Best Practices Guidelines for Handling
Sensitive Personally Identifiable Information

Introduction

As an employee of the University of Georgia, it is your responsibility to protect information that has been entrusted to you in the performance of your job responsibilities. An important part of this duty is to ensure that you properly collect, access, use, share and dispose of Personally Identifiable Information (PII). Sensitive PII requires special handling because of the increased risk of harm to an individual if it is compromised.

This best practices document explains how to identify PII and Sensitive PII and how to protect Sensitive PII in different contexts and formats.

What is PII? **PII includes: Name, email, home address, phone number** **Examples of Sensitive PII include[1]:**	
UGA Restricted Information	UGA Sensitive Information
Social Security Number &/or Last 4 digits of SSN	Records maintained relating to students, prospective students, donors and alumni
Driver's license or State ID #	UGA ID Number (aka 81x Number)
Passport number	Date of Birth
Financial account number/ Credit/debit card data	Research information related to sponsorship, funding, human subject, etc.
Account passwords	
Medical information	

Examples of UGA Documents that include Sensitive PII include:
Background Consent Forms
Information needed to request a new 810#
Individuals' W-9s for payments from Foundation Accounts
Scanned documents for I9 Uploads (e.g. drivers' licenses, Passports)
Faculty hiring packet documents (may include Visa documents, international Passports)
Foundation Scholarship forms prior to Fall 2014 (required SSN#)
Documentation necessary for H1B and permanent residency applications (e.g. scanned passports/Visas, etc.)
Internal hiring documentation which may contain 810# and/or SSN#
Checks received from the UGA Foundation
Checks received from donors
Credentialing information collected from staff, faculty and students

[1] For more information, see EITS's "Data Classification and Protection Standard" at: http://eits.uga.edu/access_and_security/infosec/pols_regs/policies/dcps/

Collect and Access Sensitive PII Only as Required
When collecting Sensitive PII, be sure that you have a specific job responsibility that requires you do to so. Likewise, only access or use Sensitive PII when you have a need to know that information as it relates to your official duties.

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

- Only share Sensitive PII if the recipient's need for the information is related to his or her official duties
- Do not create unnecessary or duplicative collections of Sensitive PII, including information stored on backup servers, network drives and/or your desktop
- **Delete** electronic files or **destroy** paper files (via shredder) when Sensitive PII is no longer needed, including information stored on backup servers, network drives and/or your desktop. Contact your supervisor or IT professional for directions on securely deleting electronic PII.

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 discussing Sensitive PII.

PII in electronic form:

- Sensitive PII should only be accessed via UGA equipment. Personally owned computers, equipment, and services (e.g Dropbox) should not be used to access, save, store or host Sensitive PII.
- Only store Sensitive PII on authorized computers and network drives with adequate security (e.g. access control, encryption, anti-virus software, data-loss prevention software, limited Internet access) in place. NEVER upload UGA Restricted Information (defined above) to OneDrive. Contact your supervisor or IT professional to determine if a system is authorized to store Sensitive PII.
- Departments should contact Tommy Jones, EITS Sr. Mgr., Client Tech Support, at tomjones@uga.edu for more information regarding the use of a virtual computer and secure network drives for long-term storage of Sensitive PII.

Hard copy PII:

- Do not take Sensitive PII from your work area, unless appropriately secured. Paper documents must be under the control of the employee or locked in a secure file drawer when not in use
- ***Never*** leave Sensitive PII in hard copy unattended and unsecured.
- Do not use campus mail to transport Sensitive PII
- Try not to send Sensitive PII using a fax machine. Scan the document and use UGA's Send Files to transmit the document to the receiver. 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.

Appendix A: SendFiles – Information and Frequently Asked Questions
Appendix B: Frequently Asked Questions Regarding Sensitive PII

Appendix A: SendFiles – Information and Frequently Asked Questions

SendFiles is an encrypted file service that allows you to securely share sensitive documents and large files online. Anyone with a UGA MyID can use SendFiles.

Using SendFiles you can transfer files up to 2GB in size and the service offers more than one solution for sending and receiving files.

How do I access SendFiles?

SendFiles is available at https://sendfiles.uga.edu

- If you have a UGA MyID, you should use your **MyID** and **MyID password** to login.
- If you do not have a UGA MyID, you should use the link that you were sent to access the service initially to set up a password. After that initial access, you should use your email address and the password that you setup to access the system. Non-MyID accounts will expire 7 days after their last activity and deleted 7 days after expiration.

How do I create an account?

Simply log in at https://sendfiles.uga.edu with your MyID and your MyID password. Your account will be created automatically upon first logging in.

What's the largest file I can send?

You can send secure messages with the total attachment size of 2GB. That means many small files that can add up to 2GB or one big 2GB file.

So if I can send large files, does that take up space in my UGAMail mailbox?

No, all messages and attachments sent through the SendFiles service never make it to your UGAMail mailbox, Inbox or Sent Items. The only items that go to your UGAMail mailbox are the notification messages, which are very small.

My secure messages are sitting in my MoveIT Outbox. Why aren't they sending?

Right click on the MoveIT task bar icon in the the bottom right hand corner and click on Pending Transfers. If you have pending transfers, then right click on the icon again and click Configuration. Verify that all your settings are correct and re-type in your MyID password. If this does not remedy the issue, please make sure that you do have access to the Internet as well. If you do, please contact the EITS Help Desk for further assistance.

Can I send a secure message or a file to (or receive one from) someone without a UGAMail email address?

Yes, you can. To send a message, simply address the email message to the person of your choice. They will be notified at that email address and will have a temporary account set up for them to access your message or files.

If you want to have someone from a non-UGA email address to send you a file, you must first send them a message through SendFiles so that a temporary account can be made for them. Once that is done, they will be able to log into and send files from SendFiles.

