Current Status: *Active*	**PolicyStat ID:** *5255750*

Origination:	*09/2013*
Effective:	*08/2018*
Last Approved:	*08/2018*
Last Revised:	*08/2018*
Next Review:	*08/2021*
Owner:	*David Behinfar: HCS-Privacy Dir*
Policy Area:	*HIPAA - Privacy*
Policy Tag Groups:	
Applicability:	*UNC Medical Center*

Identity Theft Protection

I. Description

Requirements for safeguarding personal information consistent with North Carolina's Identity Theft Protection Act, N.C. General Statutes § 75-60 *et seq.*, and, as applicable to UNC Hospitals and the clinical programs of the UNC School of Medicine only ("State Agency Entities"), section 132-1.10 of the Public Records Act, N.C. General Statutes § 132-1.10.

II. Rationale

In accordance with the Identity Theft Protection Act of 2005, North Carolina General Statutes § 75-60 *et seq.*, (the "Act"), the University of North Carolina Health Care System (UNCHCS) and its affiliates are required to safeguard certain identifying information of patients, employees, vendors and other individuals providing to the UNCHCS entity the information covered by the Act. This policy provides procedures to enable UNCHCS to comply with the Act and for the State Agency Entities to comply with the Public Records Act to the extent it affects the safeguarding of such information.

III. Policy

A. Procedure

1. Definitions

a. Security Breach

i. 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

ii. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information, along with the confidential process or key

iii. Good faith acquisition of personal information by an employee or agent of UNCHCS 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 and is not subject to further unauthorized disclosure

b. Personal Information

Personal Information (as defined by the Act and N.C.G.S. § 14-113.20, the latter of which is referenced in the Identity Theft Protection Act to define "personal information," excluding some identifiers eliminated by N.C.G.S. § 132-1.10 for state agencies) includes the first name or first initial and last name of an individual plus any of the following:

i. Social security or employer taxpayer identification numbers
ii. Drivers license, state identification card, or passport numbers (except drivers license numbers appearing on law enforcement records)
iii. Checking account numbers
iv. Savings account numbers
v. Credit card numbers
vi. Debit card numbers
vii. Personal Identification (PIN) Code as defined in G.S. §14-113.8(6): 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
viii. Digital signatures
ix. Any other numbers or information that can be used to access a person's financial resources (expressly including an email address, parent's legal surname prior to marriage, and password)
x. Biometric data
xi. Fingerprints
xii. Passwords

c. Breach Response Team.

The UNCHCS breach response shall be conducted by either the UNCHCS Chief Privacy Officer or the UNCHCS Chief Security Officer. Such other personnel and offices shall participate in the breach response as necessary and as determined by the UNCHCS Chief Privacy Officer or the UNCHCS Chief Security Officer.

2. Collection and Use of Social Security Numbers and Other Personal Information

Generally, N.C.G.S. §§ 116-37(k) and 105A-3 require that the State Agency Entities attempt to collect social security numbers ("SSN") from patients and other individuals who may become debtors to either of them, and, due to these requirements, the Act allows the State Agency Entities to continue to collect SSNs. The State Agency Entities are not required to collect other types of Personal Information, but if other types of Personal Information are provided, the information must be protected as stated below. The State Agency Entities and/or other UNC HCS entities must take the following steps with respect to all Personal Information, including SSNs:

a. The State Agency Entities must segregate SSNs on a separate page from the rest of a record, or as otherwise appropriate, so the SSN can be more easily deleted pursuant to a valid public records request.

b. Upon request, a State Agency Entity must provide to the individual, at the time of or prior to the actual collection of the SSN, a statement of the purpose or purposes for which the SSN is being collected and used.

c. The State Agency Entities must not use the SSN for any purpose other than the purpose stated.

d. The State Agency Entities and the other UNCHCS entities must not intentionally communicate or otherwise make available to the general public a person's SSN or other Personal Information. Personal Information shall be confidential and shall not be considered a public record. If a public records request is delivered to a State Agency Entity, all Personal Information will be deleted prior to sending a response.

e. The State Agency Entities must not intentionally print or imbed an individual's SSN on any card required for the individual to access government services.

f. The State Agency Entities and the other UNCHCS entities must not require an individual to transmit the individual's SSN over the Internet, unless the connection is secure or the SSN is encrypted.

g. The State Agency Entities and the other UNCHCS entities must not require an individual to use the individual's SSN to access an Internet Website, unless a password or unique personal identification number or other authentication device is also required to access the Internet Website.

h. The State Agency Entities and the other UNCHCS entities must not print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires that the SSN be on the document to be mailed. A SSN that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

i. For exceptions to and assistance with these requirements, contact the UNC HCS Compliance Officer or the Legal Department.

3. Security Breaches and Notification

All UNCHCS entities will take reasonable steps to prevent Security Breaches with respect to Personal Information. If a potential Security Breach occurs, any UNCHCS personnel who becomes aware of the potential Security Breach should notify the UNCHCS Privacy Officer (or the facility privacy Officer) either directly or through the UNCHCS Privacy and Compliance Hot-line ((800) 362-2921).

UNCHCS is required to notify in writing affected individuals of Security Breaches. The requirements for notification and other necessary actions in response to a breach are set forth in the UNCHCS privacy policies (See UNCHCS Breach Notification Policy).

IV. References

Identity Theft Protection Act, N.C.G.S. § 75-60

Public Records Act, N.C.G.S. § 132-1.10

Financial Transaction Card Crime Act, N.C.G.S. § 14-113.8(6)

Financial Identity Fraud, N.C.G.S. § 14-113.20

University of North Carolina Health Care System, N.C.G.S. § 116-37(k)

Setoff Debt Collection Act, N.C.G.S. § 105A-3

V. Related Policies/Forms

See also UNCHCS Breach Notification Policy

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
Policy Stat Administrator	Patricia Ness: Nurse Educator	08/2018
	Jerylyn Williams: VP Chief Audit & Comp Officer	08/2018
	David Behinfar: HCS-Privacy Dir	08/2018

Applicability

UNC Medical Center