HITECH Act Breach Notification Risk Assessment Tool

NCHICA Privacy/Security Officers Workgroup

November 2009

The NCHICA Privacy and Security Officials Workgroup developed this Breach Notification Risk Assessment Tool in response to the DHHS Breach Notification for Unsecured Protected Health Information Interim Final Rule posted in the Federal Register on Monday August 24, 2009. A task force made up of Privacy and Security Officials from across North Carolina has worked since the rule was published to develop a collaborative risk assessment tool to be used by HIPAA "Covered Entities". The main objective of the tool is to provide "covered entities" a consistent approach in performing a risk assessment to determine if the breach notifications are required to be implemented as a result of a possible breach of unsecured Protected Health Information. In addition to the risk assessment, a flow chart has been included that addresses the requirements of both the NC Identity Theft Protection Act and the DHHS Breach Notification Interim Final Rule. This tool is for guidance and reference and should not be used in the place of sound legal advice.

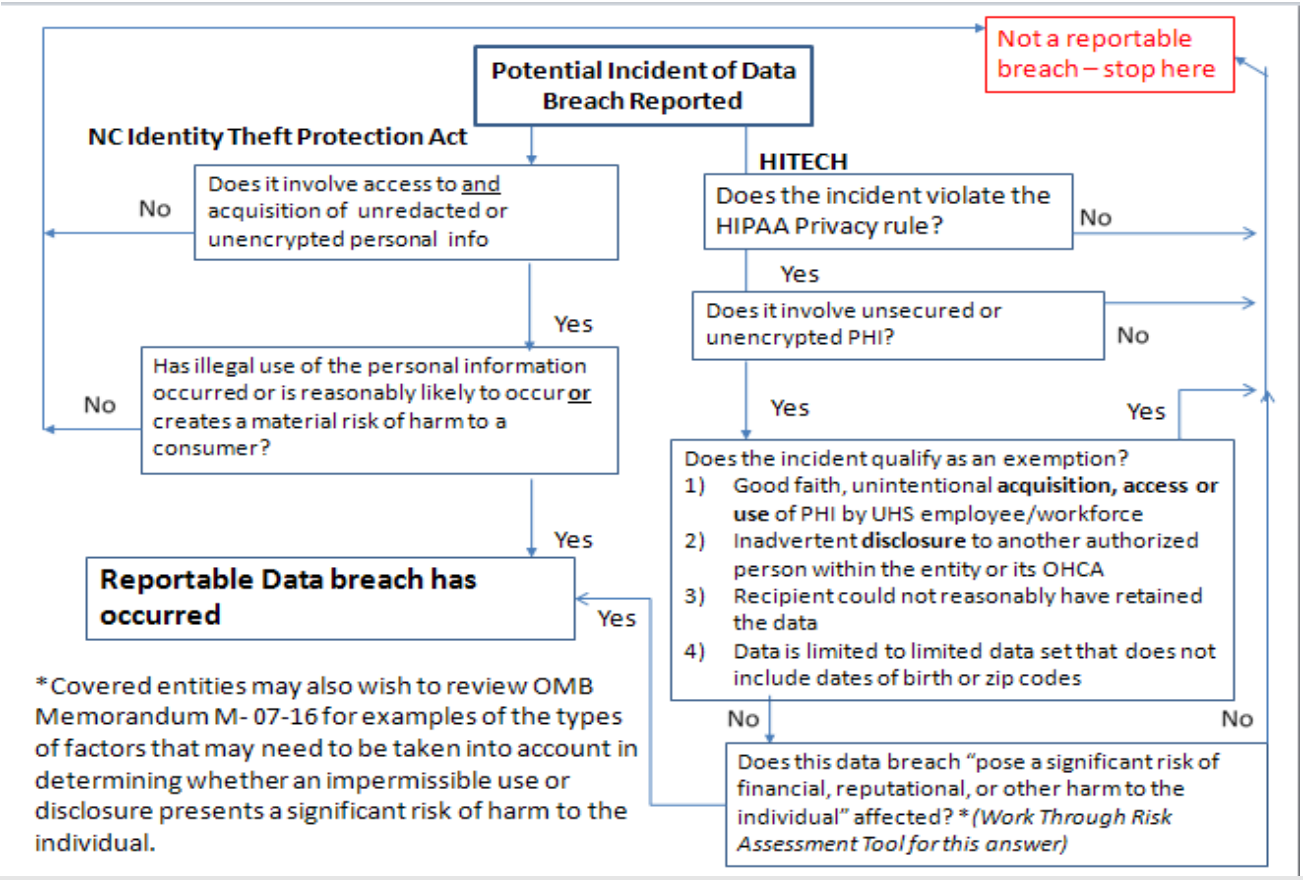
Summary of Breach Notification Rule

As required by the Privacy provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, under the American Recovery and Reinvestment Act of 2009 (ARRA), which was enacted on February 17, 2009, the Department of Health and Human Services (HHS) has issued interim final regulations for breach notification by covered entities subject to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates. These regulations require HIPAA covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information. In addition, in some cases the covered entity is required to provide notification to the media of breaches. In the case of a breach of unsecured protected health information (PHI) at or by a business associate of a covered entity, the business associate is required to notify the covered entity of the breach. Finally, it is required that the Secretary post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Risk Assessment Tool Introduction

The Breach Notification Interim Final Rule requires covered entities and business associates to perform and document risk assessments on breaches of unsecured protected health information (PHI) to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. If it is determined that the risk of harm to the individual is low, then the above notification requirements do not have to be completed. In performing the risk assessment covered entities and business associates may need to consider a number or combination of factors. The purpose of this Risk Assessment Tool is to provide some guidelines for covered entities in performing these risk assessments. As referenced in the rule, the OMB Memorandum M-07-16 is our guide for assessing the likely risk of harm to individuals affected by breaches of unsecured PHI.

