ADMINISTRATORS SERIES
PRIVACY AND SECURITY AT UF

Susan Blair  |  Chief Privacy Officer
Cheryl Granto  |  Information Security Manager, UFIT Information Security
RULES OF THE ROAD
Privacy: Not Alphabet Soup ...
Family Educational Rights and Privacy Act (FERPA): Student Records
- Authorizes Secretary of Education to end all federal funding if a university fails to comply with federal statute

Health Insurance Portability & Accountability Act (HIPAA): Protected Health Information
- Civil penalties and DOJ criminal prosecutions, which may result in penalties and up to ten years of jail time

Payment Credit Industry Data Security Standard (PCIDSS): Credit Card Information
- Noncompliant entities may be fined $500,000 per incident if cardholder information is compromised, and processing privileges may be revoked
UF Data Classifications

**Restricted**
- Data subject to specific protections under law, regulations or contracts.
  - Examples include, but are not limited to, medical records, social security numbers, credit card numbers, Florida drivers licenses, non-directory student records, research protocols and export controlled technical data.

**Sensitive**
- Data whose disclosure would impair the function of the university, cause significant financial or reputational loss or likely legal liability.
  - Examples include, but are not limited to, research work in progress, animal research protocols, financial information, strategy documents and information used to secure the University’s physical or information environment.

**Open**
- Data made generally available without specific approval.
  - Examples include, but are not limited to, advertisements, job opening announcements, university catalogs, regulations and policies, faculty publication titles and press releases.
Restricted Data

Restricted Data:
- Information, which if disclosed to unauthorized users, may have very significant adverse operational or strategic impact on an individual, a group or institution. This classification includes, but is not limited to, data restricted by law and legal contracts.

Examples:
- Personally Identifiable Information – SSNs, FDLs, financial data
- Medical Records
- Student Records
Hazard Number One

Failing to complete specific Privacy and Security general awareness trainings.

- “Privacy and Student Records in the Sunshine State”
- HIPAA General Awareness or HIPAA for Researchers
- Mobile Devices & Healthcare
- Security: Restricted Data Training
- Security: Cyber Self-Defense
Hazard Number Two

Being a Faculty member does not entitle you to any and all student information.

Share student records with individuals who have official need-to-know

- Grades, UFIDs, Student photos
- Letters of Recommendations
Hazard Number Three

Beware of including restricted data in unsecure emails systems. Do not use personal email accounts (hotmail, gmail, yahoo, etc.) to receive or transmit restricted data.

Adhere to UF’s Social Media Guidelines; do not disclose restricted information or talk about work related issues in blogs or on Facebook pages.
Hazard Number Four

Any portable device (i.e., laptop, ipad, pda, cell phone, flash drive) that is used for collecting, storing, or communicating restricted data must be encrypted - no exceptions.

Use of Social Security Numbers requires Privacy Office written permission.
Hazard Number Five

Identity Theft

Red Flag Rules for credit cards and financial data
Payment Credit Industry Data Security Standards

Phishing scams

• ALWAYS be suspicious
• UF will NEVER ask you for your password
• Never share your password with ANYONE
• Verify the information in the email by calling the UF Computing Help Desk, 392-HELP
• For more tips, visit http://security.it.ufl.edu/
Potholes and Patches

No antivirus software or software isn’t current

Computer updates are not current

- Secunia Personal Software Inspector (PSI)
  - http://secunia.com/psi
Potholes and Patches

Portable devices and media

Encryption

https://security.ufl.edu/learn-information-security/mobile-device-security/

Loss and theft protection

- FrontDoorSoftware

http://www.frontdoorsoftware.com/ufl/
Mobile Computing and Storage Devices Standard

To view the Mobile Computing and Storage Devices Policy, click here.

Purpose
To establish standards for the use of mobile computing and storage devices, and to specify minimum configuration requirements for mobile computing and storage devices used at the University of Florida consistent with the Mobile Computing and SI

Scope

There is a policy available.
To report violations, please contact abuse@ufl.edu.

