Status (Active) PolicyStat ID (14670128)

Origination	7/10/2019	Owner Faculty Organization
Last Approved	11/8/2023	
Effective	11/8/2023	Policy Area College of Nursing CNG
Last Revised	11/8/2023	Applicability MVHS
Next Review	11/7/2025	

Ensuring Security of Identification and Confidentiality when Using Technology Programs, CNG-100.55

PURPOSE

To define the process to ensure security of identification and maintain confidentiality when accessing web-based College technology programs at St. Elizabeth College of Nursing and electronic health records in health care facilities.

SCOPE

Administration, Faculty, Staff, Students, IT Department

REFERENCES

Mohawk Valley Health System Policy, MV-05-053

SECON Policy, CNG-100.3 Computer and Internet Utilization at the College of Nursing

SECON Policy, CON-100.53 Managing Student Security and Technology Access

DEFINITIONS / ABBREVIATIONS

CITRIX: Software server application

DSFD: Dean of Student and Faculty Development

EPIC: Patient medical record system

FERPA: Family Educational Rights and Privacy Act

HIPAA: Health Insurance Portability and Accountability Act

MOODLE: Web-based course management system

MVHS: Mohawk Valley Health System

RAVE: Alert System

RB: Registrar/Bursar

SONIS: School of Nursing Information System

SECON: St. Elizabeth College of Nursing

PROCEDURE / DIRECTIVE

1. Upon admission to the nursing program, secure log-ins are assigned to each student (see SECON-Managing Student Security and Technology Access Policy CNG-100.53).

2. Students sign a Confidentiality Statement (see attached) upon admission to the nursing program to ensure compliance with HIPAA. Violations of these policies include but are not limited to:

   - Accessing confidential information that is not within the scope of assignment;
   - Accessing more information than necessary to accomplish a given task/job;
   - Misusing, disclosing without proper authorization, or altering confidential information;
   - Disclosing to another person or using another person's sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas;
   - Intentional or negligent mishandling or destruction of confidential information;
   - Leaving a secured application unattended while signed on;
   - Negligence in safeguarding confidential information;
   - Failing to report a privacy or security violation;
   - Removing confidential information from properties without authorization;
   - Discussing confidential information where it can be overhead (i.e. hallways, elevators, cafeteria);
   - Printing confidential health information from an electronic medical record

3. The signed Confidentiality Statement is maintained in the student's admission file.

4. The importance of maintaining security of the log-in and password/code occurs during the admission process by the RB and is a component of the general orientation of incoming freshmen.

5. Students sign a Use of College Computer Form to ensure understanding of the use of College computers and the importance of maintaining security of their log-in and password/code (see attached).

6. The RB distributes each student a secure log-in and initial password/code to systems requiring access to the following programs utilizing technology:

a. MOODLE

b. CITRIX/EPIC

c. SONIS

7. Initial password/codes are required to be changed by the student upon first log-in into the system.

8. Violations of confidentiality may result in dismissal from the College.

9. Deactivation of access to the technology programs is completed at the time of dismissal, withdrawal, or graduation from the College of Nursing by the DSFD or RB(See CNG-100.53)

CONTENT EXPERT(S) / RESEARCHER(S) / CONTRIBUTOR(S): n/a

This Document Replaces: n/a

Attachments

MVHS Confidentiality Signoff.pdf

Use of College Computer Form (CNG-100.55).pdf

Approval Signatures

Step Description	Approver	Date
Owner	Faculty Organization	11/8/2023