

Attachment “A”

Data Breach Notification Flow

Based on:

- NC Identity Theft Protection Act

http://www.ncleg.net/enactedlegislation/statutes/pdf/byarticle/chapter_75/article_2a.pdf

- HHS Breach Notification for Unsecured PHI; Interim Final Rule

<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

Potential Incident of Data Breach Reported

Not a reportable breach – stop here

NC Identity Theft Protection Act

Does it involve access to and acquisition of unredacted or unencrypted personal info as defined on Slide 3? (See Risk Assessment Tool)

No

Yes

Has illegal use of the personal information occurred or is reasonably likely to occur or creates a material risk of harm to a consumer? (See Risk Assessment Tool)

No

Yes

Reportable Data breach has occurred (See slide 4)

HITECH

Does it involve unsecured or unencrypted PHI?

No

Yes

Does the incident violate the HIPAA Privacy rule?

No

Yes

Does this data breach “pose a significant risk of financial, reputational, or other harm to the individual” affected? *(See NCHICA Risk Assessment Tool)

No

Yes

Does the incident qualify as an exemption?
 1) Good faith, unintentional **acquisition, access or use** of PHI by UHS employee/workforce
 2) Inadvertent **disclosure** to another authorized person within the entity or its OHCA
 3) Recipient could not reasonably have retained the data
 4) Data is limited to limited data set that does not include dates of birth or zip codes

*Covered entities may also wish to review OMB Memorandum M- 07-16 for examples of the types of factors that may need to be taken into account in determining whether an impermissible use or disclosure presents a significant risk of harm to the individual. (See slide 8)

“Personal information” A person’s first name or first initial *and* last name in combination with any of the following

http://www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.20.html

- Social security or employer taxpayer identification numbers
- Drivers license, State identification card, or passport numbers
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
- 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

Reportable Data Breach Has Occurred*

NC Identity Theft Prevention Act

Contact individuals affected

(See slide 6)

Notify NC Attorney General's Office

(See slide 9)

HITECH

Contact individuals affected *(See slide 5)*

Are 500 or more individuals affected?

No

Log for annual report to HHS

Yes

Are more than 500 of the affected individuals in a single state or jurisdiction?

No

Notify HHS

Yes

Provide notice to prominent media outlets serving the state or jurisdiction of the affected residents.

If required to notify more than 1,000 consumers of a breach of security, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p).

(See slide 7)

*Determine whether or not credit monitoring services will be offered with notification

Contact individuals affected

HITECH

Notification letters must include:

- 1) Brief description of what happened, including date of breach and date of discovery
- 2) Description of unsecured PHI involved
- 3) Steps individuals should take to protect themselves from potential harm
- 4) Description of what covered entity is doing to investigate the breach, mitigate harm to the individual, protect against further breaches
- 5) Contact procedures for individuals to ask questions to include a toll-free number, email address, website or postal address.

Generate and mail 1st class letter with required contents. If urgent, telephone notice in addition.

If no known address, Email if patient provided prior authorization for email correspondence.

If deceased, to next of kin or personal representative, if known. If minor or lacking legal capacity, to parent/legal rep.

If some contact information out-of-date

No substitute notice required if parent, legal representative, or next-of-kin contact information is out-of-date.

If less than 10 individuals, substitute notice may be made by alternative written notice; e.g., telephone or email (w/o prior authorization), or posting on website if lacking current contact information.

If more than 10 individuals, substitute notice is required in the form of either:

- 1) Conspicuous notice on our webpage for 90 days
- 2) Conspicuous notice in major print/broadcast media serving geographic area of affected patients (no specified duration or frequency).
Must provide toll-free number for 90 days

Contact individuals affected

NC Identity Theft Prevention Act

Notice shall be provided by **one of the following** methods:

- (a) Written notice.
- (b) Email if individual agreed to receive communications electronically
- (c) Telephonic notice (if made directly to the affected individual)
- (d) If **one or more** individuals unknown or with insufficient contact information must provide **substitute notice** (also permitted if the cost of providing notice would exceed \$250,000 or if the affected class of affected individuals exceeds 500,000)
- (e) If more than 1,000 individuals affected, notice to all consumer reporting agencies.

(See slide 7)

Content: Notice under this section shall be clear and conspicuous and shall include at a minimum:

- (1) A description of the incident in general terms;
- (2) The type of information involved;
- (3) The entity's general acts to protect the information from further unauthorized access;
- (4) The entity's telephone number ;
- (5) Advice directing the person to remain vigilant by reviewing account statements and monitoring free credit report;
- (6) Toll-free numbers for the major consumer reporting agencies;
- (7) Toll-free numbers, address, and Website addresses for the FTC and the NC Attorney General's Office, identified a sources of additional information about preventing identity theft

Substitute notice shall consist of **all** of the following:

- (1) E-mail notice when the entity has an e-mail address for the affected individuals.
- (2) Conspicuous posting of notice on the entity's existing website.
- (3) Notification to major statewide media.

15 U.S.C. Section 1681a(p)

Consumer Reporting Agency : a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide:

1. Public record information
2. Credit account information from persons who furnish that information regularly and in the ordinary course of business

[http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=\\$\\$xa\\$\\$busc15.wais&start=8161695&SIZE=30178&TYPE=PDF](http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc15.wais&start=8161695&SIZE=30178&TYPE=PDF)

OMB Memorandum M-07-16

<http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>

Five factors to consider in assessing the likely risk of harm:

1. Nature of the data elements breached.
2. Number of individuals affected.
3. Likelihood the information is accessible and usable.
4. Likelihood the breach may lead to harm
 - a. Broad Reach of Potential Harm. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.
 - b. Likelihood Harm Will Occur. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name.
5. Ability of the entity to mitigate the risk of harm.

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business or Government Agency Owning or Licensing
Information Affected by the Breach: _____

Address: _____

Telephone: _____

Fax: _____

Email: _____

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: _____

Date the Security Breach was discovered: _____

Estimated number of affected individuals: _____

Estimated number of NC residents affected: _____

Name of business or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b):

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: _____

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. _____ If so, please describe the security measures protecting the information: _____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: _____

Date affected NC residents were/will be notified: _____

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): _____

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?

(pursuant to N.C.G.S. § 75-65(e))

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

- written notice
- electronic notice (email)
- telephone notice
- substitute notice

Signature: _____ Date: _____

Contact Person, Title: _____

Address: _____

(if different from above) _____

Telephone: _____ Fax: _____ Email: _____