HRS-EPM SECURE DATA HANDLING OVERVIEW

Restricted data is often stored in electronic format, which can make it more vulnerable to exposure. Because of this the need to protect personally identifiable information has never been greater. Each individual who creates, uses, processes, stores, transfers, administers, and/or destroys restricted University information is responsible and accountable for ensuring data is handled in a secure manner.

What is Secure Data Handling?

- Data handling related to when you view, update, delete, transfer, mail, store, or destroy data. It also relates to how you transfer the data from one location to another. Data is not always stored electronically. Occasionally it could be paper stored in a filing cabinet or in a binder.

- Complying with secure best practices when identifying, transmitting, redistributing, storing or disposing of restricted data.

What is "Restricted" Data?

Restricted information are data elements associated with a specific individual that are identified and protected by federal, state, local laws, regulations or adopted standards. Restricted information includes the following kinds of information that can be linked to an individual:

- Social Security Numbers
- Driver's License Number or State Identification Number
- Financial Account Number (including credit/debit card)
- Deoxyribonucleic Acid Profile (DNA)
- Unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation
- Protected health information (any information about the health status, provision of health care, or payment for health care)

How should I handle restricted data?

EVERYONE MUST TAKE CARE TO **SEE** THEIR DATA!

STOP
EVALUATE
ELIMINATE or MITIGATE

STOP- Before updating, deleting, transferring, mailing, storing or destroying data stop to identify if the data has restricted information.

EVALUATE- Review the data you are working with to identify if any of the six restricted data elements exist. **Being aware that you are handling restricted data is the key to handling it properly.**

ELIMINATE- There are occasions that some data you handle has restricted data included that is not necessary to complete your job. In order to avoid having to take additional steps to secure the restricted data it is often easier to eliminate it. When you are done working with the restricted data delete it. When you only have to use a portion of the data, remove it from the equation.

MITIGATE- The need for restricted data to exist is a requirement for most institutions to function. If you are unable to eliminate restricted data from your work you need to take additional steps to exercise secure data handling best practices when identifying, transmitting, redistributing, storing or disposing of restricted data.

SECURE DATA HANDLING
BEST PRACTICES FIELD GUIDE

Take care to **SEE** YOUR DATA: Being aware that you are handling restricted data is the key to handling it properly.

So you need to handle restricted data? Use the following guide to ensure that for every case you are taking the proper actions to securely handle restricted data.

GUIDE KEY:

✓ **Recommended Secure Practice**	⚠ **Additional Precautions Required**	⊘ **Prohibited Practice**

Email

Sending	⊘	Sending restricted data via email is prohibited as email by nature is unsecure and is subject to interception and being read or copied in transit to the destination.
	✓	Not preferred, hand delivery is recommended. However, if restricted information must be transmitted you are required to encrypt the email to ensure if the email is intercepted it cannot be read. This is commonly performed using digital certificates that can be issued at all UW campuses through your Information Technology departments.
Receiving	⊘	Email should never be received containing restricted data unless it was properly encrypted by the sender.
	✓	Emails that are received containing restricted data that is encrypted should be reviewed and then deleted when no longer needed (see storage). Report any emails received via email with unencrypted restricted data to HRS Security.
Storing & Destroying	⊘	The storage of unencrypted data is prohibited both online and through a backup as email storage is unsecure and can be subject to intrusion or being copied by unauthorized users.
	✓	Emails with restricted data should only be kept if encrypted. When the data is no longer needed it should be deleted from your e-mail “Sent Items” and “Deleted Items” as well as your "Inbox" to ensure complete removal of both encrypted and unencrypted data.

Instant Messenger

Sending & Receiving	⊘	Sending or receiving restricted data via instant messages (IM) is prohibited as IM by nature is unsecure and is subject to interception and being read or copied in transit to the destination.

Fax Machine

Sending & Receiving	✓	The fax machine must have limited access and be located in a non-publicly accessible area (ie. monitored office environment). Sender must ensure the receiver is present when a fax containing restricted data is being transmitted. Report any unattended fax data containing restricted data to HRS Security.
Storing	⚠	Transmitting data via fax causes the document to be saved and logged on both the sending and receiving fax machines. The logged document can be reproduced at either end by an unauthorized user. When sending or receiving faxes containing restricted data delete the document from the fax log/history.

Postal Mail / Shipping

Inter-Campus	✓	The preferred method of delivery of restricted data is by hand. However, when it is necessary to put restricted data into campus mail, the following should be performed: 1. Put the information into a non-windowed envelope. 2. Tape the envelope closed and write "confidential" on the tape that seals the envelope. 3. Put the envelope into a campus inter-office envelope with no special indications on it to avoid drawing attention to it.
External	✓	Return receipt should be used when mailing off campus. This will ensure that the restricted data was not lost in transit and received by the intended recipient.
Removable Media	⚠	Not preferred. However, in cases where restricted data must be sent on CD, DVD, Blue-Ray, or diskette, encryption of the data is required. The media must be stored in a secured area such as locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records when not in use or properly destroyed.
Jump (Flash) Drives	⚠	Not preferred. However, in cases where restricted data must be sent by jump (flash) drive the drive must be password protected and the data encrypted. The jump (flash) drive must be stored in a secured area such as locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records when not in use.

Telephone

Verbal	✓	Do not discuss or display restricted data in an environment where it may be viewed or overheard by unauthorized individuals.

Printing / Photocopying

Printing	✓	When printing documents that contain restricted data ensure that only authorized personnel will be able to see the output. The printer must have limited access and be located in a non-publicly accessible area (ie. monitored office environment). Never leave printed documents with restricted data unattended at the printer; these documents should be retrieved as soon as they are printed. Report any unattended printed documents containing restricted data to HRS Security.
Duplication	⚠	Any document containing restricted data must not be duplicated and further distributed without permission of the Campus Data Custodian. When using a photocopy machine to duplicate documents containing restricted data users should clear that document from the document history log. This is necessary as some machines save a copy of the document in the history logs that could be reproduced by an unauthorized user.
Storing	✓	Paper documents containing restricted data must be stored in a secured location such as locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records when not in use.
Destroying	✓	Crosscut shred or pulp all restricted data in paper form including all transitory work products (e.g., unused copies, drafts, notes) to ensure physical destruction beyond ability to recover.

Storage & Destruction

Paper	✓	Paper documents containing restricted data must be stored in a secured location such as locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records when not in use. Crosscut shred or pulp all highly sensitive information in paper form including all transitory work products (e.g., unused copies, drafts, notes) to ensure physical destruction beyond ability to recover.
Removable Media	✓	Restricted data stored on CD, DVD, BRD, or disk, must be encrypted. The media must be stored in a secured location when not in use or properly destroyed. Removable media must be destroyed by complete physical destruction of the media beyond ability to recover.
Jump (Flash) Drives	✓	Restricted data stored on a jump (flash) drive the must be password protected and the data encrypted. The jump (flash) drive must be stored in a secured area when not in use or data properly destroyed. If the jump (flash) drive is going to be repurposed or destroyed, then the electronic storage device must be wiped with a multiple pass/DOD secure overwrite prior to being repurposed.
Electronic Documents (Word, TXT, Excel)	✓	Workstations where users handle electronic documents that contain restricted data must comply with the following requirements: 1. Enable password protection using a strong complex password. 2. Enabled full disk encryption to protect from data theft. Electronic documents should be properly deleted and trash-bin emptied from the workstation when no longer needed. Workstation being repurposed must be wiped with a multiple pass/DOD secure overwrite prior to being repurposed.