UNIVERSITY OF FLORIDA

Cyber Safeguards for Restricted Data

Kathy Bergsma

UF Information Security Manager

5/19/2008

This introductory data security course will explain the dos and don'ts of using Restricted Data on computers. You will learn when to use encryption, proper methods for disposal, and what to do in the event of a Restricted Data exposure. Important contacts regarding Restricted Data will be presented and technical resources for data protection will be discussed.

Terminology

- Restricted data: UF's term for private and other highly confidential data
- Private data: Data unique to an individual not readily known
- Confidential data: General data term
- Sensitive data: lesser degree of confidentiality, but also availability and integrity

Major Players

- UF Privacy Office
- UF Office of IT Security Management
- UF Health Science Center
- You

Restricted Data Safeguards

Avoid the following risks:

- ✓ Storing Restricted Data on workstations, portable devices or removable media.
- ✓ Sending Restricted Data in email or instant messages.
- ✓ Using Restricted Data on unapproved non-ufl.edu web sites.
- ✓ Removing Restricted Data from UF premises without authorization.

If the need outweighs the risk or if in doubt:

- ✓ Get permission from DDD.
- ✓ It should be used only on approved systems.
- ✓ It should require authentication to access.
- ✓ Minimize the amount of data and the length of time it's used.
- ✓ It should not be the official copy.
- ✓ It should not be the only copy.
- ✓ It should have appropriate loss and theft protection. See local IT worker.
    - Exposed Restricted Data must be reported to Privacy Officer.
    - Exposed sensitive data must be reported to DDD.
- ✓ It should be encrypted for storage and transmission. See local IT worker.
- ✓ It should be rendered unreadable prior to disposal.

PCI: Payment Card Information

Credit card account number alone or with any of the following:

- Cardholder name
- Service code
- Expiration date

PCI Safeguards

- ✓ DDD authorization must be documented.
- ✓ Use PCI data only on authorized computers maintained by UF professional IT workers.
- ✓ Never use PCI data outside the confines of the authorized credit card processing system.
- ✓ On the web, look for the lock or https in the url.
- ✓ Never store PCI data on a desktop, laptop, CD, DVD, thumb drive.
- ✓ Never use PCI data in email or instant messages.
- ✓ Never download PCI data.
- ✓ Never cut & paste PCI data.

More PCI Information

UF Privacy Office Financial Information
http://privacy.ufl.edu/financial.html
UF e-Commerce Policy
http://www.it.ufl.edu/policies/documents/E-commerce%20policy.pdf
PCI safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-pci.pdf

PII: Personally Identifiable Information

Name together with one or more of the following:

- Social security number
- Driver license number
- Financial account number in combination with any security code, access code, or password.

PII Safeguards

- ✓ DDD authorization must be documented.
- ✓ Use PII data only on authorized computers maintained by UF IT workers.
- ✓ PII data should not be stored on a desktop, laptop, CD, DVD, thumb drive. Where necessary:
    - Obtain special permission
    - Use full disk encryption
    - Physically secure it.
- ✓ Avoid using PII data in email or instant messages, especially to addresses that don't end in ufl.edu.
- ✓ On the web, look for the lock or https in the url.

More PII Information

UF cyber-use limitations of PII data
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-pii.pdf

PER: Private Educational Record

- Name of the student's parent or other family member
- Address of student's family
- Personal identifier, such as the student's social security number
- A list of personal characteristics that would make the student's identity easily traceable
- Disciplinary status
- Financial – aid, tuition, payments, account balances
- Grades, exam scores, or GPA (grade point average)
- Class rosters
- Applications and admissions information
- Schedules
- Evaluations, forms, essays, memos, or correspondence to and about the student
- Birth date
- Gender
- Citizenship
- Marital status
- Religion

PER Safeguards

- ✓ DDD authorization must be documented.
- ✓ Use PER data only on authorized computers maintained by UF IT workers.
- ✓ PER data should not be stored on a desktop, laptop, CD, DVD, thumb drive. Where necessary, use full-disk encryption.
- ✓ Avoid using PER data in email or instant messages, especially to addresses that don't end in ufl.edu.
- ✓ On the web, look for https in the url or the lock.

Other PER Information

FERPA training from the UF Privacy Office
http://privacy.health.ufl.edu/training/FERPA/
FERPA information from the UF Registrar
http://www.registrar.ufl.edu/ferpahub.html
UF cyber-use limitations for FERPA data
http://www.it.ufl.edu/policies/security/drafts.html

PHI: Protected Health Information

Any information that links an individual with their physical or mental health condition such as:

- Name of individual or relative
- Any address smaller than state
- Dates such as birth, admission, or discharge
- Telephone numbers
- Electronic mail address
- Social security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary number
- Full face photographic images and any comparable images
- *Any other unique identifying number, characteristic, or code*

PHI Safeguards

- ✓ DDD authorization must be documented.
- ✓ Unique identifier required for authentication.
- ✓ Encryption required for transmission and storage on laptops, PDAs and removable media.
- ✓ PHI usage in email must be authorized by the UF Privacy Office, sent only to ufl.edu addresses, and should be extremely rare.
- ✓ Never transmit PHI by instant message.
- ✓ Workstations used with PHI must have a password protected screen saver with a short timeout.
- ✓ Do not remove from campus without DDD authorization.
- ✓ PHI must be disposed of securely.

