Data Security Classifications At A Glance

This document provides a quick reference to data security classifications. See the University Policy on IT for complete details. http://www.rochester.edu/it/policy/index.html

Basic Safe Data Handling

- **If you do not know the classification, err on a more secure classification**. Data collections or documents must be handled to the standard of the highest security classification of the content.
- **Never share** login passwords, particularly for NetID or Active Directory (AD) accounts.
- **Use University email accounts to conduct University business**. If contacted via email by a University employee or student from their non-University email account, reply to the sender's University email account.
- **Use encryption and enable** passcodes/pins to protect any devices (iPad, smart phone, laptop) used for University business. Set the inactivity timeout to the number of minutes appropriate for your department.
- **Maintain personally owned devices and computers in secure configuration** if used for University business. Secure configuration is defined as having current virus protection and current legal software versions. Install updates and security patches promptly.
- **Access only the information you need to do your work**. Utilize the minimum amount of personally identifiable information that is necessary to do your job, even when access to more data is available. Do not share information to which you have access.
- **How to send encrypted email.** When sending from University email, type !SECURE in the beginning of the subject line. This is currently available at URMC and will be available University-wide in 2013.

Protected Health Information (PHI) is health information (oral or recorded) that associates an individual with a health care provider, a health condition or diagnosis, a health care facility, or a health care plan. Because this information is so prevalent in the health care and research operations of the University, it is recommended that staff who work in these areas assume that most communication contains PHI. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA). PHI excludes health information in employment records, such as required immunizations.

Personally Identifiable Information (PII) is a group of personal data points. When two or more data points are combined, personal identity theft or forgery is possible. The University safeguards PII of any affiliated person (patient, staff, student, or volunteer) and defines PII as the following:

- SSN
- Bank account information
- Credit or debit card information
- Home address
- Home telephone number
- Personal email address
- Internet identification name or password
- Parent's surname prior to marriage
- Drivers license number or non-driver identification number

● Legally Restricted and Confidential data or information

LEGALLY RESTRICTED

What it is:

- Protected Health Information (PHI)
- Social Security Number (SSN)
- Personally identifiable Information (PII)
- State issued driver's license or non-driver ID
- Credit/debit card information
- Bank account numbers

Some common documents that *may* contain legally restricted information:

- Human subjects records
- All grant documents
- Employee tax forms
- Federal reporting requirements (Welfare benefits and wage garnishing)
- I-9 forms
- Appointment letters
- Records of payroll deductions
- Salary records& performance appraisals
- Financial aid records (SSN)
- Medical records
- Personnel records for staff and retirees

CONFIDENTIAL

What it is:

- Personnel records
- Department academic files
- Student information
- Records and communication of the Board of Trustees
- Large segments of the University budget
- Unpublished intellectual property such as patent applications, inventions, manuscripts
- Information the University has agreed to hold confidential under a contract

Some common documents that *may* contain confidential information:

- Program or administrative budgets
- Invention disclosures
- Licensing agreements
- Employment contracts
- Individual salary and benefits
- Financial aid records (excluding SSN)
- Student loan records
- Student applications, transcripts, grades
- Construction drawings for nonpublic or confidential areas

How to dispose of it:
Data must be rendered no longer readable or recoverable, whether electronic or paper. Overwrite electronic copies at all storage locations or destroy the storage locations. Shred paper (using a cross cut shredder at a minimum) or use a document destruction service. For more information on disposing of legally restricted information, contact your security liaison or your local IT Help Desk◆ *Med Center ISD Help Desk (585)275-3200◆University IT Help Desk(585)275-2000*

How to treat it safely:
Transmit with encryption. Store the information in a University approved data center or in encrypted form. Encrypt information that is moved off University systems. Use an approved authentication method to access the information. Follow Basic Safe Data Handling if you must use personally owned devices or work remotely with legally restricted or confidential information. Secure physical formats (paper, CD-ROMs) in locked storage.

Basic Safe Data Handling ◆Never share account logins. ◆ Use University email systems for University business ◆ Encrypt devices and set passcodes and inactivity time-outs ◆ Access only the information you need ◆ Maintain computing equipment with secure configurations.

Internal data or information

What it is:

- Most routine documents.
- Subsets of confidential data, such as budgets, may be classed Internal

Some common documents that may contain internal information:

- Grievance files (these are not considered personnel files)
- Sexual harassment complaints, investigations, and findings (these are not considered personnel files)
- Union agreements
- Security, accident, or incident reports
- Financial auditing work papers
- Financial statements - unaudited
- Purchase orders
- Department budgets
- Travel reimbursements
- Organizational charts with names
- Job descriptions
- Search committee records
- Tenure and promotion cases
- Affirmative action plans
- Environmental monitoring records
- Real estate materials
- Construction drawings for public or non-confidential spaces.
- Alumni data
- Gift records

How to dispose of it:
Use the normal Delete feature of any software program. Dispose of paper, plastic, microfiche and CD-ROMS through ordinary means, including recycling.

How to treat it safely:
Do not distribute via public website or distribute publically in print. Follow Basic Safe Data Handling if you use personally owned devices or work remotely. If in doubt as to whether information is internal or public, contact your security liaison or your local IT Help. ◆ *Med Center ISD Help Desk (585)275-3200* ◆ *University IT Help Desk (585)275-2000*

Basic Safe Data Handling ◆Never share account logins. ◆Use University email systems for University business ◆ Encrypt devices and set passcodes and inactivity time-outs◆ Access only the information you need ◆ Maintain computing equipment with secure configurations.

🟢 Public data or information

What it is:

- Any content accessible from the Internet that does not require authentication
- *Vital Signs, Currents, Rochester Review, Campus Times.*
- Audited financial statements
- Annual reports

Some common documents that contain public information:

- Faculty/staff/student directory
- Press releases
- Charter and By-Laws
- Organizational charts without names
- Athletic schedules
- Course schedules
- Commencement programs
- Content on UR YouTube channel

How to dispose of it:
Use the normal Delete feature of any software program. Dispose of paper, plastic, microfiche and CD-ROMS through ordinary means, including recycling.

How to treat it safely:
Safety guidelines for this classification are unnecessary.

Basic Safe Data Handling ◆Never share account logins. ◆Use University email systems for University business ◆ Encrypt devices and set passcodes and inactivity time-outs◆ Access only the information you need ◆ Maintain computing equipment with secure configurations.