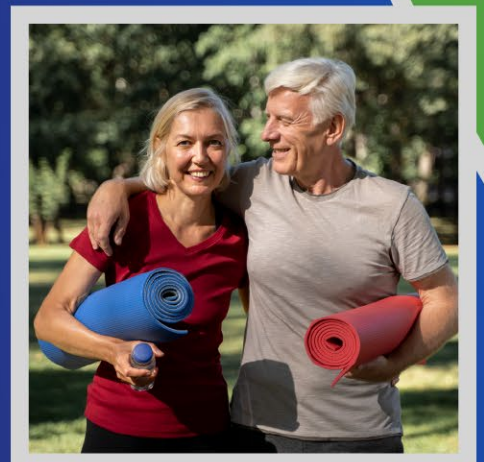

HIPAA: The Health Insurance Portability & Accountability Act

Privacy & Security Training

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

Dale R. Folwell, CPA
State Treasurer of North Carolina

HIPAA Training Goals

During this course, you will learn about:

- The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.
- The HIPAA identifiers that create protected health information (PHI)
- Recognizing situations in which PHI can be mishandled.
- Practical ways to protect the privacy and security of PHI.
- Your responsibilities when handling PHI.

This training focuses on two primary HIPAA rules:

- Section 1: HIPAA Privacy Rules
- Section 2: HIPAA Security Rules

HIPAA – Privacy & Security

Section 1: HIPAA Privacy Rules

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

Dale R. Folwell, CPA
State Treasurer of North Carolina

HIPAA – Privacy & Security

PHI Defined

- Individually identifiable health information is considered “Protected Health Information” or PHI.
- PHI is any health information that can be used to identify an individual, whether living or deceased, that relates to the individual’s past, present, or future physical or mental health or condition, including health care services provided and the payment for those services.
- You may access PHI only when necessary to perform HBR-related functions.

HIPAA – Privacy & Security

Unauthorized PHI Access

- It is never acceptable to look at an individual's PHI "just out of curiosity" even if no harm is intended (i.e., retrieving an address to send a "get well" card).
- It makes no difference if the information relates to a "high profile" person, a close friend, or a family member.
- All PHI is entitled to the same protection and must be kept confidential.

HIPAA – Privacy & Security

PHI Access, Use, and Disclosure is Restricted

- **Access, use, and disclosure is only permitted** when an HBR with appropriate training is performing authorized HBR duties.
- In any other circumstances, accessing, using, or disclosing PHI is not permitted. If you access, use, or disclose PHI for reasons other than performing authorized HBR duties, you may be removed as a Plan HBR.

HIPAA – Privacy & Security

Reality Check

- **A court ordered Walgreens to pay $1.44 million to a customer** whose PHI was impermissibly accessed and disclosed by a pharmacy employee. The employee suspected her husband's ex-girlfriend gave him an STD, looked up the ex-girlfriend's medical records to confirm her suspicions, and shared the information with her husband. He then texted his ex-girlfriend and informed her that he knew about her STD.
- **This unauthorized access to PHI violated the HIPAA Privacy Rules.**

HIPAA – Privacy & Security

How to Identify PHI: 18 Identifiers

These eighteen identifiers, used singularly or in any grouping, constitute PHI.

1. Patient name
2. Address (street address, city, county, ZIP code more than 3 digits, or other geographic codes)
3. Dates directly related to the patient
4. Telephone number
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health Plan beneficiary number
10. Account number
11. Certificate/License number
12. Any vehicle or device serial number
13. Web URL
14. Internet Protocol (IP) address
15. Finger or voice prints
16. Full facial photographs or images
17. Any other unique identifying number, characteristic, or code (in the public realm or not)
18. Age greater than 89 (due to “90-year-old and over” population being relatively small)

HIPAA – Privacy & Security

Major Components of the Privacy Rule

The five components of the Privacy Rule:

1. The Individual's (Member's) Rights
2. The "Minimum Necessary" Standard
3. Research
4. Marketing and Fund Raising
5. Business Associates

Elements 3-5 will likely not be encountered in your role as HBR, but will be briefly addressed so you will have a basic understanding if a member has any questions for you.

HIPAA – Privacy & Security

Component One: The Individual's (State Health Plan Member's) Rights.

Note: most of these rights relate to a member's interactions with the Plan as a covered entity, not with a member's interactions with an HBR.

HIPAA – Privacy & Security

Members have a right to:

- Be informed about protections and uses of their PHI through a Notice of Privacy Practices. The Plan's Notice of Privacy Practices is mailed to members annually.
- Request restrictions on use and disclosure of PHI.
- Request reasonable confidential communications.
- Access, inspect, review, and copy their records.
- Request corrections of their records.
- File a complaint if they believe their rights have been violated or that their PHI is not being adequately protected.
- An accounting of disclosures of their health information (with certain exceptions).
- Receive notice of breach of their unsecured PHI.

If a member wishes to exercise any of these rights, please contact the Plan.