More PHI Information

Health Science Center security training
https://www.security.health.ufl.edu\staff\training
Privacy Office HIPAA training
http://privacy.health.ufl.edu/training/
Electronic Media Secure Disposal
https://www.security.health.ufl.edu/disposal

Password Safeguards

- ✓ Password composition
  - Long, sometimes called passphrases
  - Complex
  - Easy to remember
- ✓ Password protection
  - Don’t share with ANYONE, EVER!
  - If you must write it down to remember it:
    - Don't write the word 'password' on the note
    - Don't write your logon id on the same note
    - Protect it like a credit card

Encryption

Storage

- Encrypted Restricted Data may be exempt from liability.
- See your local IT worker for assistance.
- Use method approved by Unit ISM.
  - File/Folder: NTFS, Truecrypt, PGP
  - Application: Winzip, Adobe Acrobat
  - Whole-disk: Bitlocker, Truecrypt, PGP-WDE

Transmission

- See your local IT worker.
- Some methods are transparent to user.
- Use method approved by Unit ISM.
  - Virtual Private Network (VPN)
  - SSL or https
  - SSH, SCP, SFTP

Workstation Safeguards

Can I store Restricted Data on my workstation?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires authorization
- PHI: Requires authorization

Avoid storing Restricted Data on your workstation

- ✓ DDD authorization must be documented.
- ✓ Use computers maintained by UF IT workers and approved by Unit ISM.
- ✓ Position screen so it's not viewable to others.
- ✓ Report exposed Restricted Data to UF Privacy Office.
- ✓ Minimize the amount of data stored.
- ✓ Minimize the length of time it's stored.
- ✓ Use encryption.
- ✓ Maintain secure backups.
- ✓ Render unreadable upon reuse or disposal.

Personally Managed Computer Safeguards

Can I store Restricted Data on my personally-managed computer?

- PCI: No
- PII: No
- PER: Requires authorization
- PHI: Requires authorization

Avoid storing Restricted Data on personally managed computers

- ✓ DDD authorization must be documented
- ✓ DDD authorization required to remove from campus
- ✓ Get device approval from the Unit ISM
- ✓ Minimize the amount of data stored
- ✓ Minimize the length of time it's stored
- ✓ Use strong passwords
- ✓ Maintain current software updates
- ✓ Maintain current anti-virus updates
- ✓ Use a firewall
- ✓ Use whole-disk encryption
- ✓ Maintain secure backups
- ✓ Report exposed data immediately to UF Privacy Office
- ✓ Render unreadable upon reuse or disposal

Portable Computing Devices Safeguards

(Laptops, PDAs, smart-phones)

Can I store Restricted Data on my laptop, PDA or smart-phone?

- PCI: No
- PII: No
- PER: Requires authorization
- PHI: Requires authorization

Avoid storing Restricted Data on portable devices

- ✓ DDD authorization must be documented.
- ✓ DDD authorization required to remove from campus.
- ✓ Use devices maintained by UF IT workers and approved by the Unit ISM.
- ✓ Use whole-disk encryption.
- ✓ Maintain secure backups.
- ✓ Minimize the amount of data stored.
- ✓ Minimize the length of time it's stored.
- ✓ Don't synchronize with home computer.
- ✓ Protect device as you would a wallet or purse.
- ✓ Report lost devices immediately to UF Privacy Office.
- ✓ Render unreadable upon reuse or disposal.

Removable Media Safeguards

(CDs, DVDs, USB drives, external hard drives, floppy disks, backup tapes)

Can I store Restricted Data on removable media?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires authorization
- PHI: Requires authorization

Avoid storing Restricted Data on removable media

- ✓ DDD authorization must be documented.
- ✓ DDD authorization required to remove from campus.
- ✓ Use media maintained by UF IT workers and approved by the Unit ISM.
- ✓ Use encryption.
- ✓ Maintain secure backups.
- ✓ Minimize the amount of data stored.
- ✓ Minimize the length of time it's stored.
- ✓ Protect media as you would a wallet or purse.
- ✓ Report lost media immediately to UF Privacy Office.
- ✓ Render unreadable upon reuse or disposal.

