McLaren HEALTH CARE		Policy Title:	Business Associate and Data Use Agreements
Effective Date:	April 1, 2010	Policy Number:	MHC_CC1106
Review Date:		Section:	Compliance
Revised Date:	June 16, 2021	Oversight Level:	Corporate
Administrative Responsibility:	Vice President, Corporate Compliance; HIPAA Council		

1. Purpose

1.1. To ensure compliance with federal regulations and HIPAA Rules regarding the use or disclosure of Protected Health Information ("PHI"), including ePHI to Business Associates within the context of a contractual relationship.

2. Scope

2.1. McLaren Health Care Corporation ("MHC"), its subsidiaries, any other entity or organization in which MHC or an MHC subsidiary owns a direct or indirect equity interest of 50% or more, provided that organization has agreed to adopt MHC policies; and MHC's workforce members, including employees and contracted agents, physicians, volunteers, vendors/suppliers, and other business partners.

3. Definitions

3.1. **Breach** means the acquisition, access, use, or disclosure of protected health information in a manner not permitted, which compromises the security or privacy of the protected health information. See MHC_CC1109 HIPAA Privacy and Security Breaches, Notifications, and Mitigation Policy for detail.

3.1.1. There are three exceptions to the definition of "breach."

3.1.1.1. The unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of MHC or its 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.

3.1.1.2. An inadvertent disclosure of PHI from a person authorized to access PHI at MHC or its Business Associate to another person authorized to access PHI at MHC or its Business Associate, or organized health care arrangement in which MHC participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

3.1.1.3. If MHC or its Business Associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

3.2. **Business Associate** means an organization or a person, other than a Workforce Member who:

3.2.1. On behalf of MHC, creates, receives, maintains, or transmits PHI for: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; fundraising or marketing, record storage, and repricing; or

3.2.2. Provides one of the following services which involves the disclosure of PHI from MHC or another Business Associate: mailing, legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; or financial services to MHC;

3.2.3. Provides data transmission services which routinely require access to PHI;

3.2.4. Provides personal health records to one or more individuals on behalf of MHC;

3.2.5. Is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate;

3.2.6. Business Associate does not include:

3.2.6.1. Subsidiaries or other covered entities which are part of an MHC organized health care arrangement;

3.2.6.2. Government agencies that determine eligibility for a government health plan;

3.3. **Business Associate Agreement (BAA) or "Agreement"** means an agreement, addendum to an underlying contract, or similar document such as a letter of agreement or a scope of work between MHC and a Business Associate that defines the parties duties and responsibilities under the HIPAA Rules, and enables MHC to obtain satisfactory assurances from the Business Associate regarding safeguarding Protected Health Information.

3.4. **Data Use Agreement (DUA)** means a documented agreement between MHC and a recipient that permits uses and disclosures of a Limited Data Set for purposes of research, public health, and health care operations. The purpose of the Agreement is to obtain satisfactory assurance that the Limited Data Set recipient will only use or disclose the PHI for limited purposes defined in the Agreement.

3.5. **Designated Record Set** includes any records maintained by or for an MHC Covered Entity that includes all medical and billing records that are used whole, or in part, to make healthcare decisions about Individuals.

3.6. **HIPAA Rules** means the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and implementing regulations, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"), Standards for Electronic Transactions, and the privacy, security and Breach Notification regulations of the Health Information Technology for Economic and Clinical Health Act ("HITECH Rules") and HIPAA Omnibus final rule.

3.7. **Individual** means the person who is the subject of PHI or the Authorized Representative acting on behalf of the Individual.

3.8. **Limited Data Set** is PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household member of the Individual:

3.8.1. Names;

3.8.2. Postal address information, other than town or city, State, and zip code;

3.8.3. Telephone numbers;

3.8.4. Fax numbers;

3.8.5. Electronic mail addresses;

3.8.6. Social security numbers;

3.8.7. Medical record numbers;

3.8.8. Health plan beneficiary numbers;

3.8.9. Account numbers;

3.8.10. Certificate/license numbers;

3.8.11. Vehicle identifiers and serial numbers, including license plate numbers;

3.8.12. Device identifiers and serial numbers;

3.8.13. Web Universal Resource Locators (URLs);

3.8.14. Internet Protocol (IP) address numbers;

3.8.15. Biometric identifiers, including finger and voice prints; and

3.8.16. Full face photographic images and any comparable images.

3.9. **McLaren Health Care (MHC)** means McLaren Health Care Corporation, its wholly owned subsidiaries, and any other entity or organization in which MHC or an MHC subsidiary owns a direct or indirect equity interest of 50% or more, provided that organization has agreed to adopt MHC policies.

3.10. **Protected Health Information (PHI)** is defined as any individually identifiable health information that is collected from an Individual, and is transmitted, received, created and/or maintained, in any form or medium, by MHC and/or its subsidiaries.

