



# SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

February 2018

## Abstract

A guide to identify and protect personally identifiable information (PII)  
at Oklahoma City University.

Oklahoma City University

## Table of Contents

Introduction .....	2
1.0 The difference between PII and Sensitive PII.....	3
1.1 PII that is always Sensitive .....	3
1.2 PII that is Sensitive in certain contexts .....	3
2.0 Safeguarding Sensitive PII .....	4
2.1 Collect Sensitive PII only as authorized.....	4
2.2 Limit use of Sensitive PII .....	4
2.3 Minimize proliferation of Sensitive PII.....	5
2.4 Secure Sensitive PII .....	5
3.0 Privacy Incident Reporting.....	6
3.1 How to report a privacy incident .....	7
3.2 Do not further compromise the information .....	7
Appendix A: Encrypting a file .....	8
Appendix B: Securing an email for internal recipients.....	9
Appendix C: Securing an email for external recipients.....	10
Appendix D: Frequently Asked Questions .....	10

## Introduction

As someone who works for or on behalf of Oklahoma City University (OCU or University), it is your responsibility to protect information that has been entrusted to the University. An important part of this duty is to ensure that you properly collect, access, use, share, and dispose of Personally Identifiable Information (PII).

You should exercise care when handling all PII. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised.

This document provides minimum standards that apply to every OCU employee, contractor, intern, and consultant. Your department head, the system owner, or others responsible for the security of PII data may set additional or more specific rules for handling PII based on the sensitivity of the information involved.

This document explains:

- How to identify PII and Sensitive PII,
- How to protect Sensitive PII in different contexts and formats, and
- What to do if you believe Sensitive PII has been compromised.

This document was adapted and largely duplicated from the Department of Homeland Security's document titled *Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012)*.

## 1.0 The difference between PII and Sensitive PII

The Department of Homeland Security and the Department of Education defines personal information as “Personally Identifiable Information” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

Some categories of PII are sensitive as stand-alone data elements. Examples include: SSN, driver’s license number, passport number, or financial account number. Other data elements such as immigration status, medical information, ethnic, religious, sexual orientation, school grades, and account passwords, in conjunction with the identity of the individual (directly or indirectly inferred), are also Sensitive PII.

### 1.1 PII that is always Sensitive

What is PII?	
<b>PII includes:</b> Name, email, home address, phone number	
<b>Sensitive PII includes:</b>	
<b>If stand-alone:</b>	<b>If paired with another identifier:</b>
Social Security Number	Medical information
Driver’s license or state ID number	Ethnic or religious affiliation
Passport number	Sexual orientation
Alien registration number	Account passwords
Financial account number	Last 4 digits of SSN
	Date of birth
	Criminal history
	Mother’s maiden name
	Banner ID number

### 1.2 PII that is Sensitive in certain contexts

Context matters. PII that might not include the data elements identified in 1.1 may still be sensitive and require special handling if it could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual.

For example, a collection of names:

- Is **not** Sensitive PII if it is a list, file, query result, etc. of:
  - Attendees at a public meeting

- Members of a university committee or group
- Employees and students in the Campus Directory
- **Is** Sensitive PII if it is a list, file, query result, etc. of:
  - Students with their grades
  - Employees with poor performance ratings
  - Students on academic probation

## 2.0 Safeguarding Sensitive PII

You should exercise care when handling all PII. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised. The following guidelines explain how you must properly collect, access, use, share and dispose of Sensitive PII at the University.

### 2.1 Collect Sensitive PII only as authorized

When collecting Sensitive PII, be sure that you have the University's authority to do so. You may be required to attend ongoing data security training, sign a policy signifying your understanding and commitment to following University defined practices for data security, attain an official sign-off to access sensitive data, and/or other practices.

Other agencies may require the University follow certain guidelines and regulations related to particular Sensitive PII. You should ensure you understand these requirements and follow the appropriate practices. Some examples include:

- If you are collecting or maintaining student information considered Sensitive PII, insure you are following all guidelines and regulations outlined by the Family Educational Rights and Privacy Act (FERPA).
- If you are collecting or maintaining medical information for individuals, insure you are following all guidelines and regulations outlined by the Health Insurance Portability and Accountability Act (HIPAA).

