McLaren Health Care
Business Associate Breach Notification Risk Assessment Tool

Incident/Name	**Date of Discovery:**
Number of individuals effected by the breach and/or security incident (please attach a list to identify the individuals):	**Email Address of Reporter:**
Incident Reported By (Name/Title):	**Phone # of Reporter:**

Type of Incident: Please specify the type of privacy and/or security incident that occurred and details of the PHI involved below.	**Check all that apply:** ☐ **Inappropriate Access of PHI** ☐ **Inappropriate Disclosure of PHI** ☐ **Inappropriate Use of PHI**
Source of Incident: Who was responsible for the inappropriate access, use or disclosure?	☐ **Business Associate Workforce Member** ☐ **Business Associate Subcontractor** ☐ **Other Unauthorized User (ex: theft, hacker)**
Notification by Business Associate or Business Associate Subcontractor (Business Associate made us aware of incident) • Who is the BA/Contractor? • Is there an executed agreement in place with the BA/Contractor that includes HIPAA provisions (such as a Business Associate Agreement)? • When did the BA/Contractor notify the McLaren of the incident? • How was the McLaren notified of the incident?	**BA Contact Name:** **Contact Email:** **Contact Phone:** **Date BA Notified MHC:** **Date BA Discovered Incident:**

McLaren Health Care
Business Associate Breach Notification Risk Assessment Tool

--- Section 1 ---	
[Section Removed]	
1. **Was data properly secured (e.g., encrypted, or secured as specified in NIST guidance) or properly destroyed (shredded) 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**
2. **Does this incident qualify as one of the following exceptions? Check any that apply.** a. **Good faith, unintentional acquisition, access or use of PHI by Workforce Member** b. **Inadvertent disclosure to another authorized person within the entity or OHCA** c. **Recipient could not reasonably have retained the data** ***If any checked, then STOP here. No breach has occurred that requires notification.*** ***If none apply, proceed to next section to continue the assessment and determine if the breach poses more than a low probability of data compromise, to the extent that it would require breach notification.***	□ □ □

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 more than a low probability of data compromise to the extent that it would require breach notification.*

Go to Section 2

Check **all that apply** in each subsection and use highest applicable score:

--- Section 2 ---		
Variable	**Options**	**Score**
I. Method of Disclosure	□ No evidence that data was accessed or disclosed □ Attestation received that information was not further used or disclosed	**0**
	□ Unauthorized internal acquisition, access and/or use without disclosure outside of organization	**1**
	□ Verbal Disclosure □ View only	**2**
	□ Paper / Fax □ Electronic (email, mobile media, archive media, PC, server, etc.)	**3**
II. Amount of Data	□ No data accessed or disclosed	**0**
	□ Small amount – e.g., demographic information; limited data set; 1-10 individuals	**1**
	□ Moderate volume – 11-100; portions of records; a bill or EOB with coded information	**2**
	□ Large volume – over 100; unknown volume; archive or mobile media or device compromised; entire record, database with multiple fields of data	**3**

McLaren Health Care

Business Associate Breach Notification Risk Assessment Tool

--- Section 2 ---

Variable	Options	Score
III. Nature and Extent of PHI Involved	□ **No Data Acquired or Viewed**	**0**
	□ **Limited or Demographic Data Only** Limited Data Set *(evaluate possibility of re-identification if ZIP Code and/or DOB included)* Only identifiers breached are not defined under MI 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**
	□ **General PHI** Information about treatment, diagnosis, service, medication, etc.	**2**
	□ **Financial Data and/or Personal Identifiers** • Information defined by the MI Identity Theft Protection Act which 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 • Driver's 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) • Any other numbers or information that can be used to access a person's financial resources • Passwords-if the information would provide access to financial information or resources • Sensitive Protected Health Information which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health	**3**
	Specify the Type(s) of Information Accessed or Disclosed:	

--- Section 2 ---

Variable	Options	Score
IV. Who Received or Accessed the PHI	□ Not applicable	**0**
	□ A member of MHC Workforce □ Business Associate/Business Associate subcontractor □ Business Associate/Subcontractor Workforce □ Another Covered Entity	**1**
	□ Wrong Payor (not the patient's) □ Unauthorized family member □ Non-healthcare organization □ Government agency	**2**
	□ Media □ Unknown/Lost/Stolen □ Member of the general public	**3**
V. Circumstances of release	□ Unintentional access to or disclosure of PHI	**1**
	□ Lost or unable to determine whether compromise was likely	**2**
	□ Intentional disclosure w/o authorization □ Intentional acquisition/use/access w/o authorization using false pretense to obtain or disclose □ Obtained for personal gain/malicious harm □ Hack □ Theft – Device targeted or Data targeted	**3**
VI. Disposition/ Mitigation (What happened to the information after the initial disclosure)	□ Visual- viewed only with no further disclosure □ Information returned complete □ Information properly destroyed and attested to by workforce member, another covered entity or business associate □ Data Wiped by remote application □ Forensic analysis found no information accessed	**1**
	□ Information properly destroyed (outside organization/individual) □ Information/Device is encrypted or protected with proprietary software, but does not meet compliance with NIST Standards □ Information Destroyed, but does not meet compliance with NIST Standards □ Password protected – password not compromised or unknown if password compromised	**2**
	□ Password protected – password was compromised □ Data not encrypted, readable, but archived in a block format in no relational order. Password and proprietary system NOT required to view data. □ No known controls □ Unable to mitigate □ Unable to retrieve data □ Unsure of disposition or location □ Suspicion of pending re-disclosure □ PHI already re-disclosed	**3**

	□ Sent to the Media	

SCORING

Total Probability of Compromise Score *(Section 2)*	

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.

Probability of Compromise

Low ◀――――――――――――――――――▶ **High**

0 9 18

Additional information and basis for decision:	**Final Decision**	
	Low Probability of Compromise	□
	Breach Requiring Notice	□

Resolution and Corrective Action(s) (actions taken to prevent recurrence, responsible individual(s), and target dates for completion):

□ Corrected system issues (e.g., disabled auto-faxing, updated system with correct information, etc.)
□ Reviewed user security access levels for appropriateness and identified required changes
□ Changed or updated policies/procedures
□ Discussed results with leader(s) and identified changes to improve process or prevent reoccurrence
□ Counseled/educated to person or staff members to assure they understand what they did was wrong
□ Retrieved PHI or documented recipient's assurances that PHI was destroyed or not further disclosed

Document in detail all the above corrective actions in ComplyTrack.

Complete this section if breach notification is required:
Date of Notice to Individual(s):
Credit monitoring offered to individual:
Date of Notice to Secretary HHS:

____ ____________________
Individual completing Risk Assessment **Date**