3.10.1. PHI is any information that:

3.10.1.1. Relates to the past, present or future physical or mental health/condition of an Individual.

3.10.1.2. Relates to the provision of health care to an Individual.

3.10.1.3. Relates to the past, present, or future payment for the provision of health care to an Individual.

3.10.2. PHI is any information that either identifies the Individual or there is a reasonable basis to believe the information can be used to identify the Individual, including, but not limited to: name, medical record number, encounter number, social security number, address and photo, and diagnosis, diagnostic reports, procedures, progress notes, images, medications, billing documents, physician or location (if such information leads one to know or infer a diagnosis, etc.), slides, and/or blocks.

3.10.3. PHI excludes:

3.10.3.1. Records of students maintained by federally funded educational agencies: covered by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g; or

maintained by a healthcare provider and used only for the treatment of students 18 years or older, or attending post-secondary educational institutions, 20 U.S.C. 1232g(a)(4)(B)(iv);

3.10.3.2. Employment records held by MHC in its role as employer; and

3.10.3.3. Records of a person who has been deceased more than 50 years.

3.11. **Secretary** means the Secretary of Health and Human Services.

3.12. **Secured PHI** is PHI that is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

3.12.1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

3.12.1.1. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

3.12.1.2. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

3.12.2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

3.12.2.1. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

3.12.2.2. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

3.13. **Security Breach** is the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information and only applies to "unsecured PHI". A security breach requires reporting following the guidelines of the Breach Notification Rule.

3.14. **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

3.15. **Subcontractor** is a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

3.16. Trading Partner Agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a Standard Transaction.)

3.17. Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals as defined under the definition of Secured PHI.

3.18. Workforce / Workforce Members is defined as employees, temporary workers, contracted agents, physicians, volunteers, vendors/suppliers, consultants, students and other persons or entities whose conduct in the performance of work is under the direct control of MHC or its Business Associate, whether or not they are paid by MHC and/or its Business Associate.

4. Policy

4.1. Business Associate Agreements (BAA). MHC may disclose PHI to a Business Associate and allow it to create, receive, maintain, or transmit PHI on its behalf provided MHC obtains satisfactory assurance that the Business Associate will appropriately safeguard the information. Such assurance must be documented by MHC through a written contract, written agreement or arrangement with the Business Associate.

4.1.1. A BAA is not required for the following types of relationships:

4.1.1.1. *Health Care Services*. When MHC discloses PHI to a provider of health care services, for purposes of providing medical treatment to the individual to whom the PHI pertains.

4.1.1.2. *Disclosure to a Health Plan for Payment*. To disclose PHI to a health plan for purposes of obtaining payment for health care services. However, health plan contracts with MHC must conform to the standards of the Trading Partner Agreement.

4.1.1.3. *Disclosure from a Group Health Plan*. When the disclosure of PHI is from MHC's group health plan to MHC, in its capacity as plan sponsor, it is governed by the plan documents.

4.1.2. *Subcontractor*. A Business Associate may disclose PHI to a Business Associate that is a Subcontractor and may allow the Subcontractor to create, receive, maintain, or transmit PHI on its behalf, if the Business Associate obtains satisfactory assurances that the Subcontractor will appropriately safeguard the information in the form of a written agreement. The Agreement between the Business Associate and the Subcontractor must impose the same restrictions and conditions on the Subcontractor that are imposed in the Agreement between MHC and the Business Associate.

4.1.3. *Legal Requirements*. If a Business Associate is required by law to perform a function or activity on behalf of or to provide a service described in the definition of Business Associate, MHC may disclose PHI to the Business Associate to the extent necessary to comply with the legal mandate. MHC will attempt in good faith to obtain an agreement that meets the standards of this policy, and, if such attempt fails, will document the attempt and the reasons that the agreement cannot be obtained.

4.1.4. *Breach of BAA*. If MHC knows of a pattern, activity, or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the BAA or other arrangements, MHC must take reasonable steps to cure the breach or end the violation. If such actions are unsuccessful, the BAA or arrangement must be terminated, if feasible. Alternatively, the problem must be reported to the Secretary of Health and Human Services.

4.1.5. *Notification of Security Incident or Unauthorized Disclosure by a Business Associate*. A Business Associate is required to notify MHC of any Security Incident or Unauthorized Disclosure of unsecured PHI, including a Breach, upon discovery. A Security Incident or Breach is considered "discovered" as of the first day on which such Security Incident or Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a Security Incident or Breach if it is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Security Incident or Breach, who is an employee, officer, or other agent of the Business Associate.

4.1.5.1. *Security Incident*. If a Security Incident occurs at or by a Business Associate, the Business Associate must notify MHC following the discovery of the security incident. A Business Associate must provide notice to the MHC Privacy Officer as soon as possible, but no later than the time period specified in the Agreement. To the extent possible, the Business Associate must provide MHC with the details about the Security Incident, including the date of the incident, date of discovery, type of data involved, and individuals involved.

4.1.5.1.1. *Unsuccessful Security Incidents*. Business Associate is not required to report attempted Security Incidents that fail to be successful and consequently fail to result in the unauthorized use or disclosure of EPHI, such as pings and other broadcast attacks on the Business Associate's firewall, port scans, unsuccessful log-on attempts, and denials of service occur.

