INTEGRATED SERVICES OF KALAMAZOO

ADMINISTRATIVE PROCEDURE 10.08_01

Subject: Breach Notification	**Section:** Compliance & Risk Management	
Applies To: ☒ ISK Staff ☒ ISK Contract Providers		**Page:** 1 of 7
Revised: 11/19/2018	**Supersedes:**	

PURPOSE

The purpose of this policy is to provide guidance to Integrated Services of Kalamazoo (ISK) staff and contractors when there is a breach.

ISK will maintain a Protected Health Information Integrity Team (PHIIT) that will meet on a periodic basis, as defined by its members, to respond to suspected or confirmed breaches of protected health information (PHI). PHIIT members are comprised of ISK Privacy Officer, Corporate Compliance Officer, Office of Recipient Rights Director, Chief Information Officer, Health Information Manager, Quality Program Coordinator and the Compliance & Quality Improvement Coordinator. PHIIT conducts Risk Assessment to determine whether an unauthorized disclosure of PHI occurred, the level of probability that the PHI in question was compromised, and whether notification under the Breach Notification Rule is required.

The secondary purpose of this policy is to provide guidance to ISK staff and Contract Providers when there is a security breach involving information concerning individuals other than consumers consistent with the notice of security breach requirements as stated in Act 452 of 2004, the Michigan Identity Theft Protection Act.

DEFINITIONS

Breach

A breach is an acquisition, access, use or disclosure of ISK' consumers' unsecured protected health information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing rules and regulations, which compromises the security or privacy of Protected Health Information (PHI).

Protected Health Information (PHI)

1. Any information that is transmitted by electronic media, maintained in electronic media or transmitted, recorded or maintained in any other form or medium that; Is created or received by ISK.

2. Relates to the past, present or future physical or mental health condition of an individual; or the past, present, or future payment for the provision of health care to an individual.
3. Identifies the individual, or with respect to which there is reasonable basis to believe the health information can be used to identify the individual.

Unsecured Protected Health Information (Unsecured PHI)
Any PHI which is not rendered unusable, unreadable or indecipherable to unauthorized persons using technology or methodology, such as encryption or destruction, as specified by the HHS Secretary (HHS.gov).

Covered Entity
A Covered Entity is one of the following:

1. Health Plan
   This includes Health Insurance Companies, HMOs, Company Health Plans, Government programs that pays the cost of medical care (e.g., Medicare, Medicaid, military or veteran health care programs) and self- funded plans
2. Health Care Provider
   A provider of medical or health services (such as Skilled Nursing Facilities, home health, hospitals, physicians, clinics, pharmacies, etc.) that transmits any health information in electronic form
3. Health Care Clearinghouse
   This includes entities that process nonstandard health information they receive from another entity into a standard (i.e. standard electronic format or data content), or vice versa)

Workforce
ISK employees, volunteers, trainees, business associates, contract providers and vendors that could reasonably be exposed to PHI, whether they are paid or not.

PROCEDURE

I. DISCOVERY OF BREACH

A. A breach shall be treated as discovered as of the first day on which such breach is known by exercising reasonable diligence or would have been known to ISK or any person, other than the person committing the breach, who is a workforce member or agent of ISK.

B. Workforce members who believe that PHI has been used or disclosed in any way that compromises the security or privacy of that information shall notify ISK Privacy Officer or any member of ISK PHIIT, or on an ad hoc basis ISK Legal Counsel, immediately or no later than 5 business days. In case of a breach of unsecured PHI affecting 500 or more of ISK' consumers, ISK Chief Executive Officer (CEO) must also be immediately notified. An incident report must be completed and submitted to ISK Office of Recipient Rights and should include a plan of correction to address the breach. If a plan of correction is not submitted, a member of the PHI Integrity Team will contact the workforce member. Refer to Section VI of this policy for additional ISK notification requirements.

