Current Status: *Active* **PolicyStat ID:** *7944388*

Origination:	*07/2018*
Effective:	*06/2020*
Last Approved:	*06/2020*
Last Revised:	*06/2020*
Next Review:	*06/2023*
Owner:	*David Behinfar: HCS Exec Dir Privacy*
Policy Area:	*HIPAA - Privacy*
Policy Tag Groups:	
Applicability:	*UNC Health Care System (all owned and managed entities)*

Breach Notification

APPLICABILITY:

This policy applies to the following entities (collectively referred to as **"UNC Health"** in this policy):

✓	UNC Health Care System / UNC Medical Center*	✓	Johnston Health
✓	UNC Physicians Network	✓	Lenoir Memorial Hospital
✓	UNC Physicians Network Group Practices / UNC Physicians Group Practices II	✓	Margaret R. Pardee Memorial Hospital
✓	Rex Healthcare / Rex Hospital	✓	Nash Healthcare System/Nash Hospitals
✓	Chatham Hospital	✓	Wayne Memorial Hospital
✓	Caldwell Memorial Hospital		
✓	UNC Rockingham Health Care / UNC Rockingham Hospital		

***UNC Medical Center includes all UNC Hospitals' facilities and the clinical patient care programs of the School of Medicine of UNC-Chapel Hill (including UNC Faculty Physicians).**

I. Description

As required by federal law and any applicable state law, UNC Health will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as the result of a breach and as applicable, UNC Health will also notify HHS, the media, affected patients, and any designated state agency of such breaches.

Included within the scope of this policy are the patient care programs of the UNC School of Medicine (UNC SOM). As a result, this policy shall apply to all UNC SOM personnel, including but not limited to faculty, staff, students, trainees, interns and volunteers who may be full-time, part-time, paid or unpaid who create, store, transmit, access or use any patient information in support of clinical purposes for UNC Health or any other healthcare entity.

II. Policy

The UNC Health Privacy Office or the Facility Privacy Officer at a UNC Health Managed Facility, in consultation with legal counsel and appropriate workforce members, as needed, will conduct an investigation of any suspected, alleged or actual unauthorized use or disclosure of PHI. Upon confirmation by the respective UNC Health Privacy Office that an incident has occurred involving the unauthorized use or disclosure of PHI, UNC Health shall perform a written breach risk assessment under federal law and an additional analysis under state law to determine whether a breach has occurred.

FEDERAL LAW / HIPAA – RISK ASSESSMENT AND BREACH NOTIFICATION

A. **Determine whether a breach has occurred.** The UNC Health Privacy Office (and as applicable, all UNC Health Facility privacy officers) shall perform a four-step process to determine whether a breach has occurred and whether breach notification is required under federal law that includes documentation of the following steps:

   1. **Step 1: Determine whether the use or disclosure violates the Privacy Rule.** Determine whether the use or disclosure of PHI violated the HIPAA Privacy Rule.
   2. **Step 2: Determine whether the PHI was unsecured**. Determine whether the PHI was secured by a method or technology described in HHS guidance, such as encryption or destruction.
   3. **Step 3: Determine whether an exception applies**. The three exceptions to the breach notification rule are: (i) the *unintentional* acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a UNC Health Facility or a business associate, performing his/her duties, if made in good faith and within the scope of authority, and such situation does not result in a further impermissible use or disclosure; (ii) the *inadvertent* disclosure of PHI by a person authorized to access the PHI at a UNC Health Facility or a business associate's location to another person authorized to access the PHI at a UNC Health Facility or the same business associate's location, or an organized health care arrangement ("OHCA") in which the UNC Health Facility participates, and such situation does not result in a further impermissible use or disclosure; or (iii) PHI was disclosed to a person who, in the good faith judgment of the UNC Health Facility or a business associate, reasonably would *not have been able to retain* the information. If one of the above exceptions applies, continue to Step 4.
   4. **Conduct a risk assessment.** If no exception listed above applies, then a risk assessment shall be conducted to determine whether there is a low probability that PHI has been compromised. It is presumed that each impermissible use or disclosure of unsecured PHI is a breach and requires breach notification (unless an exception in Step 3 applies) or, based on a risk assessment, it is determined that there is a low probability that the PHI has been compromised. To conduct the risk assessment the UNC Health facility Privacy Officer or the UNC Health Privacy Office shall complete the UNC Health Privacy Incident and Risk Assessment Form (available from the UNC Health Privacy Office) or similar form which takes the following factors into consideration: (i) the nature and extent of the PHI involved, including the types of identifiers, the likelihood of re-identification and the ability to link the PHI to other available information; (ii) the unauthorized person who used the PHI or to whom the disclosure was made (e.g., the information was disclosed to another health care provider); (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated (e.g., the PHI has been retrieved or destroyed and the recipient signs an attestation). Based on the risk assessment, if it is determined that there is a low probability that PHI has been compromised, then a breach has not occurred and breach notification is not required. If it is