For questions concerning this policy, please contact the Office of Information Technology at (352) 951-5555.
Mobile Computing and Storage Device Policy

**Restricted Data** stored on mobile computing and storage devices must be encrypted.

Any and all mobile computing devices used within the University of Florida information and computing environments must meet all applicable UF encryption standards. Mobile computing devices purchased with University of Florida funds, including, but not limited to contracts, grants, and gifts, must also be recorded in the unit’s information assets inventory.

University of Florida information security policies applicable to desktop or workstation computers apply to mobile computing devices.

Mobile Computing and Storage Device Standard

- All laptops and portable personal computers storing restricted data must utilize whole disk encryption. In addition, any laptops and portable personal computers purchased after August 17, 2011 must utilize whole disk encryption. All other laptops and portable personal computers shall have whole disk encryption installed by August 17, 2013;

- All smartphones and PDAs that access University of Florida data must be configured to encrypt any restricted data in persistent storage. In addition, any smartphones and PDAs purchased after August 17, 2011 must utilize encryption. All other smartphones and PDAs shall have encryption installed by August 17, 2013.

- All smartphones and PDAs must include the ability to remotely wipe stored data in the event the device is lost or stolen.

- All portable storage devices must include built-in encryption. The following exceptions apply:
  
  The encryption and key management methods used must have the approval of the UF Information Security Officer or designee.

- **Restricted Data** must be protected by encryption during transmission over any wireless network and any non-University of Florida wired network.
Mobile Device Risks

If you’re using your Mobile Device for patient care, do you know what to do if:

- Your device is Lost or Stolen?
- Your device is infected by a virus or other malware?

Are you aware that you should never:

- Share your personal mobile device with anyone?
- Use your device on an unsecured network?
Before you begin using your own or a UF-owned mobile device for health care-related duties at UF Health, you must:

- Have required and approved applications, security programs, updates, and patches installed.
- Review the IT Security policies and know how they apply to you.

Help stop mobile device problems before they happen.
Required Device SAFEGUARDS

Use Proper Authentication

• Use strong password that meets or exceeds UF Health’s password requirements.
• Set an inactivity timeout of no more than 10 minutes – require a password to re-enter.
• Never share your password and change it often.

Use and Maintain Approved Software

• Install only approved software.
• Enable approved encryption software.
• Enable and maintain anti-virus and -malware protection.
• Disable file-sharing applications.
Required Device SAFEGUARDS

Maintain Physical Control

- Keep your device with you or locked up.
- Enable approved tracking or recovery software.
- Do not allow others to use your device (children, spouse, friends, etc.).
- Do not leave your device in a parked vehicle.

Use Secure Networks

- Use adequate security over Wi-Fi networks.
- Do not forward e-mail to outside accounts.

Ensure Proper Disposal
REPORT Lost or Stolen Devices

Report the loss or theft of your device immediately!

• Notify your immediate supervisor.

• Also Notify:
  • IT Security Office
  • Privacy Office
  • UF Police Department
Service Plaza
No Drop Box - No Google Docs

- **Dropbox**: File Storage and Sharing in the Cloud; UF does not have a formal agreement with Dropbox and you are not authorized to agree to their terms and conditions for official university business.

- **Googledocs**: File Storage and Sharing; Unacceptable consolidated privacy policy; similar concerns for any Google product.
eTools – What Can you Do?

### eTools Assessment

<table>
<thead>
<tr>
<th>eTool/Cloud Service</th>
<th>Guidelines Available</th>
<th>Security Review Complete</th>
<th>Privacy Review Complete</th>
<th>Approved for Restricted Data</th>
<th>Common Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ares</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Azure</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Big BlueButton*</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blogger</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td>Students present information using a variety of media</td>
</tr>
<tr>
<td>Bridgesoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calibrated Peer Review</td>
<td></td>
<td></td>
<td></td>
<td>No</td>
<td>Peer review of student work</td>
</tr>
<tr>
<td>Camtasia</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Record presentations</td>
</tr>
<tr>
<td>Canvas*</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Students collaborate in real time

---

**Guidelines**

- eTools
- eTools Assessment
  - eTools Restrictions and Caveats

**Technology Fee**

- About
- Charter
- Florida Statutes Section 1009.24
- Scoring Criteria
- Submitting a Concept Paper
Welcome to the University of Florida Qualtrics account.