C. Following the discovery of a potential breach, PHIIT shall conduct a risk assessment of the incident and upon completion must address whether to begin the process of notifying each individual whose PHI has been or is reasonably believed by ISK to have been accessed, acquired, used or disclosed as a result of the breach. ISK shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of DHHS, media outlets or law enforcement officials. Conclusion of risk assessment will be relayed by ISK Privacy Officer or a member of PHIIT to the workforce member involved in the PHI breach in cases where breach notification letter has to be sent and HHS reporting must be completed.

II. RISK ASSESSMENT

A. ISK PHIIT will first substantiate that the incident reported was in fact a violation of the HIPAA Privacy Rule by reviewing the facts of the incident and analyzing the findings against the requirements of the rules.

B. A breach is presumed to have occurred unless ISK can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
   - i. Social security numbers, credit cards, financial data.
   - ii. Clinical detail, diagnosis, treatment, medications.
   - iii. Mental health, substance abuse, sexually transmitted diseases, pregnancy.
2. The unauthorized person who used the PHI or to whom the disclosure was made.
3. Whether the PHI was acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.
5. The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be completed in good faith and the conclusions should be reasonable.

C. Risk Assessment will also determine whether violation fits into one of three exceptions to a breach. The three regulatory exceptions to a breach are:

1. Unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of ISK if such acquisition, access or use was in good faith and in the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
2. Inadvertent disclosure of PHI from a person who is authorized to access

PHI at ISK or its workforce member to another person authorized to access PHI at the same CE, BA or organized health care arrangement in which ISK participates, and the information received as a result if such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

3. Good faith belief by ISK that the unauthorized person to whom disclosure was made would not reasonably have been able to retain such information.

D. Based on the outcome of a risk assessment, ISK PHIIT will determine if there’s a need to move forward with the breach notification. ISK and its workforce, where applicable, has discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

III. NOTIFICATION OF INDIVIDUALS AFFECTED

A. If it is determined that breach notification must be sent to affected individuals, ISK standard breach notification letter (as modified for the specific breach) will be sent out to all affected individuals. Notice to affected individuals shall be written in plain language and must contain the following information, which elements are included in ISK’ standard breach notification letter:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what ISK is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

B. This letter will be sent by first-class mail to the individual at the last known address of the individual. The notification shall be provided in one or more mailings as information is available. If ISK or its workforce knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out.

C. If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided.

1. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means.
2. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of ISK or its workforce' website, or a conspicuous notice in major print or broadcast media in ISK' geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

D. Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If ISK determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. It is the responsibility of ISK and its workforce to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

IV. NOTIFICATION TO DEPARTMENT OF HEALTH AND HUMAN SERVICES

In the event a breach of unsecured PHI affects 500 or more of ISK' consumers, the Secretary of DHHS must be notified at the same time notice is made to the affected individuals in the matter specified on the DHHS website. If fewer than 500 of ISK' consumers are affected and workforce member is required to complete HHS reporting basing on the result of PHIIT Risk Assessment, proof of submission must be submitted to ISK Privacy Officer upon completion. ISK will maintain a log of the breaches submitted to the Secretary of DHHS. All submission must be completed no later than 60 days after the end of each calendar year in the manner specified on the DHHS website. The submission shall include all breaches discovered during the preceding calendar year.

V. NOTIFICATION TO MEDIA

In the event the breach affects more than 500 residents of a state, ISK CEO must be notified prior to breach media notification. Prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.

VI. NOTIFICATION TO KALAMAZOO COMMUNITY MENTAL HEALTH AND SUBSTANCE ABUSE SERVICES (The Covered Entity)

In addition to the procedure upon discover of breach noted in Section I, refer to Business Associate Agreement (BAA) entered with ISK for additional information regarding obligations of business associate and covered entity in compliance with HIPAA, HITECH, the Privacy Rule, Security Rule, and the Breach Notification Rule. Timelines for breach reporting to ISK may considerably be shorter than what is required by federal law.