All of the messages and files that I've sent and received have disappeared from my SendFiles mailbox folder. Where did they go and can I get them back?

All of the messages and files sent by you and received by you are stored in your SendFiles mailbox folders for up to 30 days. This is not a setting that can be changed. The messages and

files can not be restored. If you need to keep a message or a file longer than 30 days, you will need to download it and upload it to your Home folder to permanent storage.

How big is my Home folder? How much can I keep there?
The folder size quota on your Home folder (which includes all subfolders) is 2GB. You can keep as many files and folders there as you wish as long as they are under 2GB total.

What if I need more space?
Departments can request additional folder space through the Office of Information Security, if it's deemed necessary for the storage of sensitive information. Requests can be addressed to the EITS Help Desk. Individual accounts can not be granted additional space in their Home folders. If a department needs additional storage space, there are other options available. Please contact the EITS Help Desk for more information on these offerings.

I just changed my MyID and all of my files are gone. Can I get them back?
Please contact the EITS Help Desk, and we can make the appropriate changes to your SendFiles account so that you may have access to your files again.

Why am I not able to send to a UGA recipient? I've been able to send messages to this person in the past.
The recipient's account may be inactive in SendFiles. Please contact the recipient via UGAMail or by phone and ask for them to contact the EITS Help Desk to resolve this issue with their account in SendFiles.

Other Known Issues
If you encounter a problem when sending to a UGAMail email address, please try typing the recipient's email address in the To field rather than adding them from the Outlook Global Address Book or your Auto-Complete. This is a known issue that is currently being worked on by the product provider.

Microsoft Office applications might freeze or become unresponsive if you utilize the Send and Save option under File. This is because the MoveIT Attach File program is hidden in the background. Minimize your programs and cancel out of the MoveIT Attach File program to continue.

Visit the EITS SendFiles wiki page or contact the EITS Help Desk for more information on using SendFiles

Appendix B: Frequently Asked Questions Regarding Sensitive PII

These FAQs provide guidelines on how to protect Sensitive PII.

1. How can I protect Sensitive PII...

A. In the office?

- 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.
- Never leave Sensitive PII unattended on a desk, network printer, fax machine, or copier.
- 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.
- Lock your computer when you leave your desk.
- Do not permit your computer to remember passwords. Never share your password with anyone.
- Avoid discussing Sensitive PII in person or over the telephone when you're within earshot of anyone who does not need to know the information.
- If you must discuss Sensitive PII using a speakerphone, phone bridge or video teleconference, do so only if you are in a location where those without a need to know cannot overhear.
- 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.
- Remember that some places that seem private still pose a risk for unauthorized disclosure, such as in a taxicab or airport shuttle.
- Don't transfer files to your home computer, personal media like thumbdrives, or print university records on your home printer.
- Don't upload files to your personal cloud storage accounts (e.g. Dropbox, Google Drive, etc.)
- Don't forward emails containing Sensitive PII to your personal email account (e.g., your Yahoo, Gmail, or AOL e-mail account) so that you can work on it on your home computer.

B. In email or other electronic transfer?

If there is any doubt that the recipient needs the Sensitive PII, UGA strongly recommends that you redact the Sensitive PII before you scan, email, copy and/or print the document containing Sensitive PII. Use SendFiles to transmit Sensitive PII if the recipient's need for the information is related to his or her official duties. If related to a new hire for staff, the information may be scanned into your computer and sent via iPaws. Be sure to delete the scanned file ***immediately*** from your computer's hard drive after you have transmitted the information.

C. When sending via facsimile (fax)?

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 the machine receives it. After sending the fax, verify that the recipient received the fax.

D. In the campus mail?

Sensitive PII should be not be sent via campus mail.

E. On my office shared drive, intranet, or public websites?

Do not post Sensitive PII on shared drives or ANYWHERE that can be accessed by individuals who do not have a "need to know."

2. How can I minimize my use of Sensitive PII?

Whenever possible, minimize the duplication and dissemination of electronic files and papers containing Sensitive PII.

- Only print, extract, or copy Sensitive PII when the risk is justified by an official need that is not easily met using other means.
- Before scanning, emailing, printing and/or making paper copies, redact Sensitive PII that is not necessary for your immediate use or for a recipient to see.

3. How do I secure Sensitive PII that cannot be encrypted, such as paper copies or some external media?

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. It is important to immediately delete copies of documents containing Sensitive PII from your computer's hard drive after successful transmission (via, e.g., SendFiles or iPaws).

4. What are my responsibilities when requesting or receiving Sensitive PII?

When collecting Sensitive PII via paper or electronic form, collect Sensitive PII directly from the individual to the extent possible.

- Every request you make for Sensitive PII should be accompanied by a reminder of how to properly secure the information. UGA employees can and should use SendFiles to request information from individuals with a UGA email address AND a non-UGA email address. UGA suggests the following reminder when requesting information from someone outside of UGA via SendFiles:

  "The information I have requested is Sensitive Personally Identifiable Information. To properly secure this information, please access your temporary account which has been created for you in SendFiles to access and respond to my request."

    - In some cases, outside entities will have their own secure file transfer system, similar to our SendFiles. In those cases, it is acceptable to log into their system to retrieve the requested data.
- 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.
    - For example, if someone outside of UGA sends unsecured Sensitive PII in the body of an email to you, you must use SendFiles if you wish to email it to another non-UGA recipient.
    - UGA Information Security Department strongly recommends that you password-protect Sensitive PII you share within your Department, and/or redact the Sensitive PII before you share or print it.
    - Securely dispose of or delete the unprotected Sensitive PII data that was sent to you. Contact your supervisor or IT professional for instructions.