The **Family Education Rights and Privacy Act** (FERPA) requires Penn to protect student records from unauthorized disclosure, while also limiting access to staff with a legitimate “need to know”.

**Personally Identifiable Information** (PII) is any combination of data that can identify an individual person. PII ranges in sensitivity, from Social Security Numbers, credit card information, birthdates, phone numbers, PennKey name, and HR records.

### 5 Easy Steps to Help Protect Sensitive Data

1. Access Penn systems using your assigned work computer or through a secure remote connection. Lock your computer when not in use.

2. Secure sensitive data in locked cabinets, network drives, approved secured cloud services like Penn+Box.

3. Use Penn’s online “Secure Share” portal instead of email to send and receive documents containing PII.

4. Work with a “clean desk” policy: clear your desk and computer display of PII and student data when not in use.

5. Immediately retrieve any printouts containing sensitive information.

---

**Additional Resources**
- University Policy on Confidentiality of Student Records
- FERPA Frequently Asked Questions
- Data Risk Classification Matrix
- Information Security’s Tips on Foreign Travel
- How to Remotely Connect to the Finance Network
- DoF ITS Top 10 Information Security Tips
- FERPA Online Training in Knowledgelink

---

**Lost Computers and Mobile Devices**
Report all lost or stolen Penn computing devices to the ITS team immediately by calling 215-898-4578

**Reporting Theft, Loss or Breach of Data**
- Contact ITS immediately at 215-898-4578
- Contact Information Security at (215) 898-2172

**Don’t:**
- Access university systems using a public computer like those in libraries or kiosks; your account name and password may not be secure
- Leave computing devices unsecured in a hotel room; always use a safe
- Store Penn data on a personal, non-Penn computer
- Use portable storage devices, like USB “thumb” drives or portable hard drives