# Data Definitions

***Highly Restricted Data:*** *Some examples include:*

*a) an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: social security number, driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity, or financial account numbers;*

*b) user name (e.g., NID) or email address, in combination with a password or security question and answer that would permit access to an online account;*

*c) data concerning an individual that is considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 11 Statute 1338) (as amended) and its implementing regulations, and;*

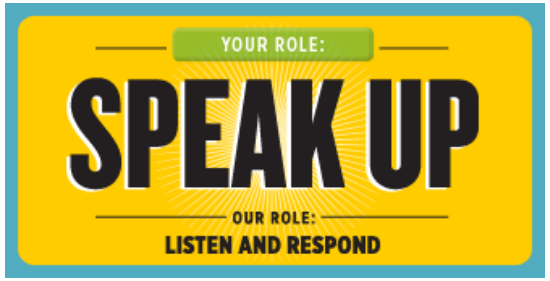
*d) data concerning an individual that is considered "protected health information" within the meaning of the Health Insurance Portability and Accountability Act of 1996 (as amended) and its implementing regulations, and the HITECH Act. Protection of such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.*

*Other examples of highly restricted data include the home addresses, telephone numbers, social security numbers, and photographs of certain university employees, such as police officers and their spouses, as specified in F.S. 119.07(4)(d)1-7.*

***Restricted Data:*** *This includes electronic information the unauthorized access, modification, or loss of which could adversely affect the university (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the university), or adversely affect the public.*

*Examples of restricted data include business-sensitive data, proprietary intellectual property data, and student academic records as defined by the Family Educational Rights and Privacy Act (FERPA) of 1974, and other data protected by law or regulation.*

Doing the right thing means acting with honesty and integrity and speaking up when you know of or suspect unethical behavior. To report a suspected information security incident contact sirt@ucf.edu. To report anonymously, contact the UCF IntegrityLine.




Our INTEGRITYLINE allows you to report ethical concerns without the fear of retaliation — 24/7. Secure. Anonymous.

**If you have questions or need assistance appropriately securing, transferring, processing, or storing university restricted data, including protected health information, personal or other confidential information, please contact Privacy Compliance (see below).**

H
I
GDPR
A
FERPA

**UNIVERSITY OF CENTRAL FLORIDA**
PRIVACY COMPLIANCE
UNIVERSITY COMPLIANCE, ETHICS, AND RISK
4365 ANDROMEDA LOOP N., MH 328
ORLANDO, FLORIDA 32816-0001

## FOR MORE INFORMATION

407.823.0129
PRIVACY@UCF.EDU
UCF.EDU/INTERNET-PRIVACY-POLICY

# Privacy Compliance@UCF

UNIVERSITY COMPLIANCE, ETHICS, AND RISK
UNIVERSITY OF CENTRAL FLORIDA. ORLANDO,FL

UCF

# What is Privacy Compliance?

Privacy Compliance exists within University Compliance, Ethics, and Risk, providing centralized and coordinated oversight of UCF's adherence to state and federal laws, as well as regulations imposed by other countries, that involve the protection and privacy of personal information.

# What You Can Do

We are all data stewards as we come in contact with personal and private data every day. We are expected to treat personal information belonging to others in a manner that avoids unnecessary sharing, transferring, processing (using), and storing. Along those lines, if we must collect personal information, we should only capture the minimum necessary to fulfill a request or perform a job function. If we learn that the personal information of one or more individuals has been compromised, we must immediately report it by e-mailing SIRT@ucf.edu.

Protect private and personal (restricted) data by locking it up when no longer in use. Avoid leaving restricted data where others can see, copy, or steal it. If the restricted data is digital, be sure to store it where unauthorized users cannot access it and use secure transfer mechanism, such as encryption, when sending restricted data to others.

ucf.edu/internet-privacy-policy

## Privacy Laws, Regulations, & Standards that impact UCF

**DFAR and FAR - Defense Federal Acquisition and Federal Acquisition Regulations**

**FERPA - Family Educational Rights & Privacy Act**

**GDPR - General Data Protection Regulation**

**HIPAA - Healthcare Insurance Portability & Accountability Act**

**NIST - National Institute of Standards and Technologies**

**PCI DSS - Payment Card Industry Data Security Standard**

...and more to come!

## Did you know?

**FERPA grants students the following rights:**

- ⇒ **The right to inspect and review educational records within 45 days (State of Florida law = 30 days)**
- ⇒ **The right to seek to amend educational records**
- ⇒ **The right to have some control over the disclosure of information from – educational records**
- ⇒ **The right to obtain a copy of the institution's student records policy**
- ⇒ **The right to file a complaint with the Department of Education**

**For questions or more information, simply contact the UCF Registrar's Office.**

**If you have questions or need assistance regarding a data privacy issue, contact privacy@ucf.edu or call 407-823-0129.**

# How To Handle Requests Involving Personal Data

Students and others' requests for:

A copy of their personal information
To delete their personal information

Direct them to email privacy@ucf.edu
If they hand you a request in writing, send a fax or email, scan and/or forward it to privacy@ucf.edu immediately

Advise the individual that Privacy Compliance will initiate a **Data Subject Access Request (DSAR)** and communicate from that point forward.

"If a service is free, you — and your data — are the product."

**- Andrew Lewis**

UCF | University Compliance, Ethics and Risk Office
UNIVERSITY OF CENTRAL FLORIDA

For more information, email privacy@ucf.edu or call (407) 823-0129