4.1.5.2. *Breach of Unsecured PHI*. If a Breach of Unsecured PHI occurs at or by a Business Associate, the Business Associate must notify MHC following the discovery of the breach. A Business Associate must provide notice to the MHC Privacy Officer immediately or within the time period specified in the Agreement. To the extent possible, the Business Associate must provide MHC with the following:

4.1.5.2.1. Each Individual whose PHI has been or is reasonably believed to have been Accessed, acquired, or Disclosed during the occurrence;

4.1.5.2.2. A brief description of what happened including the date of the occurrence and the date of the discovery of the occurrence, if known;

4.1.5.2.3. A description of the types of PHI that were involved in the occurrence (such as full name, social security number, date of birth, home address, account number, etc.);

4.1.5.2.4. A brief description of what the Business Associate is doing to investigate the occurrence, to mitigate losses and to protect against further occurrences;

4.1.5.2.5. The actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the occurrence;

4.1.5.2.6. A corrective action plan that includes the steps the Business Associate has taken or shall take to prevent future similar occurrences;

4.1.5.2.7. Any additional information reasonably requested by MHC for purposes of investigation a Breach.

4.1.5.3. At MHC's option, or as specified in the BAA, the Business Associate will notify Individuals under the direction of MHC Privacy Officer or designee, or cover the associated costs if MHC provides notice to Individuals.

4.1.5.4. MHC shall determine whether further investigation by an independent forensic expert is required.

4.1.6. *Designated Record Sets*. The BAA will include the Business Associate's responsibilities to respond to MHC and Individual requests if it maintains PHI in a Designated Record Set on behalf of MHC.

4.1.7. *Availability of Books and Records including Audits.* The BAA will include the Business Associate's responsibility to provide books and records to McLaren as well as to the Secretary of HHS. In addition, the BAA will include a provision requiring Business Associate to cooperate with periodic audits to determine the Business Associate's compliance with HIPAA Rules.

4.1.8. *Activities Outside the United States.* The BAA will include the Business Associate's warranty that neither it nor any agents or Subcontractors will transfer, access, store, or otherwise handle PHI outside the United States without the prior written consent of McLaren. Further, the Business Associate will not use off-shore employees, agents, or Subcontractors to provide the Services.

4.1.9. *Permitted and Required Access, Use, and Disclosure*. The Agreement between MHC and the Business Associate must establish permitted and required accesses, uses, and disclosures of PHI by the Business Associate, and permit the Business Associate to access, use, and disclose PHI for the proper management and administration of the Business Associate or permit the Business Associate to provide data aggregation services relating to the healthcare operations of MHC.

4.1.9.1. Data aggregation services by a Business Associate that do not relate to the healthcare operations of MHC must be reviewed and approved by the Corporate Compliance Officer or the subsidiary Compliance Officer.

4.1.10. *Responsibilities and Duties the Business Associate*. The Agreement must include the responsibilities and duties of the Business Associate to comply with the HIPAA Rules, including:

4.1.10.1. Limiting access, use, and disclose of the information other than as permitted or required by the BAA or as required by law;

4.1.10.2. Adhering to the Minimum Necessary Standard when accessing, using, and disclosing PHI;

4.1.10.3. Implementing appropriate safeguards to prevent access, uses, or disclosures of the information other than as provided for by its BAA;

4.1.10.4. Reporting to MHC any access, uses, or disclosures of the information not provided for by its BAA, including Breaches of Unsecured PHI and Security Incidents, of which it becomes aware;

4.1.10.5. Ensuring that any agent, including a Subcontractor, to whom it provides PHI, received from, or created or received by, the Business Associate on behalf MHC, agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information;

4.1.10.6. Making available PHI in accordance with federal regulations;

4.1.10.7. Complying with requirements and requests made by Individuals and/or MHC if the Business Associate maintains PHI in Designated Record Sets on behalf of MHC. This includes confidential communication requests, making PHI available for amendment or access, restricting disclosures including those to a health plan, documenting accounting of disclosures of PHI, and responding to requests for accountings.

4.1.10.8. Making its internal practices, books, and records relating to the use and disclosure of PHI received from, created or received by MHC available to MHC and the Secretary of Health and Human Services for purposes of determining MHC's compliance with federal regulations;

4.1.10.9. Not receiving remuneration, directly or indirectly, in exchange for disclosing PHI, except as specifically permitted under the HIPAA Rules; and

4.1.10.10. At the termination of the BAA, if feasible, return or destroy all PHI, and copies received from, created or received by the Business Associate and its agents or Subcontractors, on behalf of MHC that the Business Associate still maintains in any form. If such return or destruction is not feasible, extend the protections of the BAA to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible.

4.1.11. *Termination Authorization*. The BAA may authorize termination of the BAA by MHC, if MHC determines that the Business Associate has violated a material term of the BAA. MHC may omit the termination authorization, if such authorization is inconsistent with statutory obligations of MHC or its Business Associate.