VII. DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES

A. If a law enforcement official states to ISK or a business associate that a notification, notice or posting would impede a criminal investigation or cause damage to national security, ISK shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

B. This applies to notices made to individuals, the media, DHHS and by business associates.

VIII. MAINTENANCE OF BREACH INFORMATION

ISK shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of consumers affected. The following information should be collected for each breach:

A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).

C. A description of the action taken about notification of patients regarding the breach.

D. Steps taken to mitigate the breach and prevent future occurrences.

IX. WORKFORCE TRAINING

ISK and its workforce shall ensure that members are adequately trained in Privacy and Security standards and measures.

X. COMPLAINTS

ISK provides a process for individuals to make complaints concerning ISK's privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about ISK' breach notification processes.

XI. SANCTIONS

Members of ISK' workforce who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

XII. RETALIATION / WAIVER

ISK may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

XIII. BURDEN OF PROOF

ISK and its Business Associates has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Business Associate Agreements are in place to ensure that business associates appropriately safeguard protected health information and use and disclose the information only as permitted or required by the Privacy Rule.

REFERENCES

A. Health Insurance Portability and Accountability Act of 1996

B. HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

C. Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009

D. Act 452 of 2004, Identity Theft Protection Act

E. Michigan Social Security Number Privacy Act (Act 454 of 2004)

EXHIBITS

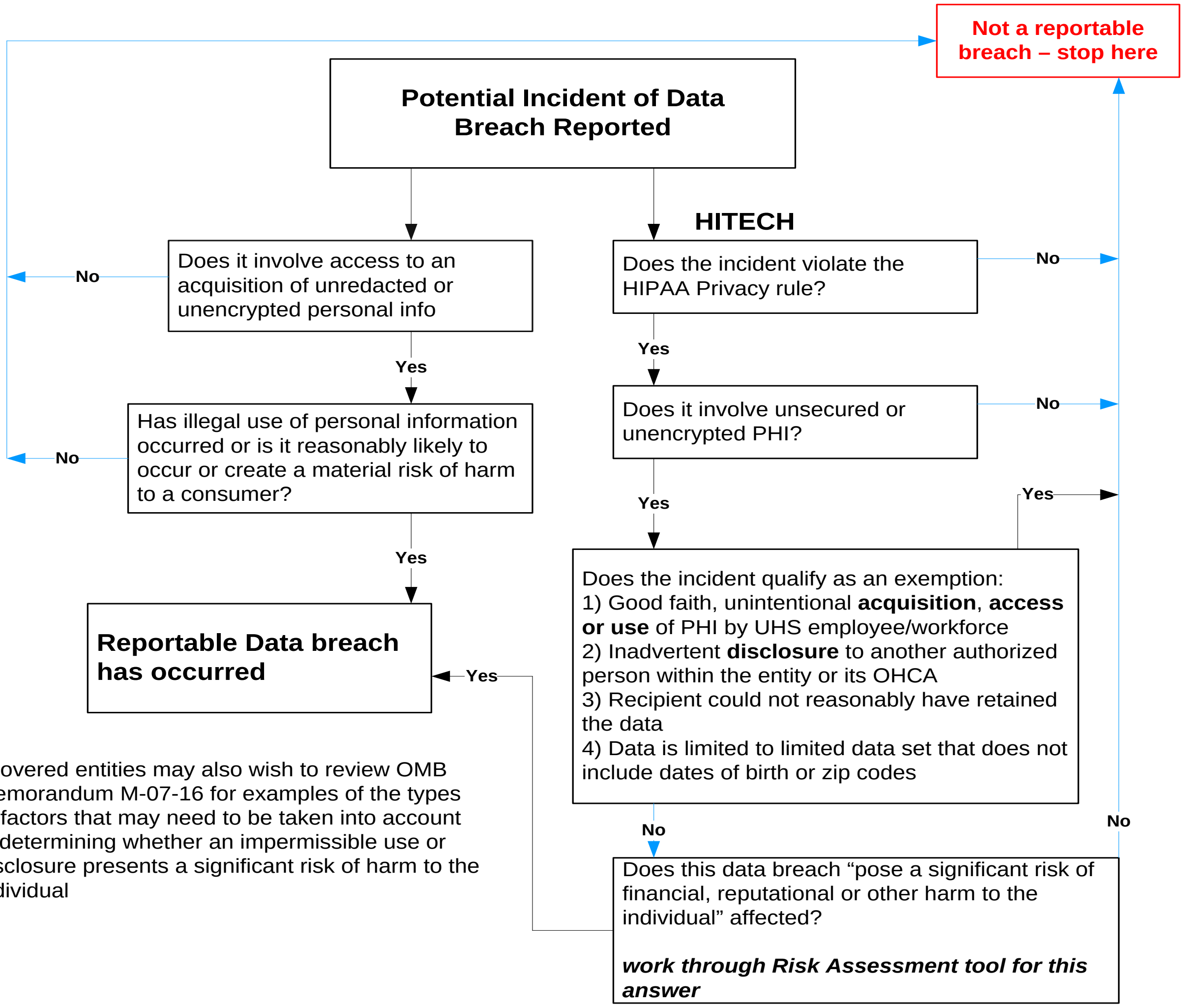
A. Breach Notification Risk Assessment Guide and Tool