determined that there is more than a low probability that PHI has been compromised, UNC Health shall issue a written breach notice to all affected individuals as set forth below.

B. **Discovery of a Breach**. A breach of unsecured PHI will be treated as discovered by UNC Health or a Business Associate as of the first day on which the breach is known, or should reasonably have been known, to have occurred. A breach is considered "discovered" if it is known by someone (other than the person committing the breach) who is an employee, officer, or other agent of UNC Health or the Business Associate.

C. **Completion of Risk Assessment**. The UNC Health Privacy Office or his/her designee (or the Facility Privacy Officer or his or her designee, will document the risk assessment on the UNC Health Privacy Incident and Risk Assessment Form (available from the UNC Health Privacy Office).

D. **Notice of breach at UNC Health Managed Member Facility to UNC Health Privacy Office**. Facility Privacy Officers at UNC Health Managed Facilities are encouraged to consult with UNC Health Privacy Office on any breaches in which there is a greater than low probability of compromise that have been substantiated at UNC Health Managed Facilities.

E. **Timeliness of notice**. All required notifications to patients and/or the Office for Civil Rights must be made without unreasonable delay, but in no case later than sixty (60) days after the discovery of the breach. Additionally, pursuant to NC state laws notification to the NC State Attorney General and or affected individuals may also need to be made (*see Section II below in this policy*) in which case such written notifications must be made without unreasonable delay.

F. **Delay of notification for law enforcement purposes**. UNC Health may delay a required notification if a law enforcement official determines that such notice or notification would impede a criminal investigation or cause damage to national security. UNC Health will delay its report of the incident until the date specified by the law enforcement agency, but not to exceed thirty (30) days for an oral request, for the time period specified by the law enforcement official in writing. UNC Health will document all requests by law enforcement agencies made orally, including the agency name, the official's name, and the date of the request.

G. **Content of notification**. UNC Health will, to the extent possible, include the following information in the notice, in plain language: (a) description of the incident(s); (b) date(s) of the breach; (c) date the breach was discovered; (d) description of the types of unsecured PHI involved (e.g., name, social security number, etc.); (e) steps an individual should take to protect himself/herself against potential harm; (f) description of investigation, mitigation efforts, and prevention of future breaches; and (g) toll-free contact information for UNC Health.

H. **Types of notice.** UNC Health will provide all of the following type(s) of notice that apply to the breach of unsecured PHI.

    1. **Individual notice**. In all cases, except as set forth in paragraph I(b) below, written notice will be provided to each affected individual by first-class mail, or if requested by the individual, by email. Additional mailings may be utilized as information becomes available.

    2. **Substitute notice**. If there is insufficient or out-of-date contact information that precludes individual notice, UNC Health will provide a substitute form of notice. If there are ten (10) or more individuals for whom there is insufficient or out-of-date information, the substitute form of notice will be a conspicuous web posting on the UNC Health home page (or if applicable, the UNC Health Member's home web page) or notice in major print or broadcast media (including geographic areas where affected individuals reside). The notice will include the toll-free number where the affected individual can obtain further information, as required by federal law.

3. **Additional notice.** If UNC Health determines that the breach requires urgency because of the possible imminent misuse of unsecured PHI, UNC Health may, in addition to written notice, provide notice to individuals by telephone, or other means, as appropriate.
4. **Media notice.** If the breach involves more than 500 individuals, UNC Health will also provide notice in prominent media outlets (in the State or jurisdiction where those individuals reside).
5. **Notice to HHS.** If the breach involves 500 or more individuals, UNC Health will provide notice to HHS immediately. If the breach involves less than 500 individuals, Facility will maintain a log of any such breach and submit the log for the previous calendar year to HHS prior to March 1st of the calendar year following the year in which the breach occurred.