When collecting PII from members of the public, ensure that all paper or electronic forms or processes are reviewed and approved by your supervisor prior to collection.

### 2.2 Limit use of Sensitive PII

Only access or use Sensitive PII when you have a need to know that information as it relates to your official duties. If you are unsure about whether a specific use is appropriate, you should confirm with your supervisor.

If you are a contractor or other 3<sup>rd</sup> party to the University, you may be required to provide a nondisclosure agreement and other documentation stating your understanding and responsibilities prior to handling Sensitive PII.

**Never** browse files containing Sensitive PII out of curiosity or for personal reasons.

## 2.3 Minimize proliferation of Sensitive PII

Minimizing proliferation of Sensitive PII helps to keep it more secure and reduces the risk of a privacy incident.

Refer requests for Sensitive PII from members of the media to the University's Communications and Marketing department.

### Limit the sharing of Sensitive PII:

You are authorized to share Sensitive PII internally with other University employees or contractors, or externally with outside entities, only if the recipient's need for the information is related to his or her official duties. Formal authorization may be required before these recipients access Sensitive PII.

### Creating data extracts of Sensitive PII:

Do not create unnecessary or duplicative collections of Sensitive PII, such as duplicate, ancillary, "shadow," or "under the radar" files. In some instances, it may be appropriate to create new spreadsheets or databases that contain Sensitive PII from a larger file or database. Before doing so, consult your supervisor and ensure you are following all designated minimum requirements to secure the data. When you need to print, copy, or extract Sensitive PII from a larger data set, limit the new data set to include only the specific data elements you need to perform the task at hand. Additionally, if you need to create duplicate copies of Sensitive PII to perform a particular task or project, delete or destroy them when they are no longer needed.

## 2.4 Secure Sensitive PII

When you handle, process, transmit, transport and/or store Sensitive PII, you should limit the potential for unauthorized disclosure. For example, protect against "shoulder surfing" or eavesdropping by being aware of your surroundings when processing or discussion Sensitive PII.

### PII in electronic form:

Sensitive PII should only be accessed via University-approved portable electronic devices (PEDs) such as laptops, USB flash drives, and external hard drives. PEDs must be encrypted when storing Sensitive PII. Personally-owned USB flash drives or other external storage devices may not be used.

Personally owned computers should not be used save, store, or host Sensitive PII. Sensitive PII can be accessed from a personally owned computer through a University Virtual Desktop or through a University approved secure web interface. When authorized by your supervisor and approved through CTS, you may access Sensitive PII stored on your University desktop computer or University file share remotely via a virtual private network (VPN). This data must not be moved or copied from these University locations to your personal computing device.

### Transporting hard copy PII:

Obtain authorization from your supervisor before removing documents containing Sensitive PII from the workplace. Do not take Sensitive PII home or to any non-University approved worksite, in either paper or electronic format, unless appropriately secured. Paper documents must be under the control of the employee or locked in a secure container when not in use.

Physically secure Sensitive PII when in transit. Do not mail or courier Sensitive PII on CDs, DVDs, hard drives, USB flash drives, or other removable media unless the data are encrypted. Also, do not pack laptops or electronic storage devices in checked baggage or leave them in a car for an extended period of time. Never leave paper files or electronic devices in plain site in an unattended vehicle. Additionally, do not return failed hard drives to vendors for warranty repair or replacement if the device was ever used to store Sensitive PII. These devices should be returned to CTS for proper handling.

#### Hard copy PII in the workplace:

**Never** leave Sensitive PII in hard copy unattended and unsecured.

Physically secure Sensitive PII (e.g. in a locked drawer, cabinet, desk, or safe) when not in use or not otherwise under the control of a person with a need to know. Sensitive PII may be stored in a space where access control measures are employed to prevent unauthorized access by members of the public or other persons without a need to know (e.g. a locked room or floor, or other space where access is controlled by a guard or card reader). But the use of such measures is not a substitute of physically securing Sensitive PII in a locked container when not in use.

Try not to send Sensitive PII using a fax machine. If possible, scan and then encrypt the document(s) and email it. If the information must be sent by fax, do not send Sensitive PII to a fax machine without contacting the recipient to arrange for its receipt.