The following decision tree can be utilized in instances of an incident that may require notification from the HITECH Breach Rule or the NC Identity Theft Protection Act.



NCHICA Breach Notification
Risk Assessment Tool

Incident/Name	**Date of event**
Number of individuals effected……	
Point of Contact	**Phone #**
Brief Summary/Findings	**Final Decision**

Source of Incident: Who was responsible for the inappropriate access, use or disclosure (incident)? *Circle your answer…* If Business Associate is the source of the incident, enter the date the Business Associate made us aware of incident.	Internal to our organization or Business Associate **Date:**
Are we the Business Associate? *Circle your answer…* If we are the Business Associate, enter the date we notified the other Covered Entity of the incident Enter the date that our organization became aware of the incident	**Yes / No** **Date:** **Date:**

_____
Section 164.404(a)(2) further provides that a covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

Additional information considered in your determination:

Analysis
Mitigation

--- Section 1 ---

1. Is there a HIPAA Security/Privacy Rule violation? ***If No, then STOP here. No breach has occurred that requires notification.*** ***If Yes, then proceed to next question.***	Y/N
2. Was data secured or properly destroyed in compliance with the requirements in the Breach Notification Rule? ***If Yes, then STOP here. No breach has occurred that requires notification.*** ***If No, then proceed to next question.***	Y/N
3. Does this incident qualify as one of the following exceptions? ***If Yes, then STOP here. No breach has occurred that requires notification.*** ***If No, then proceed to next section to work through the rest of the assessment to determine if the breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent that it would require notification.***	Y/N
Note: *The Examples below were taken directly from the Interim Final Rule. See* ***Addendum B*** *for complete regulation text of each exception listed below.*	
a. Good faith, unintentional acquisition, access or use of PHI by employee/workforce *Example- A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it.*	
b. Inadvertent disclosure to another authorized person within the entity or OHCA *Example- a physician who has authority to use or disclose protected health information at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital.*	
c. Recipient could not reasonably have retained the data *Example, a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information.*	
d. Data is limited to limited data set that does not include dates of birth or zip codes	

If you did not hit a STOP above in Section 1, then work through the rest of the assessment to determine if the *breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent that it would require notification.*

Go to Section 2

Circle **all that apply** in each subsection:

