

# McLaren Health Care

## Breach Notification Risk Assessment Tool

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

<b>Type of Incident:</b> Please specify the type of privacy and/or security incident that occurred and details of the PHI involved below.	<b>Check all that apply:</b> <input type="checkbox"/> Inappropriate Access of PHI  <input type="checkbox"/> Inappropriate Disclosure of PHI  <input type="checkbox"/> Inappropriate Use of PHI
<b>Source of Incident:</b> Who was responsible for the inappropriate access, use or disclosure?	<input type="checkbox"/> Workforce Member  <input type="checkbox"/> Business Associate  <input type="checkbox"/> Business Associate Subcontractor  <input type="checkbox"/> Other Authorized User  <input type="checkbox"/> Other Unauthorized User (ex: theft, hacker)
<b>Notification by Business Associate or Business Associate Subcontractor</b> (Business Associate made us aware of incident) <ul style="list-style-type: none"> <li>Who is the BA/Contractor?</li> <li>Is there an executed agreement in place with the BA/Contractor that includes HIPAA provisions (such as a Business Associate Agreement)?</li> <li>When did the BA/Contractor notify the McLaren of the incident?</li> <li>How was the McLaren notified of the incident?</li> </ul>	<b>BA Contact Name:</b>  <b>Contact Email:</b>  <b>Contact Phone:</b>  <b>Date Notified by BA:</b>  <b>Date BA Discovered:</b>
<b>Are we the Business Associate?</b>  Enter the date that our organization became aware of the incident  If we are the Business Associate, enter the date we notified the other Covered Entity of the incident	<input type="checkbox"/> Yes  <input type="checkbox"/> Not Applicable  <b>Date of Discovery:</b>  <b>Date Covered Entity Notified:</b>

# McLaren Health Care

## Breach Notification Risk Assessment Tool

### --- Section 1 ---

<p><b>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? OR Was the use/disclosure 'incidental to' a permitted disclosure (limited in scope and cannot reasonably be prevented)?</b></p> <p><i>If Yes, then <b>STOP</b> here. No breach has occurred that requires notification.</i>  <i>If No, then proceed to next question.</i></p>	<input type="checkbox"/> YES  <input type="checkbox"/> NO
<p><b>2. Does this incident qualify as one of the following exceptions? Check any that apply.</b></p> <ul style="list-style-type: none"> <li>a. Good faith, unintentional acquisition/access/use/disclosure of PHI by a Workforce Member</li> <li>b. Inadvertent disclosure to another authorized person within the entity or OHCA</li> <li>c. Recipient could not reasonably have retained the data</li> </ul> <p><i>If any checked, then <b>STOP</b> here. No breach has occurred that requires notification.</i>  <i>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.</i></p>	<input type="checkbox"/>  <input type="checkbox"/>  <input type="checkbox"/>

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
<b>I. Method of Disclosure</b>	<input type="checkbox"/> No evidence that data was accessed or disclosed	<b>0</b>
	<input type="checkbox"/> Unauthorized internal acquisition, access and/or use without disclosure outside of organization	<b>1</b>
	<input type="checkbox"/> Verbal Disclosure <input type="checkbox"/> View only	<b>2</b>
	<input type="checkbox"/> Paper / Fax <input type="checkbox"/> Electronic (email, mobile media, archive media, PC, server, etc.)	<b>3</b>
<b>II. Amount of Data</b>	<input type="checkbox"/> No data accessed or disclosed	<b>0</b>
	<input type="checkbox"/> Small amount – e.g., demographic information; limited data set; 1-10 individuals	<b>1</b>
	<input type="checkbox"/> Moderate volume – 11-100; portions of records; a bill or EOB with coded information	<b>2</b>
	<input type="checkbox"/> Large volume – over 100; unknown volume; archive or mobile media or device compromised; entire record, database with multiple fields of data	<b>3</b>

# McLaren Health Care

## Breach Notification Risk Assessment Tool

--- Section 2 ---		
Variable	Options	Score
<b>III. Nature and Extent of PHI Involved</b>	<input type="checkbox"/> <b>No Data Acquired or Viewed</b>	<b>0</b>
	<input type="checkbox"/> <b>Limited or Demographic Data Only</b> <i>Limited Data Set (evaluate possibility of re-identification if ZIP Code and/or DOB included)</i> 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	<b>1</b>
	<input type="checkbox"/> <b>General PHI</b> Information about treatment, diagnosis, service, medication, etc.	<b>2</b>
	<input type="checkbox"/> <b>Financial Data and/or Personal Identifiers</b> <ul style="list-style-type: none"> <li>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:</li> <li>Social security or employer taxpayer identification numbers</li> <li>Driver's license, State identification card, or passport numbers</li> <li>Checking account numbers</li> <li>Savings account numbers</li> <li>Credit card numbers</li> <li>Debit card numbers</li> <li>Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)</li> <li>Any other numbers or information that can be used to access a person's financial resources</li> <li>Passwords-if the information would provide access to financial information or resources</li> <li>Sensitive Protected Health Information which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health</li> </ul>	<b>3</b>
	<b>Specify the Type(s) of Information Accessed or Disclosed:</b>	

# McLaren Health Care

## Breach Notification Risk Assessment Tool

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

# McLaren Health Care

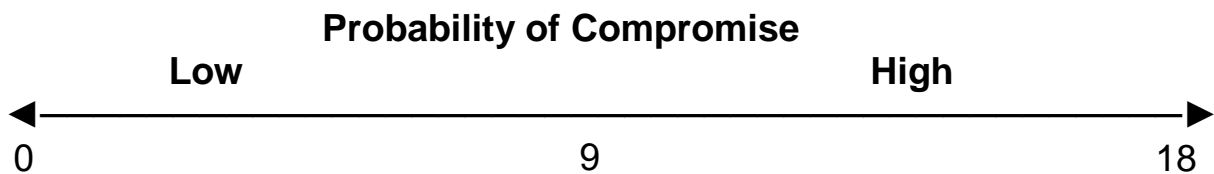
## Breach Notification Risk Assessment Tool

	<input type="checkbox"/> Sent to the Media	
--	--------------------------------------------	--

### SCORING

<b>Total Probability of Compromise Score</b> <i>(Section 2)</i>	
-----------------------------------------------------------------	--

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 in 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.



<b>Additional information and basis for decision:</b>	<b>Final Decision</b>	
	<b>Low Probability of Compromise</b>	<input type="checkbox"/>
	<b>Breach Requiring Notice</b>	<input type="checkbox"/>
<b>Resolution and Corrective Action(s) (actions taken to prevent recurrence, responsible individual(s), and target dates for completion):</b>  <input type="checkbox"/> Corrected system issues (e.g., disabled auto-faxing, updated system with correct information, etc.) <input type="checkbox"/> Reviewed user security access levels for appropriateness and identified required changes <input type="checkbox"/> Changed or updated policies/procedures <input type="checkbox"/> Discussed results with leader(s) and identified changes to improve process or prevent reoccurrence <input type="checkbox"/> Counseled/educated to person or staff members to assure they understand what they did was wrong <input type="checkbox"/> Retrieved PHI or documented recipient's assurances that PHI was destroyed or not further disclosed  <b>Document in detail all the above corrective actions in ComplyTrack.</b>		

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

\_\_\_\_\_  
**Individual completing Risk Assessment**

\_\_\_\_\_  
**Date**