To login you will need your GatorLink username and password. Once you are logged in, you will be able to create, deliver, collect, and analyze online surveys in support of your teaching, research, and studies.

Please note that Restricted Data is not permitted in the questions or answers of Qualtrics. For questions about what constitutes Restricted Data see [http://www.it.ufl.edu/policies/infosecdefinitions.html](http://www.it.ufl.edu/policies/infosecdefinitions.html) or contact the IT Security Office or the Privacy Office.

For assistance, contact e-Learning Support Services: 352.392.4357, option 3 | learning-support@ufl.edu | Hub 132
Traffic Violations
Privacy Sanctions

Sanctions for HIPAA violations are serious:
• FBI involvement
• Hefty fines – starting at $25K per patient affected, up to $1.5M
• Jail-time

Residents are often the **slowest to respond** to required HIPAA mitigation, often missing the 30 day “cure” requirement.
• Places the University in jeopardy
• An OCR audit is not limited to the original subject
Residents and Students tend to be HIPAA violators in these areas:

**Unauthorized disclosures** – the most common violation:
- Be aware of your surroundings when discussing patients – do not chat in elevators.
- Be especially careful with patients diagnosed with HIV.

**Not de-identifying PHI**

**Improper use of portable devices**: laptops, PDAs, camera phones, etc.
- Recording (and sharing) unauthorized pix and videos
- Failure to use encryption
- Losing or misplacing equipment
- Downloading unnecessary PHI

**Removal of PHI** or health records from UF premises.
- There are ways to do this properly – don’t cut corners.
New Penalties

So, a breach involving PHI for 10 individuals could cost **you** anywhere from $100 to $50,000 per disclosure.

<table>
<thead>
<tr>
<th>Tiers</th>
<th>Description</th>
<th>Minimum per Violation</th>
<th>Max per Year (for identical violations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier A</td>
<td>Did not know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier B</td>
<td>Reasonable cause – not willful neglect</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier C</td>
<td>Willful neglect – corrected w/in 30 days</td>
<td>$10,000 - 50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier D</td>
<td>Willful neglect – uncorrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Other Consequences

UF Sanctions include:

• Mandatory remedial training
• Counseling and Letters of Reprimand
• Loss of access to computer systems
• Loss of student privileges
• Suspension or expulsion
• Reporting to professional licensing or credentialing boards
Staying Between the Lines
Travel Advisors
Who Are Key People?

Unit Information Security Administrator (ISA)

Unit Information Security Manager (ISM)
Information Security Roles

**ISA: Information Security Administrator, UF_SEC_ISA**
SEE DSA

- Ensures compliance to policies and standards by faculty and staff within your Unit
- Disseminates information and educational materials to Unit users
- Knows the information security rules and can provide guidance to Unit users

**ISM: Information Security Manager, UF_SEC_ISM**
SEE DSA

- Typically the manager or director of your IT department
- Ensures information systems in your Unit are compliant with security policies and standards
- Provides technical security solutions on Unit systems
- Makes use of enterprise security solution

**Technical Contact, UF_SEC_TECHCONTACT**
SEE DSA

- Anyone that manages security controls on an information system

UF Information Technology
www.it.ufl.edu
Crash Test

Risk Assessments

New products, services, upgrades, major enhancement or migrations must be assessed
Traffic Alert
Electronic Media Secure Disposal Service

UF requires the destruction of data on electronic equipment being disposed, transferred or reused. This includes all forms of electronic media, such as hard drives, solid-state and flash drives, tapes, and devices with built-in storage.

Media Disposal Dropoff Locations

UF Computing Helpdesk
HUB 132
Hours of Operation

HSC Communicore
Room C2-22A
Tuesdays 10am – 12pm
or by appointment
When in Doubt ...

Privacy:
Susan Blair
273-1212
sablair@ufl.edu

Information Security Office
Cheryl Lyn Granto
Security@ufl.edu