence.

Unless the full number is required (i.e., to notify an individual of his or her UPI number), only the last four digits of the UPI should be displayed in the text of an email or any other correspondence.

UPI numbers will be assigned to the following groups: students, employees, and other University affiliates.

- **Students:** A UPI is issued to anyone enrolling in University academic —including credit and non-credit instruction—that are recorded in the Student Information System (PeopleSoft). The UPI is the identifier of individuals within University academic systems and will be available to appropriate University officials with a legitimate educational need for the records. Students will be required to provide the UPI when requested to obtain access to services at the University.

  NOTE: Under interpretations of Family Educational Rights and Privacy Act of 1974 (FERPA) regulations, the UPI cannot be used to display a student's scores or grades publicly. This also precludes posting grades using only the last four digits of the UPI.

- **Employees:** All University employees, including wage payroll, are issued a UPI at the time of employment. The UPI will be used to identify the individual within University administrative systems. University retirees will also be assigned UPIs under this affiliation.

- **Other Entities:** There are other constituents associated with the University who may be issued a UPI. These include—but are not limited to—alumni, donors, and "friends of the University." The

University's Privacy Officer will determine when a UPI may be issued for those falling into the "other entities" category.

If an individual does not have a UPI, one will be assigned. Assigning a UPI will require certain minimum information about the individual. Those University offices assigning UPI must notify constituents of their new UPI in a timely manner, using consistent methods and wording.

Efforts must be made to prevent assignment of multiple UPIs to the same individual. If multiple UPIs have been issued to a single individual or if two individuals are issued the same UPI, the University unit discovering the duplicate or multiple must contact Panther Central and—after verification of the multiple assignments—the records will be merged or separated and the individual or individuals notified of which UPI will be valid in the future.

If an assigned UPI has been compromised and used fraudulently, an individual may request a new UPI number, subject to the review and approval of the University's Privacy Officer.

Use of UPI Numbers on the University's Panther Card

The UPI may be printed on the Panther Card as part of the card's 2P value so that individuals have a permanent record of their UPI for reference purposes. Individuals issued Panther Cards will be expected to keep the card secure. Panther Cards must have a brief disclosure statement on the back of the card regarding the individual's responsibility for keeping his/her Panther Card secure.

If a Panther Card must be replaced, the UPI will remain the same, but a new 2P card number will be issued.

2P numbers should consist of the following fields:

- Eleven-digit UPI
- Two-digit card type (01 students, 02 faculty and staff, 03 other affiliates)
- One-digit lost card indicator (starting with 0 and incrementing with each new card number)
- One-digit check digit based on a modulus 36-hash function (this check digit is used to validate the first 14 digits).

2P numbers are to be generated using the University's Central Directory Service (CDS) and issued when University affiliates receive their Panther Cards on the Pittsburgh campus by Panther Central or when their ID cards are received at one of the University's regional campuses.

V. SANCTIONS

It shall be the responsibility of each University unit to meet the requirements set forth in this policy. Violation of this policy may result in disciplinary action up to and including termination of employment. Violation may also result in civil and criminal penalties based on state and federal privacy statutes.

VI. ADDITIONAL INFORMATION

For additional information about this policy or to file a report, contact the University's Privacy Officer:

David N. DeJong, Ph.D.
Vice Provost for Academic Planning and Resource Management
801 Cathedral of Learning
Pittsburgh, PA 15260
Email: dejong@pitt.edu
Web site: http://www.provost.pitt.edu/
Personal: http://www.pitt.edu/~dejong/
Phone: (412) 624-4228

For information about security controls for protecting SSNs, contact the University's Information Security Officer.