

# Protecting Restricted Data At RBHS

## What is restricted data?

### TERMINOLOGY



**Restricted Data** is the most sensitive information that requires the highest level of protection.

This information is also described as 'non-public personal information' (NPPI) about people or critical business, academic or research operations under the purview of the Owner/Data Custodian.

Restricted Data includes, but is not limited to, data that the University is required to protect under regulatory or legal requirements. Unauthorized disclosure or access may 1) subject the University to legal risk; 2) adversely affect its reputation; 3) jeopardize its mission; 4) present liabilities to individuals (e.g. HIPAA penalties).



Information Security Office, a division of the  
Office of Information Technology and  
Information Protection and Security  
Rutgers Biomedical and Health Sciences  
Rutgers, The State University of New Jersey  
30 Bergen Street  
Newark, New Jersey 07107

Fax: 973-972-1213  
E-mail: [infosecurity@ca.rutgers.edu](mailto:infosecurity@ca.rutgers.edu)  
[rbhs.rutgers.edu/ca/infosecurity](http://rbhs.rutgers.edu/ca/infosecurity)

### OIT/INFORMATION SECURITY OFFICE



### BASICTENETS OF INFORMATION SECURITY



#### Know the following:

**Confidentiality:** Restricted data should be accessed only by authorized individuals.

**Availability:** Restricted data must be accessible to authorized individuals.

**Integrity:** Expectation that the University's data will be protected from intentional, unauthorized or accidental changes.

#### Do the following:

- ◇ **Review Applicable Security Policies (e.g. Information Classification Policy);**
- ◇ **Follow Established Procedures in Your School or Unit for Securing Restricted Data;**
- ◇ **Ensure that University-issued Mobile Devices are Encrypted;**
- ◇ **Lock your computing devices when unattended; and**
- ◇ **Never share your network account or password information with anyone!**

### ADMINISTRATIVE & PHYSICAL CONTROLS