#### Emailing PII:

**Within OCU:** You can email Sensitive PII without protection if the recipient's need for the information is related to his or her official duties. Email traffic between University email accounts is secure. However, if you have any doubt about the recipient's need for the information, or to ensure protection, you are strongly recommended to password-protect Sensitive PII you email within the University, or redact Sensitive PII before you email or print it. Refer to Appendix A for techniques to encrypt file attachments. Refer to Appendix B for the process to limit email access to only University email addresses.

**Outside of OCU:** Two methods exist to securely email Sensitive PII to an external recipient: send the PII in an encrypted mail attachment (see Appendix A for details), or encrypt the message so external recipients must access the email through a secured web portal (see Appendix C for details).

#### Storing PII on shared drives or SharePoint site:

Store Sensitive PII on shared access computer network drives ("shared drives") or on a University SharePoint site only if access is restricted to those with a need to know by permissions settings or passwords. Consult with CTS for the processes to control access to a network shared drive folder and a SharePoint document library.

### 3.0 Privacy Incident Reporting

The University defines a **privacy incident** as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users and for an authorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both **suspected and**

**confirmed incidents**, whether intentional or inadvertent, involving PII which raise a reasonable risk of harm.

### 3.1 How to report a privacy incident

- You must report all privacy incidents, whether suspected or confirmed, to your supervisor immediately. If your supervisor is unavailable, or if there is a potential conflict of interest, report the incident to the University's Risk Manager, Chief Information Officer, or General Counsel.
- Document or maintain records of information and actions relevant to the incident, as they may be required in the privacy incident handling report.
- Any alleged violations that may constitute criminal misconduct, identity theft or other serious misconduct, or reflect systemic violations within the University, will be reported to the University's Risk Manager and General Counsel as part of the privacy incident reporting process.

### 3.2 Do not further compromise the information

Beware of these common mistakes so that your response to a privacy incident does not cause another incident:

- Do not forward compromised information (e.g. SSN, full name, birth date, etc.) when reporting an incident.
- If and when the compromised Sensitive PII is needed by your supervisor, Risk Manager, Chief Information Officer, or General Counsel in order to respond to an incident, you will be given instructions regarding the individual to send it to.
- If you see Sensitive PII in an email that you suspect constitutes a privacy incident, remember that the information is duplicated and further compromised if you forward or reply to it.

For more details related to privacy incident reporting, reference the University's *Data and Network Security Policy*.

## Appendix A: Encrypting a file

Encryption is the process of changing plain text into cipher text for the purpose of security or privacy. Many software applications exist that have the capability of encrypting files. It is the University's policy to use 256-bit AES encryption as the standard. When encrypting a file to secure Sensitive PII, ensure the application used to encrypt meets this as the minimum standard. Below are instructions for encrypting with WinZip, 7-Zip File Manager, and Adobe Acrobat Pro.

### To encrypt a file using WinZip:

1. Save the file that needs to be encrypted.
2. Open up Windows Explorer and locate the file.
3. Right click on the file.
4. Select "WinZip, Add to Zip file..."
5. The "Add" dialog box will open.
6. The "Add to archive" box should be automatically populated with your file path. If not, select "New" and pick the path where the zipped file will reside. Insert the name of the "File name" box and click "OK".
7. In the "Action" box, select "Add (and replace) files".
8. In the "Compression" box, select ".Zip: Legacy compression (maximum compatibility)".
9. In "Split Zip file" box, select "Don't split".
10. In the "Options" area, click the "Encrypt added files" check box and uncheck the "Include system and hidden files" box.
11. In the "Archive Attributes" area, do not select either option.
12. Click the "Add" button.
13. Click the "OK" button on the "WinZip Caution" dialog box.
14. On the "Encrypt" dialog box, enter a string of characters as a password composed of letters, numbers, and special characters (a minimum 8 characters, a maximum of 64) in the "Enter password" box.
15. Retype the password in the "Re-enter password (for confirmation)" box.
16. Check the "Hide the password" checkbox if it has not already been checked.
17. Select the "256-Bit AES encryption" radio button.
18. Click "OK".
19. You have successfully created the new Zip file which has the file encrypted and password protected in it. The new Zip file can now be attached to an email.