4.1.12. *Other Permissions*. A BAA or other arrangement between MHC and the Business Associate may permit the Business Associate to use the information received by the Business Associate in its capacity as a Business Associate to MHC, if necessary:

4.1.12.1. for the Business Associate's proper management or administration, or to carry out the legal responsibilities of the Business Associate;

4.1.12.2. if the disclosure is required by law; or

4.1.12.3. the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and accessed, used, or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

4.1.12.4. the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

4.1.13. *Notification by a Business Associate*. A Business Associate is required to notify MHC of all Security Incidents and Breaches of Unsecured PHI, subject to paragraph 4.1.5.1. The detail of the Security Incident or Breach may be documented in the *Notification to McLaren about a Security Incident and/or Breach of Unsecured Protected Health Information Form* MHC_CC1106.7.4 and sent to the MHC Privacy Officer.

4.1.13.1. The MHC Privacy Officer will obtain from the Business Associate the required information related to the Breach noted in Section 4.1, and provide notice to Individuals as required by the HIPAA Privacy and Security Breaches, Notification, and Mitigation Policy (MHC_CC1109). The Business Associate may document the risk assessment process in the Breach Notification Risk Assessment Tool (MHC_CC1109.7.3b).

4.1.14. *Vendor Security Risk Assessment Project Initiation Form and Audits.* The MHC Privacy Officer, or designee, will obtain from the Business Associate prior to execution of the BAA and underlying agreement, a completed Vendor Security Risk Assessment Project Initiation Form.

4.1.14.1. Periodic audits may be conducted following implementation of the Agreement.

4.1.14.2. Designated Security certifications, (e.g, HITRUST or SOC II) may be accepted in lieu of an audit conducted by McLaren.

4.1.15. *McLaren Entity as a Business Associate*. When a McLaren entity is the Business Associate, the BAA will include provisions similar to those listed above, except those which may not be required by the contracting Covered Entity.

4.2. Data Use Agreement (DUA). MHC must enter into a DUA in order to disclose a Limited Data Set.

4.2.1. MHC will only enter into a DUA and disclose a Limited Data Set for the purpose of research, public health or Health Care Operations.

4.2.2. MHC must assure that the DUA includes all elements listed in Contents of the DUA noted in paragraph 4.2.4 below.

4.2.3. If MHC learns of a pattern of activity or practice of the Limited Data Set recipient that constitutes a material breach or violation of the DUA, MHC will take reasonable steps to cure the breach as applicable, and, if such steps were unsuccessful:

4.2.3.1. Discontinue disclosure of PHI to the recipient; and

4.2.3.2. Report the problem to the Secretary.

4.2.4. *Contents of the DUA*. To use or disclose a Limited Data Set, the DUA must:

4.2.4.1. Establish the permitted uses and disclosures of such information by the Limited Data Set recipient. The DUA may not authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate the requirements of the HIPAA Rules, if done by MHC;

4.2.4.2. Establish who is permitted to use or receive the Limited Data Set; and,

4.2.4.3. Provide that the Limited Data Set recipient will:

4.2.4.3.1. Not use or further disclose the information other than as permitted by the DUA or as otherwise required by law;

4.2.4.3.2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the DUA;

4.2.4.3.3. Report to MHC any use or disclosure of the information not provided for by its DUA of which it becomes aware;

4.2.4.3.4. Ensure that any agents, including a subcontractor, to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and

4.2.4.3.5. Not identify the information or contact the Individuals.

5. Procedure

5.1. Business Associate Agreement. For those relationships that constitute "Business Associate" relationships, MHC shall enter into appropriate written agreements with the Business Associate.

5.1.1. *BAA Template*. The MHC BAA template will be used whenever possible in contractual relationships in which the agreement is required. The template for McLaren Entity as the Business Associate will be used when McLaren is the BA.

5.1.1.1. Occasionally, there may be exceptions. Any exceptions will require the approval of the Corporate Compliance Officer, or if a subsidiary agreement, the subsidiary Compliance Officer, and the BAA must meet all requirements established in Section 4.1 of this policy.

5.1.2. *BAA Tracking.* All BAAs will be created by or provided to the Corporate Compliance Officer, or if a subsidiary BAA, the Subsidiary Compliance Officer. The Compliance Officer will use the established tracking system to track implementation of all BAAs, including contact information for company representatives and individuals executing the BAA. BAA's will be entered into the Contract Management System with the underlying agreement.

5.1.3. *Vendor Security Risk Assessment Project Initiation Form.* The completed Form will be forwarded to the Chief Information Security Officer (CISO) via the email address noted on the Form. When determined by the CISO, additional information may be required from the vendor to verify that mitigating controls are in place when a risk exists, e.g., cloud or off-shore services. The completed Vendor Security Risk Assessment Project Initiation Form will be entered into the Contract Management System.

5.2. Data Use Agreement. MHC shall enter into a DUA to permit uses and disclosures of a Limited Data Set for purposes of research, public health, and health care operations.

5.2.1. *Data Use Agreement Template.* The MHC DUA will be used whenever possible in contractual relationships where a DUA is required. Non-McLaren DUA's may be used if they contain substantively the same provisions as the MHC template. DUA and BAA language may be combined in a single document.