Integrated Services of Kalamazoo

HITECH ACT
BREACH NOTIFICATION RISK ASSESSMENT GUIDE

RISK ASSESSMENT 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. The following decision tree can be utilized in instances of an incident that may require notification from the HITECH Breach Rule.


Not a reportable breach – stop here
Potential Incident of Data Breach Reported
HITECH
Does it involve access to an acquisition of unredacted or unencrypted personal info
No
Yes
Has illegal use of personal information occurred or is it reasonably likely to occur or create a material risk of harm to a consumer?
No
Yes
Reportable Data breach has occurred
Does the incident violate the HIPAA Privacy rule?
No
Yes
Does it involve unsecured or unencrypted PHI?
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
Yes
No
Does this data breach "pose a significant risk of financial, reputational or other harm to the individual" affected?
work through Risk Assessment tool for this answer
No
Yes

*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

Breach Notification / Risk Assessment

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…*	Internal to our organization or Business Associate
If Business Associate is the source of the incident, enter the date the Business Associate made us aware of incident.	**Date:**
Are we the Business Associate? *Circle your answer…*	□ **Yes** □ **No**
If we are the Business Associate, enter the date we notified the other Covered Entity of the incident	**Date:**
Enter the date that our organization became aware of the incident	**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.***	□ **Yes** □ **No**
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.***	□ **Yes** □ **No**
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.***	□ **Yes** □ **No**

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

CHECK ALL THAT APPLY IN EACH SUBSECTION:

SECTION 2

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…***	

CHECK ALL THAT APPLY IN EACH SUBSECTION

SECTION 3

*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. 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 includes the person's first name or first initial and last name in combination with any of the following: ~ 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 (Non-State Agencies) ~ 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 (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	***Add highest score from each subsection above and enter here…***	

SCORING

[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.*

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 the risk assessment tool cannot foresee or predict. An attempt was made to develop this in a way that would help you in documenting your actions, considering 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.