NOTE: In a **SEPARATE** medium (i.e. by phone or in person), send the password to the recipients of the email. As a last resort, the password can either be sent out by email prior to sending the file, or afterwards, but NEVER in the same email to which the file is attached.

### To encrypt using 7-Zip File Manager:

1. Save the file that needs to be encrypted.
2. Open up Windows Explorer and locate the file.
3. Right click on the file.
4. Select "7-Zip, Add to archive..."
5. The "Add to Archive" dialog box will open.

6. The “Archive:” box should be automatically populated with the location and file name of the archive to be created. Adjust as needed.
7. The “Archive format” should be set to “zip”.
8. In the “Encryption” section under “Enter password”, enter a string of characters composed of letters, numbers, and special characters (a minimum 8 characters, a maximum of 64).
9. Retype the password in the “Reenter password” box.
10. In the “Encryption method” dropdown box, choose “AES-256”.
11. Click “OK”.
12. You have successfully created the new Zip file which has the file encrypted and password protected in it. The new Zip file can now be attached to an email.

NOTE: In a **SEPARATE** medium (i.e. by phone or in person), send the password to the recipients of the email. As a last resort, the password can either be sent out by email prior to sending the file, or afterwards, but NEVER in the same email to which the file is attached.

#### To encrypt a PDF file using Adobe Acrobat Pro:

NOTE: Adobe Acrobat Professional software must be purchased. The recipient of the encrypted file will need Adobe Acrobat Reader the same version or higher than your version of Adobe Acrobat Pro.

1. Open up Windows Explorer and locate the file.
2. Make sure the file is in PDF format. If not, right click on the file and click “Convert to Adobe PDF” to save the file with a PDF extension.
3. With the PDF file open in Adobe Acrobat Pro, click “Advanced, Security, Encrypt with Password”.
4. Click “Yes” when prompted to change the security on the document.
5. Set “Compatibility” to “Acrobat 9.0 or later” so that the encryption level is 256-bit AES. Ensure that “Encrypt all document contents” is selected.
6. Check the box labeled “Require a password to open the document”.
7. Enter a password in the “Document Open Password” field. Please make sure the password is at least 8 characters long and is a combination of letters, numbers, and special characters. Click “OK”.
8. In the “Adobe Acrobat – Confirm Document Open Password” box, retype the password in the “Document Open Password” field.
9. Click “OK” if you see a message that the settings do not take effect until the document is saved.
10. Close the PDF document or close Adobe Acrobat Pro.
11. You have successfully created the new encrypted and password protected PDF file which. The new PDF file can now be attached to an email.

NOTE: In a **SEPARATE** medium (i.e. by phone or in person), send the password to the recipients of the email. As a last resort, the password can either be sent out by email prior to sending the file, or afterwards, but NEVER in the same email to which the file is attached.

## Appendix B: Securing an email for internal recipients

While email sent between two University email addresses is secure, you may further secure an email with Sensitive PII by:

- Placing the Sensitive PII in an encrypted file before sending the message (see Appendix A), or

- Adding the keyword “(okcu only)” in the subject line (make sure to include the parenthesis) so that the email system provides an extra layer of security, preventing it from being accessed by anyone without a University email address.

## Appendix C: Securing an email for external recipients

Extra caution should be taken when sending Sensitive PII to a recipient external to the University email system. Appendix A describes how to encrypt Sensitive PII in a password protected file before sending. A second method to protect Sensitive PII sent via email to external recipients is to include the keyword “(encrypt)” in the subject line (make sure to include the parenthesis) so that the email system routes the outbound email to an encrypted web portal where the external recipient can access the content with a one-time code.

## Appendix D: Frequently Asked Questions

These FAQs provide guidelines on how to protect Sensitive PII.