5.2.2. *DUA Tracking.* All DUAs will be created by or provided to the Corporate Compliance Officer, or if a subsidiary BAA, the Subsidiary Compliance Officer. The Compliance Officer will use the established tracking system to track implementation of all DUAs, including contact information for company representatives and individuals executing the DUA. DUA's will be entered into the Contract Management System with the underlying agreement, if one exists.

6. References

6.1. HIPAA Privacy Regulations: 45 CFR 164.502(e)(1); 164.304; 164.308; 164.502(e)(2); and 164.504(e)

6.2. HIPAA Security Standards: 45 CFR 164.308(b)(1)

6.3. HITECH Act from American Recovery and Reinvestment Act of 2009.

6.4. MHC_CC0118 Identity Theft Prevention Program Policy

6.5. MHC_CC1109 HIPAA Privacy and Security Breaches, Notifications, and Mitigation

7. Appendix

7.1. MHC Business Associate Addendum Template

7.2. MHC as Business Associate Template

7.3. MHP Business Associate Template

7.4. Notification of Security Incident and/or Breach of Unsecured Protected Health Information Form

7.5. McLaren Vendor Security Risk Assessment Project Initiation Form

7.6. MHC_CC1109.7.3b Breach Notification Risk Assessment Tool

7.7. MDwise Business Associate Template

Previous Revisions: March 18, 2010, March 20, 2014, May 21, 2015, June 15, 2020

Supersedes Policy: Not Applicable

Approvals:

HIPAA Council: March 3, 2010, March 5, 2014, May 6, 2015, October 4, 2017, September 4, 2019, June 3, 2020, June 16, 2021
Corporate Compliance Committee: March 18, 2010, March 20, 2014, May 21, 2015, November 13, 2017, September 26, 2019, June 15, 2020, July 20, 2021

Signature on File
Gregory R. Lane
Sr. VP and Chief Administrative Officer

July 20, 2021
Date

BUSINESS ASSOCIATE ADDENDUM

This BUSINESS ASSOCIATE ADDENDUM ("**BAA**") is effective as of the last date appearing on the signature page hereto (the "**Effective Date**") and is entered into by and between the following parties (referred to herein collectively, as the "**Parties**" and individually, each a "**Party**"):

Vendor: **«Company_Name»** ("**Business Associate**")

and including but not limited to, the following McLaren entities, each a Covered Entity ("**McLaren**"):

«Subsidiaries_Included».

RECITALS

A. Pursuant to the Underlying Agreement (as defined below), Business Associate provides certain services, including, without limitation, **«Description_of_Contract_Services»** ("**Services**") to McLaren, which involves the creation, receipt, maintenance, access, transmission, Use, or Disclosure of PHI by Business Associate.

B. The Parties desire to ensure that their respective rights and responsibilities under the Underlying Agreement reflects applicable legal requirements relating to the protection of confidentiality and security of PHI in accordance with federal and state laws, to the extent that state laws are more restrictive, including the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), as amended by the Health Information Technology for Economic and Clinical Health Act ("**HITECH**") provisions of the American Recovery and Reinvestment Act of 2009, and Title I of the Genetic Information Nondiscrimination Act of 2008, and any regulations promulgated thereunder, including but not limited to the Privacy Rule, Security Rule, and Breach Notification Rule, as such laws and regulations may be amended from time to time (collectively, the "**HIPAA Rules**", together with HIPAA and HITECH, as the "**Privacy Laws**").

C. To comply with the Privacy Laws, the Parties must enter into an agreement that governs the creation, receipt, maintenance, access, transmission, Use, and Disclosure of the PHI by Business Associate in the course of performing the Services in connection with the Underlying Agreement.

NOW, THEREFORE, the Parties agree as follows:

1. DEFINITIONS.

1.1. General Statement. The following terms used in this BAA will have the same meaning as those terms in the HIPAA Rules: Administrative Safeguards, Availability, Breach, Business Associate, Code Set, Confidentiality, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information ("**EPHI**"), Health Care Operations, Individual, Integrity, Minimum Necessary, Physical Safeguards, Protected Health Information ("**PHI**"), Required by Law, Secretary, Security Incident, Standard Transaction, Subcontractor, Technical Safeguards, Unsecured PHI, Uses and Disclosures, and Workforce. A change to the Privacy Laws which modifies any defined term, or which alters the regulatory citation for the definition will be deemed incorporated into this BAA.

1.2. "**Breach Notification Rule**" means Part 2, Subtitle D of HITECH and Notification in the Case of Breach of Unsecured Protected Health Information at 45 C.F.R. Part 164 Subpart D.

1.3. "**Privacy Rule**" means the standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

1.4. "**Security Rule**" means the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part 164.

2. SCOPE AND STATUS. The terms and conditions of this BAA will supplement and amend all agreements and relationships between the Parties, whether in effect as of the Effective Date or thereafter (collectively, the "**Underlying Agreement**"), that provide for Business Associate's creation, receipt, maintenance, access, transmission, Use, or Disclosure of PHI, in any form or medium, including EPHI, in Business Associate's capacity as a "Business Associate" of McLaren, as such quoted term is defined in the HIPAA Rules.