--- Section 2 --- NCHICA Breach Notification Risk Assessment Tool		
Variable	**Options**	**Score**
I. Method of Disclosure	• Verbal	1
	• Paper	2
	• Electronic	3
II. Recipient(s)	• Your Business Associate • Another Covered Entity • Internal Workforce	1
	• Wrong Payor (not the patient's) • Unauthorized family member • Non-covered entity	2
	• Media • Unknown/Lost/Stolen • Member of the general public	3
III. Circumstances of release	• Unintentional disclosure of PHI	1
	• Intentional use/access w/o auth • Intentional disclosure w/o auth • Theft – Device targeted • Lost	2
	• Using false pretense to obtain or disclose • Obtained for personal gain/malicious harm • Hack • Theft – data targeted	3
IV. Disposition (What happened to the information after the initial disclosure)	• Information returned complete • Information properly destroyed and attested to	1
	• Information properly destroyed (unattested) • Electronically Deleted (unsure of backup status)	2
	• Sent to the Media • Unable to retrieve • Unsure of disposition or location • High (suspicion of pending re-disclosure) • Extremely High (PHI already re-disclosed)	3
V. Additional Controls	• Data Wiped • Information/Device Encrypted, but does not meet compliance with NIST Standards • Information Destroyed, but does not meet compliance with NIST Standards	1
	• Password protected – password not compromised	2
	• Password protected – password was compromised • No Controls • Other _____	3
Section 2 - Total	***Add highest score from each subsection above and enter here…***	

Circle **ALL** that apply:

--- Section 3 ---

NCHICA Breach Notification Risk Assessment Tool

Below are general guidelines for ranking levels of risks for different types of information breached. ***The circumstances surrounding each breach may impact how you will rank the risk level for the data breached.*** *For example, if a file of known abuse victims is breached that includes the victims' addresses, then you will probably want to rank the breach of this data as a high probability of causing harm to the person(s) impacted by the breach. However, under other circumstances just the release of an address may be considered a low risk of harm to the person(s) impacted by the breach.*

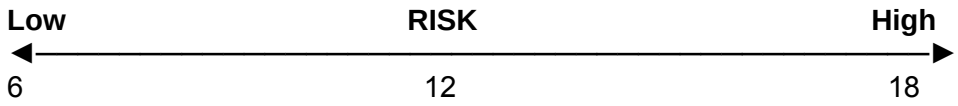
Variable	Options	Score
VI. Type of Information Breached	**Lowest Risk – Impacts Financial, Reputational & Other Harm** • Limited Data Set *(evaluate possibility of re-identification if ZIP Code and/or DOB included)* • Only identifiers are breached that are not defined under NC Identity Theft Protection Act and no other health information is breached: name, address, city, state, telephone number, fax number, e-mail address, admission/discharge dates, service dates, date of death	1
	Medium Risk – Impacts Financial, Reputational & Other Harm • Non-Sensitive Protected Health Information which may include information about treatment, [1]diagnosis, service, medication, etc… *(Evaluate closely the possibility of the information causing harm to the person(s) impacted by the breach, because the information breached may not typically fall under our definition of sensitive information, but looking at the circumstances it may still cause harm to the patient.)*	2
	Highest Risk • **Impacts Financial Harm** - Information defined by the NC Identity Theft Protection Act which includes the person's first name or first initial and last name in combination with any of the following: o Social security or employer taxpayer identification numbers o Drivers license, State identification card, or passport numbers o Checking account numbers o Savings account numbers o Credit card numbers o Debit card numbers o Personal Identification (PIN) Code as defined in G.S. 14-113.8(6) o Electronic identification numbers, electronic mail names or addresses (Non-State Agencies) o Internet account numbers, or Internet identification names o Digital signatures o Any other numbers or information that can be used to access a person's financial resources o Biometric data, fingerprints o Passwords o Parent's legal surname prior to marriage (Non-State Agencies) • **Impacts Reputational or Other Harm** - Sensitive Protected Health Information which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health.	3
Section 3 - Total	***Enter highest score selected above in Section 3 here…***	

[1] *Further, in the interim final rule at §164.404(c)(1)(B), we add the term "diagnosis" in the parenthetical listing of examples of types of protected health information to make clear that, where appropriate, a covered entity may need to indicate in the notification to the individual whether and what types of treatment information were involved in a breach.*

SCORING

The scoring is meant to serve as a guide in your decision making and not designed to make the decision for you. There are a variety of factors and mitigations that may be involved in your incident that this tool cannot foresee or predict. An attempt was made to develop this is a way that would help you in documenting your actions, consider factors and circumstances and then aid in your final decision of making a breach notification or not making a breach notification.