HIPAA – Privacy & Security

Component Two: The “Minimum Necessary” Standard

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

State Treasurer of North Carolina
Dale R. Folwell, CPA

HIPAA – Privacy & Security

Minimum Necessary Standard: For most uses or disclosures of PHI permitted under the Privacy Rules, HIPAA requires that **ONLY** the amount of PHI that is the **MINIMUM NECESSARY** to accomplish the intended purpose be used and disclosed.

Remember: PHI should not be accessed, used, or disclosed unless it is necessary to perform an authorized HBR function.

HIPAA – Privacy & Security

Using PHI

HIPAA regulations permit use or disclosure of PHI for:

- Providing medical treatment (Treatment).
- Processing health care payments (Payment).
- Conducting health care business operations (Health Care Operations).
- Public health purposes as required by law.

Employees of the State Health Plan and HBRs may not otherwise access or disclose PHI unless:

- The member has given written permission.
- It is within the scope of an employee's job duties.
- Proper procedures are followed for using data in research.
- Required or permitted by law.

Note: PHI of a deceased individual is protected for five years following the death of that individual.

HIPAA – Privacy & Security

Component Three: Using PHI for Research

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

State Treasurer of North Carolina
Dale R. Folwell, CPA

HIPAA – Privacy & Security

Research Data

HIPAA regulates how PHI may be obtained and used for research. This is true whether the PHI is completely identifiable or partially "de-identified" in a limited data set.

A researcher or health care provider is not entitled to use PHI without the appropriate HIPAA documentation, including an individual member authorization or an institutionally approved waiver or authorization.

Requests for research data from third parties must be reviewed and approved by the State Health Plan.

HIPAA – Privacy & Security

Component Four: Using PHI for Marketing and Fund-Raising

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

Dale R. Folwell, CPA
State Treasurer of North Carolina

HIPAA – Privacy & Security

Marketing and Fund Raising

The Plan must first obtain authorization from its members before using or disclosing their individual PHI for marketing or fund-raising purposes. The Plan must also inform members of their right to “opt out” of receiving marketing or fund-raising communications from our partners.

For fund-raising purposes, HIPAA permits a covered entity to themselves use, or disclose to a Business Associate or institution-related foundation, only two types of PHI without specific written member authorization:

1. Basic demographic information relating to an individual.
2. Dates of health care provided to an individual.

The Plan does not use other individual PHI for marketing or fund-raising purposes.

Use of any other kind of PHI for fund raising by the Plan requires that an individual be allowed the right to opt out.

HIPAA – Privacy & Security

Component Five: Business Associates

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

Dale R. Folwell, CPA
State Treasurer of North Carolina

HIPAA – Privacy & Security

Business Associates

A Business Associate relationship exists when an individual or entity creates, receives, maintains, or transmits PHI on behalf of the Plan or the Department.

The Department's Business Associates must:

- Have a Business Associate Agreement (BAA) with the Plan.
- Use appropriate safeguards to prevent the unauthorized use or disclosure of PHI.
- Notify the Plan's HIPAA Compliance Officer if any PHI has been improperly accessed, used, or disclosed.
- Ensure that their employees and/or subcontractors receive HIPAA training.
- Protect PHI to the same degree as required of the Plan.
- Obtain "satisfactory assurances" from subcontractors, in the form of a written agreement, that they will appropriately safeguard PHI.
- Notify the State Health Plan HIPAA Compliance Officer in the event of a breach of PHI.

HIPAA – Privacy & Security

Section 2: HIPAA Security Rules

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

State Treasurer of North Carolina
Dale R. Folwell, CPA

HIPAA – Privacy & Security

Forms of PHI include:

- Written
- Spoken
- Electronic Data
- Any other means of communicating PHI

It is the responsibility of every HBR to protect the privacy and security of PHI in all its forms.

HIPAA – Privacy & Security

Verbal Communication – Be aware of your surroundings when discussing confidential information, including PHI. Do not discuss confidential information or PHI in public areas such as in cafeterias or restaurants, while walking in the facilities, or outside around the building.

Use caution when conducting conversations in semi-private rooms, cubicles, corridors, elevators, and stairwells.

Phone Calls – While there is no foolproof way to identify a member over the phone, the goal should be to significantly increase the degree of certainty. If a member calls regarding their health benefits, request that they verify their identification by providing you with their date of birth.

Voice Mails – Avoid leaving PHI in your message. Identify yourself leaving only your name, phone number, and call-back instructions.

HIPAA – Privacy & Security

Confidentiality, Integrity, and Availability of PHI (CIA)

The Security Rule focuses on safeguarding PHI by maintaining the confidentiality, integrity, and availability of PHI in all its various forms.

Confidentiality means that PHI is not improperly made available or disclosed.

Integrity means that PHI has not been improperly altered or destroyed.

Availability means that PHI is accessible and useable upon demand by an authorized person or system.