3. BUSINESS ASSOCIATE OBLIGATIONS.

3.1. Data Use and Disclosure.

3.1.1. *Limits on Use and Disclosure.* Except as otherwise provided by this BAA, Business Associate may only Use and Disclose the PHI to perform the Services for, or on behalf of, McLaren, as set forth in the Underlying Agreement, *provided that* such Use or Disclosure, if made by McLaren, would not violate the Privacy Laws or other applicable laws. Business Associate agrees to make Uses, Disclosures, and requests for PHI consistent with the Privacy Rule's Minimum Necessary requirements and, to the extent practicable, the Limited Data Set requirements set forth in HITECH § 13405(b). Business Associate further agrees that it will institute and implement policies and practices to limit Uses and Disclosures to that which is minimally necessary to perform the Services. Additionally, Business Associate may:

(a) Use PHI for its own proper management and administration or to carry out its legal responsibilities; and

(b) Disclose PHI for its own proper management and administration or to fulfill any of its legal responsibilities, *provided that* **(i)** Disclosures are Required by Law, or **(ii)** Business Associate obtains reasonable assurances from the third party to whom the information is Disclosed that such PHI will be **(x)** held secure and confidential as provided pursuant to this BAA and will only be used or further disclosed for the purpose that it was disclosed to such third party or as may otherwise be Required by Law, and **(y)** that such third party agrees to notify Business Associate of any Breach involving Unsecured PHI or any Security Incident that results in a Use or Disclosure of EPHI that becomes known to such third party.

3.1.2. *De-Identification.* Business Associate may not de-identify PHI except as and only to the extent necessary to provide the Services. Business Associate may not Use or Disclose any such de-identified information for its own purposes without the prior written consent of McLaren, which consent may be granted at McLaren's sole discretion. Business Associate is further prohibited from disclosing such de-identified information to any third party who may re-identify such information.

3.1.3. *Data Aggregation.* Business Associate may not Use PHI in its possession to provide Data Aggregation services relating to the Health Care Operations of McLaren or any other Covered Entity to whom Business Associate provides services.

3.2. Safeguards. Business Associate will use reasonable and appropriate Administrative, Physical, and Technical Safeguards pursuant to the HIPAA Rules to prevent the Use and Disclosure of PHI other than pursuant to the terms and conditions of the Underlying Agreement, this BAA, or as Required by Law and to reasonably and appropriately protect the Confidentiality, Integrity, and Availability of PHI that Business Associate creates, receives, maintains, accesses, or transmits on behalf of McLaren. Such safeguards will include, at a minimum, (a) a comprehensive written information privacy and security policy addressing the requirements of the Privacy Laws, that are directly applicable to Business Associate with a named individual responsible for its overall execution; (b) periodic and mandatory privacy and security training and awareness program for Business Associate's Workforce members; (c) encryption for any mobile devices and (d) periodically conducting a risk analysis to identify potential risks and vulnerabilities that may affect the PHI and Business Associates ability to deliver the Services and timely remediating any identified risks and vulnerabilities as reasonably appropriate. Business Associate will, upon reasonable request, provide reports to McLaren related to the security measures implemented by Business Associate in connection with the Services provided to McLaren, which may be in the form of a third-party audit report. Further, Business Associate will, upon reasonable request, provide to McLaren reports regarding Services-related security issues.

3.3. Subcontractors and Agents. Business Associate will ensure that any Workforce member or agent, including a Subcontractor, that creates, receives, maintains, accesses, or transmits PHI on behalf of Business Associate agrees in writing to substantially similar, but not more permissive, restrictions and conditions that apply to Business Associate with respect to such information. Business Associate agrees to provide to McLaren copies of any such written agreements, within 10 business days of a written request from McLaren, *provided that* Business Associate may redact any sensitive business or financial terms. To the fullest extent permitted by applicable law and notwithstanding any contrary term in the Underlying Agreement, Business Associate will be liable to McLaren for any acts, failures, or omissions of the agent or Subcontractor in providing the Services and complying with the Privacy Laws as if they were Business Associate's own acts, failures, or omissions.

3.4. Reporting Unauthorized Uses, Breaches, and Security Incidents.

3.4.1. *Notification Time Frame.* Business Associate will notify McLaren's Privacy Officer in writing, promptly, but in no event longer than 5 business days, after becoming aware of **(a)** any Use or Disclosure of PHI that is not authorized by this BAA or the Underlying Agreement] **(b)** any Breach or reasonably suspected Breach involving Unsecured PHI; or **(c)** any Security Incident that results or is reasonably suspected to result in access to or a Use or Disclosure of EPHI in violation of this BAA or the Underlying Agreement (collectively with (a) and (b), as a "**Reported Incident**"). All incidents of ransomware that involve McLaren's PHI will be considered a Security Incident that is reportable to McLaren.

