This SPICE EduGuide applies to HSC users of **Restricted** information on removable media. **Restricted** information includes protected health information (PHI), personal identification information, personally identifiable student records, and other information whose access is **Restricted** by laws. Examples of removable media are CDs, DVDs, magnetic tapes, floppy disks, external hard drives, and universal serial bus (USB) drives also known as memory sticks, jump drives and thumb disks.

Removable media is commonly used by users to transfer electronic files from one computer to another, and as a mechanism to back up important information from their workstations. The security controls in place on HSC computer systems do not follow information as users place it on removable media. Users who place **Restricted** information on removable media, must maintain a heightened awareness of the security risks, recognizing that the responsibility for protection rests entirely in their hands.

Lost – Removable media is small and easily misplaced. People leave them behind on computers in labs, libraries and other public places. USB drives known as memory sticks or thumb disks, are especially easy to lose track of after slipping in a pocket, backpack, or briefcase.

Forgotten – Similarly, it is easy to forget what data is stored on removable media. This is especially common when removable media is used to back up information. Back up disks and tapes aren't often needed on a day to day basis. Although they might initially be stored in a secure place, they are commonly forgotten about and end up being left unprotected.

Disclosure of Restricted Information – Because removable media is easily lost and often forgotten, they present a high risk of an inappropriate disclosure if **Restricted** information is stored on them.

Use safeguards for removable media to keep **Restricted** information protected:

- Storage of **Restricted** information on removable media by users should be avoided whenever possible. Our important and highly confidential information should be stored and shared on secured servers which are backed up routinely and securely. Information needed to be carried on removable media by users, should be stripped of any personal identification information.
- Users who believe they have a valid reason to store **Restricted** information on removable media, must contact their Unit Information Security Manager (ISM) to discuss alternatives, and to ensure they know how to implement the required security measures:
  - **Restricted** information stored on removable media, must also be stored on a secure server so notification obligations can be carried out expediently in the event of an inappropriate disclosure.
  - Media must be labeled as **Restricted**, and with user's contact information; label the outside of the media, and in electronic form on the media
  - The **Restricted** information must be protected by encryption and a strong password.
- When removable media is no longer needed, proper disposal techniques must be employed. The user is responsible, but should contact their Unit ISM for the most up to date techniques to employ.
- Removable media should never be left unattended, without physically locking it up.
- If removable media is misplaced, the user must contact their Unit ISM immediately, so necessary steps can be taken to limit damage and liability of an inappropriate disclosure.

Policy & Standards References:

PS0003 Device and Media Controls
PS0006 Physical Security and Usage of End-User Computing Devices and Related Facilities
TS0010 Portable Computing Device Security
IR0001 Security Incident Response Team Charter