I. **Costs and Expenses Associated with Notification**.

1. **UNC Health Owned Member Facilities - Costs of Notification:** While the UNC Health Privacy Office will oversee and/or provide support for the notification process, the Department, Division, Clinic, or other UNC Health unit or UNC School of Medicine Department or Division from where the information was acquired or otherwise was responsible for the loss, theft or unauthorized access of PHI will be responsible for the costs and labor associated with notifying the affected persons including any and all other associated costs such as costs associated with outside vendors providing call center support services or credit monitoring or identity theft protection services.
2. **UNC Health Managed Member Facilities – Costs of Notification**: Each UNC Health Managed Facility shall be responsible for its own costs of notification including any and all other associated costs such as costs associated with outside vendors providing call center support services or credit monitoring or identity theft protection services.

NORTH CAROLINA – SECURITY BREACH ANALYSIS AND NOTIFICATION

A. **Determine whether a Security Breach has occurred.** The UNC Health Privacy Office and/or any UNC Health Managed Member Facility Privacy Office performing an incident investigation shall follow the process below to determine whether a security breach has occurred and whether a security breach notification is required under state law. The following steps have been incorporated into the UNC Health Privacy Incident and Risk Assessment Form (available from the UNC Health Privacy Office) and are referred to below by reference:

1. **Step 1 – Determine whether someone has obtained unauthorized access to and acquired records or data from a UNC Health Member**. If no one has obtained unauthorized access to and acquired records or data **from a UNC Health Member**, a security breach has not occurred. If someone has obtained unauthorized access to and acquired records or data **from a UNC Health Member**, continue to Step 2.
2. **Step 2 – Determine whether the accessed and acquired records or data contain personal information ("PI"), as defined in the Definitions section below**. If the records or data do not contain PI, a security breach has not occurred. If the records or data do contain PI, continue to Step 3.
3. **Step 3 – Determine whether the PI in the records or data was encrypted or redacted**. If the PI was redacted (rendered unreadable or truncated so that no more than the last four digits of the identification number is accessible), a security breach has not occurred. If the PI was encrypted, a security breach has not occurred UNLESS the key or confidential process for decrypting the PI was accessed or disclosed along with the encrypted records or data. If the PI was not redacted or encrypted, or was encrypted but the key/confidential process was also accessed/disclosed, continue

to Step 4.

4. **Step 4 – Determine whether an employee or agent of UNC Health acquired the PI in good faith and for a legitimate purpose**. If an employee or agent of UNC Health acquired the PI in good faith and for a legitimate purpose, and you are able to verify that the PI (1) was not used for a purpose other than a lawful purpose of Facility and (2) is not subject to further unauthorized disclosure, then a security breach has not occurred. Otherwise, continue to Step 5.
5. **Step 5 – Analyze the facts to determine the risk**. If it is determined that illegal use of the PI has occurred, illegal use of the PI is likely to occur, or the unauthorized access to and acquisition of the PI creates a material risk of harm to an individual, a security breach has occurred and notification must be issued as set forth below. If it is determined that illegal use of the PI has not occurred and is not likely to occur, and that the unauthorized access to and acquisition of the PI does not create a material risk of harm to an individual, a security breach has not occurred and notification is not required.

B. **Timeliness of notice**. Notifications to the affected person(s) shall be made without unreasonable delay following discovery or notification of the security breach, consistent with the legitimate needs of law enforcement (as set forth below), and consistent with any measures necessary to determine sufficient contact information, determine the scope of the security breach, and restore the reasonable integrity, security, and confidentiality of the data system.