3.4.2. *Unsuccessful Security Incidents.* For Security Incidents that do not result in access to or a Use or Disclosure of EPHI in violation of this BAA or the Underlying Agreement (an "**Unsuccessful Security Incident**"), this Section 3.4.2 will be deemed as notice to McLaren that Business Associate periodically receives unsuccessful attempts for unauthorized access, Use, Disclosure, modification, or destruction of information or interference with the general operation of Business Associate's information systems and the Services, including pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, and denial-of-service attacks, and, even if such events are defined as a Security Incident under the HIPAA Rules, Business Associate will not provide any further notice regarding such unsuccessful attempts. To the extent required by the Security Rule, Business Associate will record or otherwise log all Unsuccessful Security Incidents, will maintain such records for the period required under the Security Rule, and will, upon McLaren's written request, provide a copy of any such records to McLaren.

3.4.3. *Investigation and Cooperation.*

(a) With respect to any Reported Incident, Business Associate will provide the notice in the manner and format specified by McLaren and such notice will include all information that is necessary for McLaren to comply with McLaren's obligations under the Breach Notification Rule including, without limitation, **(i)** a brief description of what happened, including the date of the occurrence, if known, and the date of the discovery of the occurrence; **(ii)** each Individual whose PHI has been or reasonably believed to have been accessed, acquired, or Disclosed, if known; **(iii)** a description of the types of PHI that were involved, if known; **(iv)** a brief description of what Business Associate is doing to investigate the occurrence and to mitigate losses and any harmful effects; and **(v)** a corrective action plan that includes the steps Business Associate has taken or will take to prevent future similar occurrences. Following the initial notice of a Reported Incident, Business Associate will provide periodic updates to McLaren as reasonably necessary. Business Associate will further reasonably cooperate with McLaren's investigation and risk assessment with respect to such Reported Incident and will provide any additional information reasonably requested by McLaren. Business Associate will maintain complete records regarding any event requiring reporting for the period required by 45 C.F.R. § 164.530(j) or such longer period as may be required by state law and, subject to any applicable legal privileges, will make such records available to McLaren promptly, but in no event longer than 10 days, upon any reasonable request.

(b) Business Associate will abide by McLaren's decision with respect to whether a Reported Incident constitutes a Breach of PHI. With respect to any Breach, McLaren will have the sole right to determine: **(i)** whether further investigation by an independent forensic expert is required; **(ii)** whether notice is to be provided to Individuals, regulators, law enforcement agencies, consumer reporting agencies, media outlets, the Secretary, and/or others as may be provided under applicable Privacy Laws; **(iii)** the contents of such notice and whether Business Associate or McLaren will be responsible for giving such notice, and if provided by Business Associate, the documentation required to demonstrate that notice was made in accordance with the Privacy Laws; and **(iv)** whether any type of remediation may be offered to affected Individuals, and the nature and extent of any such remediation. Business Associate agrees that with respect to any Reported Incident, notwithstanding any limitation of liability in the Underlying Agreement, Business Associate will pay or, at McLaren's discretion reimburse McLaren for all costs related to the following: investigation costs, provision of notices as contemplated herein, any remediation that McLaren determines is required or reasonably necessary, commercially reasonable mitigation efforts, any fines or penalties assessed against McLaren, settlements, and attorneys' fees incurred as a result of any of the foregoing or any third-party claims arising from a Reported Incident.

3.5. Mitigation. Business Associate will mitigate, to the extent practicable, any harmful effect, which is known to Business Associate, of a Use or Disclosure of PHI by Business Associate, its Workforce member or agents, including Subcontractors, if any, in violation of the requirements of the Underlying Agreement, this BAA, or the Privacy Laws. Business Associate will further take prompt action to mitigate, to the extent practicable, any harmful effect, which is known to Business Associate, of any Security Incident or Breach involving Unsecured PHI.

3.6. Access to PHI. In the event that the PHI in Business Associate's possession constitutes a Designated Record Set, Business Associate will promptly, but no more than 5 business days, make available to McLaren or, upon McLaren's request, to the Individual, access to the PHI so that McLaren may meet the requirements of 45 C.F.R. § 164.524. In the event any Individual delivers a request for access to PHI directly to Business Associate, Business Associate will, within 2 business days, forward such request to McLaren. McLaren will be responsible for determining whether an Individual obtains access to the PHI requested. In accordance with HITECH § 13405(e), if Business Associate controls access to PHI in an electronic health record, Business Associate agrees to provide a copy of the information in electronic format or, upon the Individual's request, to transmit such copy to an entity or person designated by the Individual.

3.7. Amendment of PHI. In the event that the PHI in Business Associate's possession constitutes a Designated Record Set, Business Associate will promptly, but no more than 5 business days, make available to McLaren access to the PHI so that McLaren may amend and Business Associate will incorporate such amendment in the PHI in accordance with 45 C.F.R. § 164.526. In the event any Individual delivers a request for amendment of PHI directly to Business Associate, Business Associate will, within 2 business days, forward such request to McLaren. McLaren is responsible for responding to Individuals' request for amendment of PHI.

3.8. Accounting of Disclosures of PHI. Business Associate will document all Disclosures of the PHI and such other information related to the Disclosure of PHI as may reasonably be necessary for McLaren to respond to any request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528. Within 10 business days of notice by McLaren to Business Associate that McLaren has received a request for an accounting of Disclosures of PHI regarding an Individual, Business Associate will make available to McLaren information, in the manner and format specified by McLaren, to permit McLaren to respond to the request for an accounting of Disclosures of PHI. In the event any Individual delivers a request for an accounting of Disclosures of PHI directly to Business Associate, Business Associate will forward such request to McLaren within 2 business days of receipt and McLaren is responsible for preparing and delivering any such accounting to the Individual.