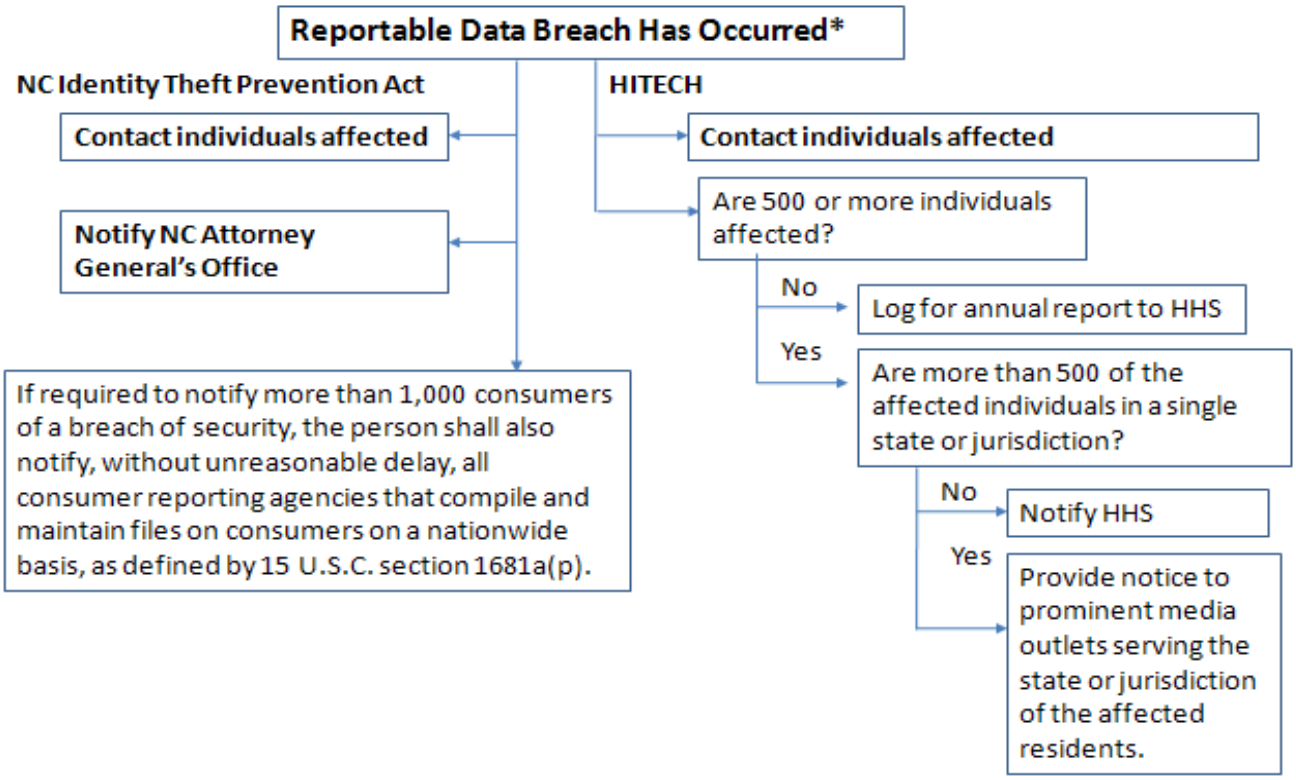
The range of scoring is 6 -18. A low score of 6 does not necessarily mean you should not take any action but a high score of or near 18 could indicate either a need to notify or a need to take further actions. The scoring was designed to be subjective so that each separate entity can consider their own policies, technical safeguards/constraints, mitigation strategies and details specific to the incident they are reviewing at the time.