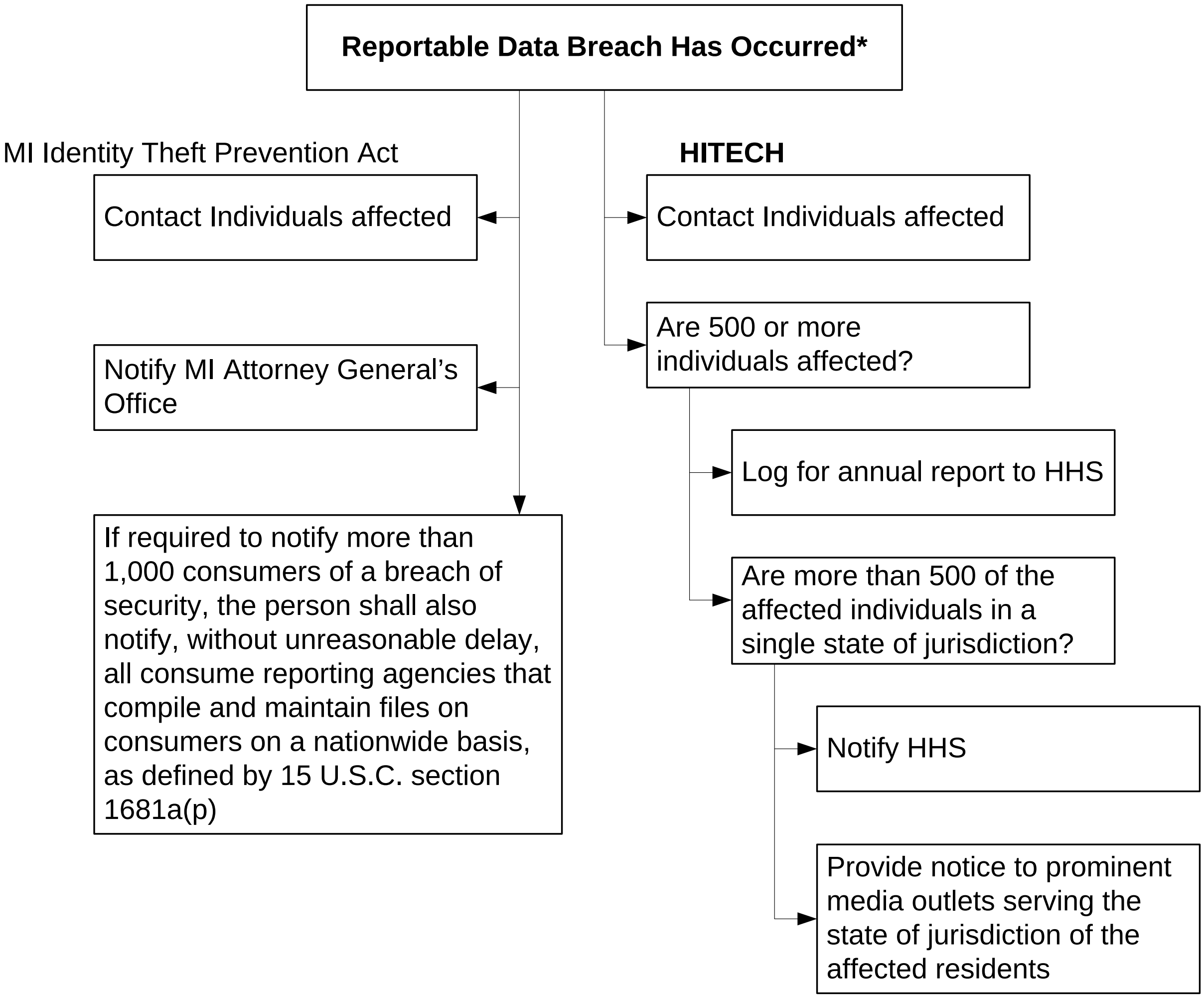
Low	**RISK**	**High**
◄		►
6	**12**	**18**

