Breach Risk Assessment Tool

Date:

Core Members	Absent	Reportable	Not Reportable
Ad hoc Members			

Notification not required

Notification required

- Affected individual(s)
- State Attorney General
- Credit Bureaus
- Media
- Website
- Substitute Notice
- Secretary, US Dept. Health & Human Services

Police Report

Credit Monitoring Services

Other

- Vendor (Call center, web hosting, etc.)

Purpose: To determine if a substantiated breach presents a compromise to the security and/or privacy of the PHI ***and*** poses a significant risk to the financial, reputational or other harm to the individual or entity, to the extent it would require notification to the affected individual(s).

***NOTE:* Any external disclosures to a non-covered entity containing a person's first name or first initial and last name in combination with the person's social security number are automatically considered as reportable security breaches.**

Department:	Completed By:
Date of Event:	Date Completed:
Date Reported:	
Date Investigation Completed:	
Brief Summary of the Issue:	
Number of individuals affected:	

	YES	NO	
Is there a HIPAA Security/Privacy Rule violation?			**If both "No", STOP HERE**
Is there a State data breach violation?			
Was data encrypted, secured or properly destroyed?			**If "Yes", STOP HERE** *No reportable breach occurred.*

Business Associate (BA) – Source of Disclosure	YES	NO
Was the Breach committed by a BA of the organization?		
Was the Breach committed by the organization as a BA?		
Date Covered Entity was made aware of the Breach?		

SECTION 1 - For each of the Following Items, Select the Best response

Method of Disclosure

Type	Level
Unauthorized internal acquisition, access or internal use/disclosure	0
Verbal disclosure	1
View only	1
Paper	2
Electronic	3
Both paper and electronic	3

Method of Disclosure Score _____

Recipient

Type	Level
Business Associate of the Organization	1
Another Covered Entity	1
Internal Workforce Member	1
Wrong Payor/Insurance Company	2
Unauthorized family member or other patient	2
Unknown Recipient – Information lost or stolen	3
A company (non-covered entity), member of general public, media, etc.	3

Recipient Score _____

Circumstances of Release

Type	Level
Unintentional Disclosure	1
Intentional use/access without authorization	2
Intentional disclosure without authorization	2
Loss or Theft	2
Using false pretense to obtain or disclose	3
Obtain for personal gain or with malicious intent to cause harm	3
Hacked or targeted data theft	3

Circumstance of Release Score _____

Disposition of Information

Type	Level
Original, complete information returned	1
Information properly destroyed (Written attestation/assurance obtained)	1
Information could NOT be reasonably retained	1
Information properly destroyed (No attestation/assurance obtained)	2
Electronically deleted	2
Disclosed to Media	3
Unable to retrieve or unsure of location/disposition	3
High probability of re-disclosure or suspected re-disclosure	3

Disposition of Information Score _____

Additional Controls

Type	Level
Data Wiped	1
Encrypted/Destroyed – Non-NIST compliant	1
Physical/Policy Controls	1
Password Compliant (not compromised)	2
Password Protected (compromised)	3
No Controls/Unencrypted	3
Other – Explain below	3

Additional Controls Score _____

Add the score from each section: TOTAL SCORE: _____

Continue to SECTION 2

SECTION 2 – Please choose one of the following below.

Below are general guidelines for ranking levels of risks for different types of information breached. ***The circumstances surrounding the breach may impact the risk level ranking associate with the data breached.*** *For example, if a file of known abuse victims is breached and it includes the victims' addresses, then you will likely rank the breach of such data as a high probability of risk and potential harm to the person(s) impacted by the breach. However, under other circumstances if the information breached included name and address and was not associated with "abuse victims," it may warrant a lower risk threshold.*

Type of Information Breached – Risk Threshold

Type of Risk	Category & Description of Information	Level
Low	Other • Limited Data Set (evaluate possibility of re-identification of de-identified information if Zip Code and/or Date of Birth included) **AND** • The ONLY identifiers included are NOT defined under Florida Information Protection Act (FIPA) and NO other health information is included (i.e. Demographic information including: Name, Full Address, Telephone number, Email address, Admission/Discharge or Dates of Service, Diagnosis or Treatment information)	1
Medium	Non-Sensitive – Demographic information with no financial or sensitive treatment related information. Such information may include date of service, facility or provider name, etc.	2
High	An individual's first name or first initial and last name in combination with any one or more (SCORE 4 if more than ONE) of the following data elements of the individual: • Social Security Number • Driver's license or State Identification card number, passport number, military identification number, or other similar number issued on a government document that may be used to verify identity. • Financial account number or debit/credit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account • Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional • An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual • A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account	3
Highest	An individual's first name or first initial and last name in combination with • Sensitive Protected Health Information such as information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health. • More than one "high risk" combination	2
Total Section 2	ENTER HIGHEST SCORE FROM ABOVE	

Section 2 continued on next page

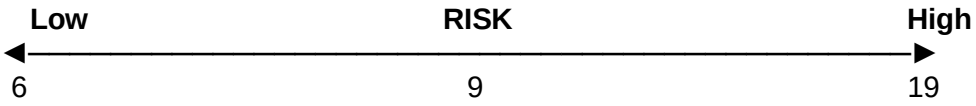
SECTION 2 Continued

Escalators and Minimizers

Escalator (+ 5)	Believable threat of reporting to patient/regulatory body – asserted.	
Minimizer (-5)	Self-reported, no indication of further reporting/disclosure.	

The range of 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 take place in your incident that this tool cannot foresee or predict.

The range of scoring is 6 - 19. A low score of 6 does not necessarily trigger notice obligations but a high score of or near 19 would likely indicate either a need to notify or a need to take other actions.



Enter Combined Risk Score: Sections One and Two plus/minus Escalators and Minimizers	

Comments/Mitigation - Additional information considered

SECTION 3 – Please Choose Y or N to answer the following questions.

Does this incident qualify as an exception?	**Y/N**
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.*	
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.*	
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.*	
Data is limited to limited data set that does not include dates of birth or zip codes	

If “Yes” is selected as an answer to one or more of the above questions, continue to Section Four (Notification is NOT required under HIPAA)

If “No” is selected as an answer to ALL of the above, Notification may be required under HIPAA. (Continue to Section Four).

SECTION 4 – Please Choose Y or N to answer the following questions.

FLORIDA INFORMATION PROTECTION ACT (FIPA)

"Personal information"	Y/N
Did the information include an individual's first name or first initial and last name in combination with any one or more of the following data elements of the individual (a) Social Security Number (b) Driver's license or State Identification card number, passport number, military identification number, or other similar number issued on a government document that may be used to verify identity. (c) Financial account number or debit/credit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account (d) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional (e) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual (f) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account	

IF NO, Stop here!

Was the information illegally used *or* is reasonably likely to be used illegally? (Yes/No)	
Is the disclosure reasonably likely to create a material risk of harm to a consumer to the extent it would require notification to the affected individual? (Yes/No) ***NOTE:* Any unencrypted electronic data sent over the internet which contains a person's first name or first initial and last name in combination with the person's social security number is automatically considered a reportable security breach.**	

IF NO, to both of the above, STOP here!

IF YES, to one or both of the above, NOTIFICATION IS REQUIRED under the FLORIDA INFORMATION PROTECTION ACT