"CIA"

HIPAA – Privacy & Security

Administrative Safeguards for "CIA"

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

State Treasurer of North Carolina
Dale R. Folwell, CPA

HIPAA – Privacy & Security

Faxing and Printing

- Documents containing PHI should be picked up immediately from printers, copiers, or fax machines.
- Transmit the minimum amount of information necessary to accomplish the purpose for which the request is made. A request for PHI should not be honored unless it is specific as to the purpose and the information required.
- Verify fax numbers before sending, and verify receipt of the faxed document.
- All documents with PHI must be accompanied by a cover sheet with a notification that the information being transmitted is confidential.
- Documents containing especially sensitive medical information, including, but not limited to, AIDS/HIV information; mental health and developmental disability information; sexual or other abuse information; and sexually transmittable disease information should not be faxed and should only be sent by secure means.

HIPAA – Privacy & Security

Handling and disposing documents & electronic media

- Hard copies of PHI should be treated with care. If possible, shred or otherwise securely destroy paper, CDs, flash drives, or other portable electronic media containing PHI.

Secure Transportation and Transfer of PHI

- You should not remove PHI from your workplace.
- If you must remove PHI from your workplace, physical transfer of PHI must be handled in a way that protects its security.
- Do not leave PHI in areas visible to the public while transporting.
- Minimum security precautions during transfer include placing laptops, documents, etc., in the trunk of your vehicle, or in another area not visible to others.
- No information should be transferred to another entity or business associate unless it is necessary to complete a duty as an HBR.

HIPAA – Privacy & Security

Physical Safeguards to Ensure "CIA"

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

State Treasurer of North Carolina
Dale R. Folwell, CPA

HIPAA – Privacy & Security

Facility Access Controls

- Follow building access policies and procedures regarding security codes, facility access, badges, and visitors.

- **Workspace**
- Desks should be cleared of all paperwork and files prior to leaving at the end of each day.
- Documents containing PHI should be stored in a secure location, or within a locked desk drawer when you are out of sight of your desk or workstation.
- Computer and other equipment used to access PHI must be located in secured areas.
- Monitors should be positioned in a way or shielded from view so that an unauthorized individual cannot read the displayed PHI.

Never leave your laptop unattended in public spaces.

HIPAA – Privacy & Security

Technical Safeguards to Ensure “CIA”

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

State Treasurer of North Carolina
Dale R. Folwell, CPA

HIPAA – Privacy & Security

eBenefits

- As a Health Benefits Representative for the State Health Plan, you may have access to the Document Center in eBenefits to upload secure files containing PHI to share with the Plan.

Email Security

- If possible, email containing PHI must be encrypted before sending to prevent unauthorized access.
- Don't open attachments in emails unless you know who sent it and what it is.
- Don't click on email links. Instead, type the URL of the site directly into your browser.

Email transmission of any highly sensitive PHI, such as related to mental health, HIV/AIDS, STDs, alcohol & chemical dependency and pregnancy, is prohibited. This information should be sent only by secure means.

HIPAA: Additional Email Security Procedures

- HBRs who need to send the Plan a HIPAA sensitive document may send an email to HBRInquiries@nctreasurer.com requesting an ENCRYPTED email be sent back to them.
- The HBR will then attach the document to the ENCRYPTED email and send it back to the HBRInquiries@nctreasurer.com email.
- This will ensure the document containing HIPAA information gets to the Plan securely.
- This procedure should only be used when an HBR has view-only access to eBenefits and the HBR has a time sensitive document that needs to be sent to the Plan.
- Note: Sending HIPAA sensitive documents to the Plan via a regular (unsecured) email address constitutes a violation of the HIPAA Policy and can hold the HBR accountable if discovered.

HIPAA – Privacy & Security

WiFi Security

- Never connect a device containing PHI to public WiFi. Those WiFi access points are not secure and could be provided by malicious individuals looking to gain unauthorized access to your device.

Working Offsite

- If you take your laptop or other device out of the office never leave it unattended in unsecured areas. Immediately report the loss or theft of any mobile devices to your supervisor, IT, or Information Security Office.

HIPAA – Privacy & Security

Passwords are your best line of defense!

Many security breaches come from within an organization – and many of these occur because of bad password habits.

- Always use strong passwords (at least eight characters, containing a combination of letters, numbers, and special characters).
- To protect PHI and yourself, never share your password. If you share your password, someone can impersonate you. They may also have access to your private data!
- Don't write your password down.

HIPAA – Privacy & Security

Breaches of PHI – What is a Breach?

- A breach is, generally, an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI.

HIPAA – Privacy & Security

Breaches of PHI – What is a Breach?

- A breach is, generally, an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI.

Breaches of PHI

HBRs are Responsible for Reporting Breaches or Suspected Breaches

- The Plan is required to take reasonable steps to lessen the harmful effects of a confirmed breach involving compromised PHI. This includes notifying the individuals whose information has been breached. The Plan also has the legal obligation to report breaches to the federal government's Secretary of Health and Human Services.
- If you believe that there has been a significant breach of data involving PHI, please contact the Plan as soon as possible. The Plan will work with you to determine whether further action is needed.

If you're unsure about how to handle HIPAA-related issues, talk to your supervisor or contact the Plan.

You can also learn more about HIPAA here.

Thank you!

North Carolina State Health Plan
FOR TEACHERS AND STATE EMPLOYEES
A Division of the Department of State Treasurer

Dale R. Folwell, CPA
State Treasurer of North Carolina