C. **Delay of notification for law enforcement purposes**. Notification shall be delayed if a law enforcement agency informs UNC Health that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the UNC Health documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. Notification shall be provided without unreasonable delay after the law enforcement agency communicates to UNC Health its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

D. **Content of notification.** The notice shall be clear and conspicuous and include all of the following: (a) a description of the incident in general terms; (b) a description of the type of PI that was subject to unauthorized access and acquisition; (c) a description of the general acts of UNC Health to protect the PI from further unauthorized access; (d) a telephone number for a representative of UNC Health that the person may call for further information and assistance (if one exists); (e) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports; (f) the toll-free numbers and addresses for the major consumer reporting agencies; and (g) the toll-free numbers, addresses, and Web site address for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

E. **Types of notice**. UNC Health will provide **all of the following type(s) of notice that apply** to a security breach:

1. **Individual notice**. In all cases, except as set forth in paragraph E.2 below, notice will be provided to each affected individual in writing; by e-mail, but only if UNC Health has a valid e-mail address for the individual and the individual has agreed to received communications electronically if the notice provided is consistent with the provisions regarding electronic records and signature for notices legally required to be in writing set forth in 15 U.S.C. § 7001; or by telephone provided that contact is made directly with the affected individual.

2. **Substitute notice**. UNC Health may provide substitute notice in lieu of individual notice if (a) UNC Health demonstrates that the costs of providing individual notice would exceed $250,000; or (b) UNC Health demonstrates that the affected class of individuals to be notified exceeds 500,000; or (c) if UNC Health does not have sufficient contact information or consent to provide individual notice in writing, by email or by phone, but only for those individuals without sufficient contact information or consent; or (d) if UNC Health is unable to identify particular individuals affected, but only for those unidentifiable individuals. Substitute notice shall consist of: (a) e-mail notice when UNC Health has an e-mail address for the individual; (b) conspicuous posting of the notice on UNC Health Web page (if one is maintained); and (c) notification to major statewide media.
3. **Notice to the North Carolina Attorney General's Office**. In all cases, UNC Health shall notify without unreasonable delay the Consumer Protection Division of the North Carolina Attorney General's Office of the nature of the breach, the number of individuals affected by the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice to individuals. UNC Health shall use the North Carolina Security Breach Reporting Form provided by the North Carolina Attorney General's Office.
4. **Notice to consumer reporting agencies**. In the event that UNC Health provides notice to more than 1,000 individuals in connection with the breach, UNC Health shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

III. Definitions

Breach – means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the PHI."

HHS – means the Department of Health and Human Services.

Personal Information or PI – means a person's first name or first initial and last name in combination with any of the following identifying information:

- Social security or employer taxpayer identification numbers.
- Driver's license, State identification card, or passport numbers.
- Checking account numbers.
- Savings account numbers.
- Credit card numbers.
- Debit card numbers.
- Personal Identification (PIN) Code (a numeric and/or alphabetical code assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that financial transaction card).
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
- Digital signatures.
- Any other numbers or information that can be used to access a person's financial resources.
- Biometric data.
- Fingerprints.
- Passwords.
- Parent's legal surname prior to marriage.

Personal information does **not** include publicly available directories containing information an individual has

voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.

Security Breach – means an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

Unsecured PHI – means PHI not secured through the use of a technology or methodology that (i) is specified in guidance from HHS and (ii) renders the information unusable, unreadable, or indecipherable to unauthorized individuals. Pursuant to Guidance, HHS has identified encryption and destruction as technologies/methodologies that render PHI unusable, unreadable or indecipherable.

IV. References

Federal Statute: §§ 13400, 13402 of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Public Law 111-5; 42 USC 17932, 17932.

State Statute: N.C. Gen. Stat. § 75-60 *et seq*. (North Carolina Identity Theft Protection Act)

Regulations: 45 C.F.R. Part 164, Subpart D, §§ 164.400-164.414, 74 Fed. Reg. 42,740-42,770 (Aug. 24, 2009).

Guidance: Guidance to Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (updated annually by OCR) ("Guidance")

V. Related Policies/Forms

None

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
	Jerylyn Williams: Chief Audit & Compliance Ofcr	06/2020
SYSTEM Site Administrator	Emilie Hendee: HCS Attorney Sr	06/2020
	David Behinfar: HCS Exec Dir Privacy	06/2020

Applicability

Caldwell Memorial Hospital, Chatham Hospital, Johnston Health, Nash UNC Health Care, Pardee Hospital, UNC Health Care System, UNC Lenoir Health Care, UNC Medical Center, UNC Physicians Network, UNC Rex Healthcare, UNC Rockingham Health Care, Wayne Memorial Hospital