# HIPAA Policies

<table>
<thead>
<tr>
<th>SECTION: Administrative Safeguards</th>
<th>NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER: Security Awareness and Training</td>
<td>ISSUED: REV. A REV. B</td>
</tr>
<tr>
<td>POLICY: Malicious Software Policy</td>
<td>PAGE 1 OF 2</td>
</tr>
</tbody>
</table>

## PURPOSE

The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information (ePHI).

## SCOPE

This policy covers all electronic protected health information (ePHI), which is a person’s identifiable health information. This policy covers all ePHI, which is available currently, or which may be created, used in the future. This policy applies to all faculty, staff, students, residents, postdoctoral fellows, and non-employees (including visiting faculty, courtesy, affiliate, and adjunct faculty, industrial personnel, and others) who collect, maintain, use, or transmit ePHI in connection with activities at Creighton University.

## POLICY

Creighton University requires any and all systems that store, access, transmit, manipulate, input, or output Protected Health Information must have a mechanism to isolate PHI from malicious software infection. This includes Creighton owned and non-Creighton owned computers.

## DEFINITIONS

- **Malicious software**
  Software developed for the purpose of doing harm, examples may include viruses, worms, Trojan horse programs, spyware, any program that adversely consumes a disproportionate amount of bandwidth, etc.

- **Protected Health Information (PHI)**
  Individually identifiable health information transmitted or maintained in any form.

- **Electronic Protected Health Information (ePHI)**
  Individually identifiable health information transmitted or maintained in electronic form.

## RESPONSIBILITIES

- **Individuals accessing PHI** are responsible for adhering to this and other Creighton University policies.

- **Administrator of systems containing PHI** are responsible for notifying the HIPAA Security Officer if malicious software has been identified and is a potential threat to other systems or networks.
Administrator of systems containing PHI are responsible for ensuring that any system that has been infected by malicious software is immediately cleaned and properly secured or isolated from the rest of the network.

ADMINISTRATION AND INTERPRETATIONS

This policy shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE POLICIES


EXCEPTIONS

None

VIOLATIONS/ENFORCEMENT

Any known violations of this policy should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures.

The University may advise law enforcement agencies when a criminal offense may have been committed.