1. How can I protect Sensitive PII...
  - a. In the office?
    - i. Physically secure Sensitive PII (e.g., in a locked drawer, cabinet, desk, or safe) when not in use or not otherwise under the control of a person with a need to know. Sensitive PII may be stored in a space where access control measures are employed to prevent unauthorized access by members of the public or other persons without a need to know (e.g., a locked room or floor, or other space where access is controlled by a guard, cipher lock, or card reader). But the use of such measures is not a substitute for physically securing Sensitive PII in a locked container when not in use.
    - ii. Never leave Sensitive PII unattended on a desk, network printer, fax machine, or copier.
    - iii. Use a privacy screen if you regularly access Sensitive PII in an unsecured area where those without a need to know or members of the public can see your screen, such as in a reception area.
      1. Lock your computer when you leave your desk. Depending on your equipment, you may lock your computer by (1) holding down “+ “L”, (2) holding down “Ctrl”+ “Alt” + “Delete” and then hitting “Enter”.
      2. Do not permit your computer to remember passwords.
    - iv. Avoid discussing Sensitive PII in person or over the telephone when you are within earshot of anyone who does not need to know the information.
      1. If you must discuss Sensitive PII using a speakerphone or video teleconference, do so only if you are in a location where those without a need to know cannot overhear.
      2. Keep in mind that phone conversations are easily overheard between cubicles, so Sensitive PII is most securely discussed in an office or conference room behind a closed door.
      3. Remember that some places that seem private still pose a risk for unauthorized disclosure, such as in a taxicab.

- b. While traveling?
  - i. Sensitive PII should only be accessed via University-approved PEDs such as laptops, tablets, USB flash drives, and external hard drives, all of which must be encrypted.
  - ii. Personally owned computers should not be used to save, store, or host Sensitive PII. Sensitive PII may be accessed from a personally owned computing device through a secured web interface, a University Virtual Desktop, or a VPN connection.
  - iii. When transporting your laptop or PED:
    - 1. If you must leave it in a car, lock it in the trunk so that it is out of sight. Do not leave your laptop or PED in a car overnight.
    - 2. Do not store a laptop or PED in an airport, a train or bus station, or any public locker.
    - 3. Avoid leaving a laptop or PED in a hotel room. If you must leave it in a hotel room, lock it inside an in-room safe or a piece of luggage.
    - 4. At airport security, place your laptop or PED on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on it until you can pick it up. Never place a PED in checked luggage.
    - 5. If your PED is lost or stolen, report it as a lost asset to your supervisor and to CTS.
- c. While teleworking?
  - i. Sensitive PII should only be accessed via University-approved PEDs such as laptops, tablets, USB flash drives, and external hard drives, all of which must be encrypted.
  - ii. Personally owned computers should not be used to save, store, or host Sensitive PII. Sensitive PII may be accessed from a personally owned computing device through a secured web interface, a University Virtual Desktop, or a VPN connection.
    - 1. Do not move or copy files with Sensitive PII to your personal computing device.
    - 2. Do not print Sensitive PII on your home printer.
    - 3. Do not forward emails containing Sensitive PII to your personal email account (e.g., your Yahoo, Gmail, or Cox e-mail account) so that you can work on it on your home computer.
  - iii. Obtain authorization from your supervisor to remove documents containing Sensitive PII from the office.
  - iv. Secure your PED and any hard copy Sensitive PII while teleworking, and ensure that other household members cannot access them.
- d. In email or other electronic transfer?
  - i. **Within OCU:** You can email Sensitive PII without protection if the recipient's need for the information is related to his or her official duties. However, if you have any doubt about that, or to ensure protection, you are strongly recommended to password-protect Sensitive PII you email within the University,

or redact Sensitive PII before you email or print it. Refer to Appendix A for techniques to encrypt file attachments. Another line of security is to limit access of an email with Sensitive PII to only University email addresses. See Appendix B for details.

