RADFORD UNIVERSITY

Clinical Simulation Center

Data Storage and Media Protection Policy

Original Date: April 2014 Review/Revision Date: April 2019

Approved: May 2019

I. Purpose: Radford University is committed to maintaining a reliable and secure technology infrastructure. Secure storage of media where sensitive data stored is critical to the security of University information. This policy provides guidelines for handling of sensitive data and protecting data from compromise.

II. Policy:

1. Data owners are responsible for classifying their data sensitivity and for notifying system owners of the sensitivity and data protection requirements of the data they own.
2. Data custodians are individuals or entities that are in physical or logical possession of data for owners. Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage.
3. **Highly sensitive data** is prohibited from being stored on any mobile device, including laptops and non-network drives, unless the data is **encrypted** and an exception identifying the business need, risks involved, mitigating security controls, and acceptance of any residual risk is approved by the Agency Head or designee.
4. Data storage media containing highly sensitive data must be physically and logically secured.
5. Employees, who have approval to store highly sensitive data on mobile devices, must receive security awareness and training specific to data media protection requirements.
6. Only authorized personnel are permitted to pick up, accept, transfer, or deliver data storage media containing highly sensitive data including tape backups. Backup tapes must be secured in a locked enclosure during transport and moved directly from the data center to the offsite storage vault.
7. All media storage devices such as hard drives, removable disk drives, diskettes, CD
8. ROMs, zip drives, jump drives, personal digital assistants and other storage media are required to be purged of all data when they are reassigned, salvaged, or transferred to another agency as described in the COV ITRM SEC2003 02.1 standards.

III. Procedure:

1. Data storage records/media is physically secured in server room behind locked door and logically secured using SIMIQ simulation management software.

2. The SIMIQ System uses built-in password protection and access control protocols. SIMIQ system password requirements comply with best practices recommended by "Code of Practice for Information Security Management".
3. Access control provides multilayered access for variety of roles from participant student up to Administrator level. Within each role access to data is limited by scope and/or by the time period during which access may be granted.
4. Video files are purged from system within 2 years of student graduation.

IV. Definitions:

1. Highly Sensitive Data
    a. For purposes of this policy, highly sensitive data currently include personal information that can lead to identity theft if exposed and health information that reveals an individual's health condition and/or history of health services use. While other types of sensitive data, such as student names in combination with course grades obviously exist, the negative impact of unauthorized exposure of data specifically covered by this policy (and described in detail below) is especially acute.
        i. Personal information that, if exposed, can lead to identity theft. "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements about the individual:
            1. Social security number
            2. Driver's license number or state identification card number issued in lieu of a driver's license number
            3. Passport number
            4. Financial account number
            5. Credit card number
            6. Debit card number.

V. Information Technology Policy and Procedures Policy: Data Storage and Media Protection:

1. Health information that, if exposed, can reveal an individual's health condition and/or history of health services use. Encrypted: The transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.