Total Risk Score (section 2 + section 3) □

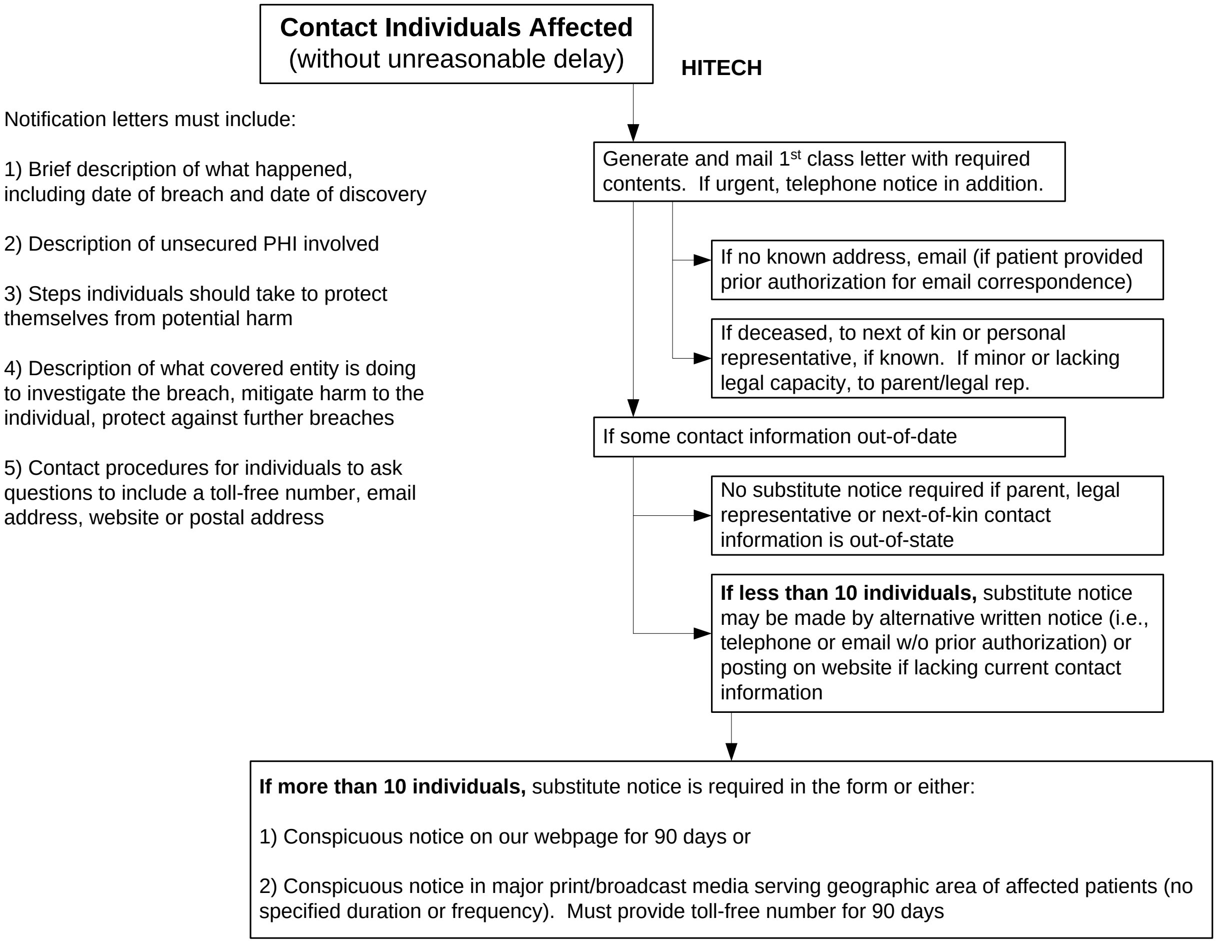
After completing the assessment and scoring your responses do you feel the disclosure compromises the Security and Privacy of the PHI **and** poses a significant risk to the financial, reputational or other harm to the individual to the extent it would require a notification to the affected individuals?

Next Steps

If you determined from this assessment that you should notify affected individuals of a breach, consider the steps in the continuation of the Flow Chart.