Total Risk Score *(Section 2 + Section 3)*	

After completing the assessment and scoring your responses do you feel the disclosure compromises the Security and Privacy of the PHI **AND**
Poses a significant risk to the financial, reputational or other harm to the individual to the extent it would require a notification to the affected individuals?

Next Steps: **If you determined from this assessment that you should notify affected individuals of a breach then consider the steps in the continuation of the Flow Chart for both NC ITPA and HITECH on the next couple of pages…**



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

Contact individuals affected
(without unreasonable delay)

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 OR
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) **Substitute notice**, if the cost of providing notice would exceed $250,000, if the affected class of affected individuals exceeds 500,000, or for individuals with insufficient contact information
(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.

Addendum "A" NC ID Theft Protection Act

The North Carolina Identity Theft Protection Act
North Carolina passed the Identify Theft Protection Act of 2005 in December 2005. We included it in this assessment due to the fact that a breach could be covered and reportable under this statute in NC but not be reportable under the new HIPAA breach standards. By the same token a breach may be coved by both. It should be noted that the tool cannot score your risk independently. You need to keep the risk factors for each type of breach in proper context.

Although this act is focused on protecting financial information, it addresses the protection of personal information that can be used to gain access to that information. The parts of this legislation that have major impact are; Social Security Numbers (SSNs) may not be transmitted over Internet in unencrypted form; SSNs may not be used for authentication without other identifying information; SSNs may not be printed on any card or may not be printed on any material mailed to an individual unless specifically required by federal law; Individuals must be notified of security breaches when there's a reasonable likelihood that their "identifying information" was compromised; Identifying information covers a wide range of data, including SSNs, bank account numbers, driver's license numbers, biometric data (fingerprints), passwords, and parent's legal surname prior to marriage (often used by financial institutions as a form of authentication); A violation of this act can result in significant monetary damages, exposure of personal information that could result in damages to the individual, and security breaches that could tarnish the reputation of your agency.

Definitions from NC ITPA:

"Encryption" – The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

"Personal information" – A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). 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"*** – 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 [2]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.

[2] A potential decision point when trying to determine "reasonably likely to occur or that creates a material risk of harm." The HITECH portion of the risk assessment may be helpful in making this decision.

Addendum "B" HITECH Definitions (164.402)

"Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) **Breach excludes**:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (Example out of regulation: A staff person receives and opens an e-mail from a nurse containing protected health information about a patient that the nurse mistakenly sent to the staff person, realizes the e-mail is misdirected and then deletes it.)

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further, used or disclosed in a manner not permitted under subpart E of this part. (Example out of regulation: A nurse calls a doctor who provides medical information on a patient in response to the inquiry. It turns out the information was for the wrong patient. Such an event would not be considered a breach, provided the information received was not further used or disclosed in a manner not permitted by the Privacy Rule.)

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (Example out of regulation: A nurse hands a patient a medical report, but quickly realizes that it was someone else's report and requests the return of the incorrect report. In this case, if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then providing the patient report to the wrong patient does not constitute a breach.)

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS Web site.

Addendum "C" OMB Memorandum M07-16

	The regulation suggests you 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. We have used this as a guide and referenced the location of each one of the concepts in the assessment.	
	OMB Memorandum M07-16 Information/Questions	**Location in Assessment**
	Five factors should be considered to assess the likely risk of harm: • Nature of the Data Elements Breached.	Section 3 - "Type of Information"
	• Number of Individuals Affected.	Header - Number of Individuals Affected
	• Likelihood the Information is Accessible and Usable.	Section 2 - "Methods, Circumstances, Recipient and Disposition"
	• Likelihood the Breach May Lead to Harm o 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. o 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.	"Harm" and "Likelihood of Harm" will be determined by each agencies scoring of each risk, the results of their risk assessment and their response/ mitigation plans
	• Ability of the Agency to Mitigate the Risk of Harm.	Section 2 - "Additional Controls"