

What is HITRUST?

HITRUST stands for the Health Information Trust Alliance.

- It helps organizations from all sectors—but especially healthcare—effectively manage data, information risk, and compliance.
- HITRUST certification by the HITRUST Alliance enables vendors and covered entities to demonstrate compliance to HIPAA requirements based on a standardized framework
- In order to meet HITRUST certification standards, the entire Cone Health workforce must read and acknowledge the Policies and Procedures listed in this module





IMPORTANT

In this presentation

There is a slide for **each of the policy statements and procedures**. A link will be provided for each procedure.

Please review each slide and know how to access these individual policies and procedures.

There will be a quiz at the end of this presentation.

Information Technology Acceptable Use

Policy Statement:

Cone Health's employees/contractors will perform their job responsibilities in an ethical, professional, and secure manner that does not jeopardize the confidentiality, integrity, and availability of covered information; put Cone Health workforce, customers, or patients at risk of harm; or bring about reputation or legal damage to the organization.

Procedure Link:

[Information Technology Acceptable Use Procedure](#)
[\(conehealth.com\)](#)



Personal Device Use

Policy Statement:

Cone Health will ensure personally owned devices used for work-related purposes are subject to the same security requirements and organizationally owned assets.

Procedure Link:

[Personal Device Use Procedure \(conehealth.com\)](https://www.conehealth.com)

Breach Notification

Policy Statement:

This policy defines a breach pursuant to the HIPAA Privacy Rule and provides guidance pertaining to the steps team members and affiliates of Cone Health should take in the event they become aware of a breach.

Procedure Link:

[Breach Notification \(conehealth.com\)](https://www.conehealth.com)



Contingency Plan Management

Policy Statement:

Cone Health will continue to provide ongoing services during natural, environmental, man-made and technology related disruptions.

Procedure Link:

[Contingency Plan Management Procedure \(conehealth.com\)](https://www.conehealth.com/contingency-plan-management-procedure)

Data Classification and Handling

Policy Statement:

Cone Health will identify and assign a unique classification and associated handling instructions to each data/information type the organization owns or is entrusted with.

Procedure Link:

[Data Classification and Handling Procedure \(conehealth.com\)](https://www.conehealth.com/Data-Classification-and-Handling-Procedure)



Disposal of Covered Information

Policy Statement:

Cone Health will dispose of hard copy covered information in a secure and accountable manner.

Procedure Link:

[Disposal of Covered Information Procedure \(conehealth.com\)](https://www.conehealth.com/Disposal-of-Covered-Information-Procedure)

Facility and Environmental Security Management

Policy Statement:

Cone Health will implement and maintain physical security over areas requiring strict access control for the purpose of safety, security, and privacy requirements.

Procedure Link:

[Facility and Environmental Security Management Procedure
\(conehealth.com\)](https://www.conehealth.com)

Information Security Training and Awareness

Policy Statement:

Cone Health will maintain a formal information security training and awareness program.

Procedure Link:

[Information Security Training and Awareness
Procedure \(conehealth.com\)](https://www.conehealth.com/information-security-training-and-awareness-procedure)

Information and Technology Services

This Policy document contains 28 policy statements with corresponding Policies or Procedures.



Policy Title: Information and Technology Services Policy Statements			
Department Responsible: Information and Technology Services	Policy Code: OP-ITS-2020-272	Effective Date: June 25, 2020	Next Review/Revision Date: June 2021
Title of Person Responsible: Chief Information Security Officer	Approval Council: Leadership Alliance Policy and Procedure Committee		Date Approved by Council: June 16, 2020

SCOPE:
This policy is intended for the entire workforce of Cone Health.

POLICY:
Cone Health Information and Technology Services is committed to the security of ITS assets, personnel, and infrastructure. This requires policies and procedures that enable Cone Health to meet the high standards of HITRUST certification. See the policy statements below; for the procedure accompanying each policy, click on the link.

- [Application Security Development](#)
 - Cone Health will maintain an application security development program that outlines the security guidelines involved in the planning, designing, coding, testing, deploying, and supporting of application development.
- [Audit Logging and Monitoring](#)
 - Cone Health will manage and maintain a process for auditing and monitoring user and system (i.e., operating system, application, and database) activity for the purpose of confidentiality, integrity, and availability of covered information.
- [Breach Notification](#)
 - This policy defines a breach pursuant to the HIPAA Privacy Rule and provides guidance pertaining to the steps team members and affiliates of Cone Health should take in the event they become aware of a breach.
- [Change Management](#)
 - Cone Health will maintain a formal process for managing changes to the organization's information technology environment.

Policy Statement:

Cone Health Information and Technology Services is committed to the security of ITS assets, personnel, and infrastructure. This requires policies and procedures that enable Cone Health to meet the high standards of HITRUST certification. [Information Technology Acceptable Use Procedure](#)



Thank you!

Please complete survey link
(as illustrated on the right)

<https://www.surveymonkey.com/r/DXBT5V2>

Please let your Cone liaison (Katina Blackwell-Mitchell)
know you have completed the task.

HITRUST Attestation for Information and Technology Services at Cone Health

1. Please enter your information.

Student Name

First and Last Name

Name of School or Program

Enter school name

* 2. Select student type in drop down. If your type is not listed, please use the text box.

Select Anesthesia or Physician Assistant, OR complete Other (below)

Other (please specify)

Please type one: NP, PMHNP, SRNA, or Midwife

3. Nursing Students, please select school. All other students go directly to #4.

- Graduate Nursing Program (not required to select school)
- North Carolina A & T State University
- Alamance Community College
- Piedmont Community College
- Appalachian State University
- University of North Carolina - Chapel Hill
- Averett University
- University of North Carolina - Greensboro
- Davidson County Community College
- Randolph Community College
- Duke University
- Rockingham Community College
- Elon College
- Winston-Salem State University
- Guilford Community College
- Other (please specify)

4. I hereby attest that I have reviewed and am aware of the Information and Technology Services nine statements and procedures. I received a copy of these policies and procedures and I am able to ask my clinical coordinator any questions or concerns in regards to HITRUST.

I Agree

Select I Agree and SUBMIT

I Disagree