- ii. **Outside of OCU:** Two methods exist to securely email Sensitive PII to an external recipient: send the PII in an encrypted mail attachment (see Appendix A for details), or encrypt the message so external recipients must access the email through a secured web portal (see Appendix C for details).
  - e. When sending via facsimile (fax)?
    - i. Avoid faxing Sensitive PII if at all possible. If you must use a fax to transmit Sensitive PII, alert the recipient prior to faxing so they can retrieve it as it is received by the machine. After sending the fax, verify that the recipient received the fax.
  - f. In the interoffice mail?
    - i. Avoid sending Sensitive PII through interoffice mail when possible to limit the number of individuals who may possess the Sensitive PII material in transit. When it is necessary to use interoffice email, seal Sensitive PII materials in an opaque envelope or container.
  - g. In the outgoing mail?
    - i. For mailings containing a small amount of Sensitive PII materials:
      - 1. Seal Sensitive PII materials in an opaque envelope or container.
      - 2. Mail Sensitive PII materials using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service (e.g. UPS).
    - ii. For large data extracts, database transfers, backup tape transfers, or similar collections of Sensitive PII:
      - 1. Encrypt the data (if possible) and use a receipted delivery service (i.e. Return Receipt, Certified or Registered mail) or a tracking service (e.g. "Track & Return") to ensure secure delivery is made to the appropriate recipient.
  - h. On my departmental shared drive, SharePoint site, intranet, or public websites?
    - i. Do not post Sensitive PII on the University SharePoint collaboration sites, shared drives, multi-access calendars, other intranet sites, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know".
    - ii. Consult with CTS for assistance with the process to control access to a network shared drive.
    - iii. Consult with CTS for assistance with the process to control access to a SharePoint collaboration site.
2. How can I minimize my use of Sensitive PII?
- a. Whenever possible, minimize the duplication and dissemination of electronic files and papers containing Sensitive PII.
    - i. If you need to use a unique number or data element to identify individuals, use email addresses or Banner IDs instead of Social Security numbers.

- ii. Only print, extract, or copy Sensitive PII when the risk is justified by an official need that is not easily met using other means.
    - 1. For example, if you need to generate a list of employees and their salaries in a particular office for a project, query the payroll database to return only those employees' names and salaries (and not, for example, other sensitive data such as SSNs). If you cannot customize the reports generated by a database, consider loading the results into an Excel spreadsheet and deleting the data you do not need before saving the file and distributing it to others.
    - 2. Before emailing, printing or making paper copies, redact Sensitive PII that is not necessary for your immediate use or for a recipient to see.
- 3. Why shouldn't I store sensitive PII on unauthorized equipment?
  - a. University approved PEDs such as laptops, tablets, USB flash drives, and external hard drives, are encrypted. Encryption protects the data on the device from being accessed by an unauthorized user if the device is lost or stolen.
  - b. Non-university issued equipment, even if encrypted, may have unauthorized software or allow an unauthorized person to access the data. This equipment may also have viruses, spyware, or other technology that may cause harm to the University network, and could allow unauthorized access to University information, including Sensitive PII.
- 4. How do I secure Sensitive PII that cannot be encrypted, such as paper copies or some external media?
  - a. Sensitive PII in hard copy or stored on external media must be kept in a locked compartment, such as filing cabinet or desk drawer. Alternatively, hard copies can be scanned and password protected or encrypted. External media can be mailed using the instructions outlined in this document.
- 5. What are my responsibilities when requesting or receiving Sensitive PII?
  - a. When collecting Sensitive PII from members of the public, use only a University-approved paper or electronic form, and collect Sensitive PII directly from the individual to the extent possible.
    - i. For example, if a University employee is helping a student fill out financial aid information, the student should fill out his or her information whenever possible. This will limit unnecessary dissemination of that individual's personal data, and will also allow him or her to be aware of what information is being collected and to consent to releasing that information.
    - ii. As a best practice, every request you make for Sensitive PII should be accompanied by a reminder of how to properly secure the information. The University suggests the following reminder when requesting information from someone outside of the University: "The information I have requested is Sensitive Personally Identifiable Information. To properly secure this information, please send it within an encrypted and password-protected attachment with the password provided under a separate cover, such as in person, by phone, or in a separate email."
    - iii. If someone sends you Sensitive PII in an unprotected manner, you must protect that data in the same manner as all Sensitive PII you handle once you receive it.

1. For example, if someone outside of the University sends unsecured Sensitive PII in the body of an email to you, you must encrypt that data if you wish to email it to another non-University recipient.
  2. The University strongly recommends that you password-protect Sensitive PII you share within the University, or redact the Sensitive PII before you share or print it.
6. When and how should I destroy materials containing Sensitive PII?
  - a. Follow any and all retention and disposal policies required by your department. Sensitive PII, including archived emails containing Sensitive PII, shall be destroyed when retention of the data is no longer required, consistent with applicable record retention schedules.
    - i. Printed material must be destroyed using an approved shredder or shredding service.
    - ii. All Sensitive PII on diskettes must be permanently erased or destroyed.
    - iii. PEDs containing Sensitive PII must be sanitized by CTS or an authorized service when no longer needed by an employee or contractor.