Reportable Data Breach Has Occurred*
MI Identity Theft Prevention Act
HITECH
Contact Individuals affected
Contact Individuals affected
Are 500 or more individuals affected?
Notify MI Attorney General's Office
Log for annual report to HHS
If required to notify more than 1,000 consumers of a breach of security, the person shall also notify, without unreasonable delay, all consume reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p)
Are more than 500 of the affected individuals in a single state of jurisdiction?
Notify HHS
Provide notice to prominent media outlets serving the state of jurisdiction of the affected residents

*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

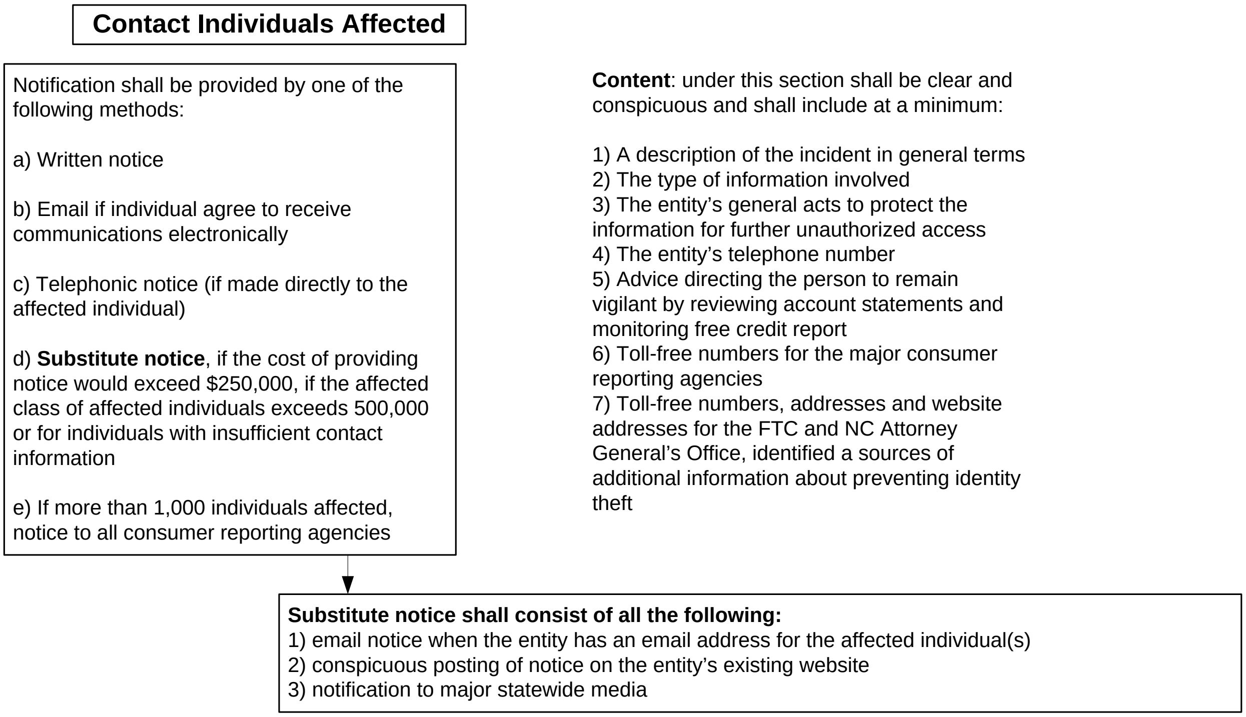
No substitute notice required if parent, legal representative or next-of-kin contact information is out-of-state

If less than 10 individuals, substitute notice may be made by alternative written notice (i.e., 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 or 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

Notification shall be provided by one of the following methods:

a) Written notice

b) Email if individual agree 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

Content: 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 for 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, addresses and website addresses for the FTC and NC Attorney General's Office, identified a sources of additional information about preventing identity theft

Substitute notice shall consist of all the following:
1) email notice when the entity has an email address for the affected individual(s)
2) conspicuous posting of notice on the entity's existing website
3) notification to major statewide media

DEFINITIONS

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 "A" 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 “B” 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 agency’s 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”