Home and Travel Safeguards

Can I store Restricted Data on my home or travel computer?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires authorization
- PHI: Requires authorization

Avoid using Restricted Data at home or when traveling:

- ✓ DDD authorization must be documented.
- ✓ DDD authorization required to remove from campus.
- ✓ Use whole-disk encryption.
- ✓ Make a backup before you travel.
- ✓ Use the UF VPN to connect with UF servers.
- ✓ Use strong passwords.
- ✓ Maintain current anti-virus and updates.
- ✓ Minimize amount of data and length of time.
- ✓ Protect portable devices and media like a wallet.
- ✓ Consider remote data destruction software.
- ✓ Consider device tracking software

Email Safeguards

Can I send Restricted Data in email?

- PCI: No
- PII: Requires special authorization and should be rare
- PER: Requires special authorization and should be rare
- PHI: Requires special authorization and should be rare

Avoid sending Restricted Data in email

- ✓ DDD authorization must be documented.
- ✓ Use email software and methods approved by the Unit ISM.
- ✓ In the email body, identify as Restricted Data and provide handling instructions.
- ✓ Minimize the amount of data sent.
- ✓ Minimize the number of recipients, no lists.
- ✓ Send only to email addresses ending in ufl.edu.
- ✓ Double-check the recipient list. Beware of auto-completion features.

Instant Messaging Safeguards

Can I send Restricted Data in instant messages?

- PCI: No
- PII: No
- PER: Requires special authorization and should be rare
- PHI: No

Avoid sending Restricted Data via any IM.

- ✓ DDD authorization must be documented.
- ✓ Do not use Restricted Data with commercial instant messaging services such AOL, Yahoo, or MSN.
- ✓ Do not use IM to send and receive attached files.
- ✓ Use software and methods approved by Unit ISM.
- ✓ In the message, identify as Restricted Data and provide handling instructions.
- ✓ Minimize the amount of data.
- ✓ Minimize the number of recipients.
- ✓ Send only to IM addresses ending in ufl.edu.
- ✓ Double-check the recipient list.

Web Safeguards

Can I use Restricted Data on the web?

- PCI: Requires authorization
- PII: Requires authorization
- PER: Requires authorization
- PHI: Requires authorization

Web safeguards:

- ✓ Beware of phishing scams. Never follow links in email or instant messages. Use bookmarks, link on your statement, Google or other search engines.
- ✓ Use browser, configuration and methods approved by Unit ISM.
- ✓ Use Restricted Data only with approved UF web sites.
- ✓ Look for the lock or https in the url.
- ✓ Do not use features to remember or auto-complete passwords.

Disposal Safeguards

- ✓ Consult your Unit ISM for approved reuse and disposal methods
- ✓ Render Restricted Data unreadable before media reuse or disposal. Protect it until this can be done.
- ✓ Maintain inventory of data that must be stored or transported prior to reuse or destruction
- ✓ Use only UF-approved reuse and disposal methods
    - UF has a disposal contract with Cintas

Contacts

Kathy Bergsma
UF Information Security Manager
392-2061
ufirt@ufl.edu
http://infosec.ufl.edu/

Susan Blair, Chief Privacy Officer
Office phone: 392-2094
Privacy Hotline: 866-876-4472
Email: privacy@ufl.edu
Web: http://privacy.ufl.edu/

Health Science Center
Colleen Ebel, HSC Unit ISM
Phone: 273-7478
Non-urgent email: HSC-Security-L@Lists.ufl.edu
Urgent email: HSCIRT@ufl.edu
Web: https://security.health.ufl.edu/

IFAS
Wayne Hyde, IFAS Unit ISM
Phone: 846-2565
Email: IFASIRT-L@lists.ifas.ufl.edu or abuse@ifas.ufl.edu

Other Units http://net-services.ufl.edu/cgi-bin/subnet-form.cgi

Useful Data Security Links

PCI Cyber Security Checklist
http://www.it.ufl.edu/policies/security/documents/PCIchecklist.pdf
PII Cyber Security Checklist
http://www.it.ufl.edu/policies/security/documents/PIIchecklist.pdf
PER Cyber Security Checklist
http://www.it.ufl.edu/policies/security/documents/PERchecklist.pdf
UF VPN:
http://net-services.ufl.edu/provided_services/vpn/
McAfee Anti-virus:
http://software.ufl.edu/mcafee/
UF Cintas disposal contract:
http://www.purchasing.ufl.edu/main_contracts-cintas.asp
UF IT Restricted Data Standards:
http://www.it.ufl.edu/policies/security/documents/data-std-rd.pdf
PCI safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-pci.pdf
PII safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-pii.pdf
PER safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-limitations-per.pdf
Workstation safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-workstation.pdf
Laptop and PDA safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-PDA-laptop.pdf
Removable media safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-removable-media.pdf
Email safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-EMAIL.pdf
Instant messaging safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-IM.pdf
Web safeguards:
http://www.it.ufl.edu/policies/security/documents/data_use_draft/use-web-service.pdf
Re-use and disposal safeguards:
http://www.it.ufl.edu/policies/security/documents/ITworker_draft/disposal.pdf