3.9. Restrictions and Communications. Business Associate will comply with any restrictions on Disclosure of PHI requested by an Individual and agreed to by McLaren in accordance with 45 C.F.R. § 164.522, including the Individual's right to restrict certain disclosures of PHI to a health plan in accordance with HITECH § 13405(a). Additionally, Business Associate will, if directed by McLaren or requested by an Individual, use alternative means or alternative locations when communicating PHI to such Individual, based on the Individual's request for confidential communications.

3.10. Sale of PHI. Business Associate will not sell PHI or otherwise receive remuneration, directly or indirectly, in exchange for PHI unless McLaren has obtained an applicable authorization from that Individual, or unless receipt of such remuneration is specifically permitted by the Privacy Laws. Business Associate understands that McLaren does not request specific authorization from Individuals for the sale of PHI.

3.11. Privacy Rule Compliance. To the extent that Business Associate's Services include Business Associate carrying out one or more of McLaren's obligations under the Privacy Rule, then Business Associate agrees to comply with the requirements of the Privacy Rule that apply to McLaren in the performance of such obligation(s).

3.12. Red Flags Rule. In the event Business Associate's Services include billing, revenue cycle, or related services, Business Associate agrees that it will **(a)** use commercially reasonable efforts to implement safeguards, policies, and procedures to prevent identity theft in accordance with the Red Flags Rule; **(b)** notify McLaren within 2 business days of any 'red flag' or identity theft incident of which Business Associate becomes aware; **(c)** reasonably cooperate with McLaren to investigate and provide notice to victim(s) if required; and **(d)** mitigate, to the extent practicable, harm related to any identity theft incident related to Business Associate's Services.

3.13. Compliance with Electronic Transactions and Code Set Standards. Business Associate agrees that, in the event the Service's include Business Associate conducting any Standard Transaction for, or on behalf, of McLaren, Business Associate will comply, and will require any agent or Subcontractor conducting such Standard Transaction to comply, with each applicable requirement of 45 C.F.R. Part 162. Business Associate will not enter into, or permit its agents or Subcontractors to enter into, any agreement in connection with the conduct of Standard Transactions for or on behalf of McLaren that **(a)** changes the definition, health information condition, or use of a health information element or segment in a Standard; **(b)** adds any health information elements or segments to the maximum defined health information set; **(c)** uses any code or health information elements that are either marked 'not used' in the standard's implementation specification(s) or are not in the standard's implementation

specification(s); or **(d)** changes the meaning or intent of the standard's implementation specification(s). It will be McLaren's responsibility to ensure that appropriate Code Sets are used in the coding of services and supplies.

3.14. Availability of Books and Records. To the extent required by law, and subject to applicable attorney-client privileges, Business Associate will make its internal practices, books, and records available to the Secretary for purposes of determining McLaren's compliance with the Privacy Laws. In such event, Business Associate will promptly notify McLaren upon receipt by Business Associate of any such request for access by the Secretary, and, if permitted, will provide McLaren, with a copy thereof as well as a copy of all materials disclosed pursuant thereto. Further, Business Associate will reasonably cooperate with a McLaren audit undertaken to determine Business Associate's compliance with the Privacy Laws and its obligations under this BAA, including by making its Workforce members available for interviews and providing copies of written materials relevant to the scope of the audit, including, but not limited to, policies, procedures, training programs, and meeting minutes. Business Associate will provide to McLaren, upon reasonable request, a written certification of Business Associate's compliance with the Privacy Laws.

3.15. Assistance in Litigation or Administrative Proceedings. Business Associate will, at its cost, make itself, its Workforce members, agents, and Subcontractors assisting Business Associate in the performance of its obligations under this BAA, available to McLaren to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against McLaren, its directors, officers, or Workforce members based upon a claimed violation of this BAA or the Privacy Laws, except where Business Associate is named as an adverse party.

3.16. Subpoenas. In the event Business Associate receives a subpoena, court or administrative order, or other discovery request or mandate (collectively, the "**Order**") for release of PHI or any records related to McLaren, Business Associate will notify McLaren in writing, to the extent permissible under such Order, prior to responding to such request to enable McLaren to object. Business Associate will notify McLaren of the request as soon as reasonably practicable, but no more than 2 days of receipt of such request.

3.17. Activities Outside the United States. Business Associate represents and warrants that neither it nor any agents or Subcontractors will transfer, access, store, or otherwise handle PHI outside the United States without the prior written consent of McLaren. Further, unless otherwise contemplated in the Underlying Agreement, Business Associate will not use off-shore employees, agents, or Subcontractors to provide the Services.

3.18. Ownership. Notwithstanding any contrary term in the Underlying Agreement, Business Associate acknowledges that Business Associate has no ownership rights whatsoever related to the PHI, including any de-identified information or Limited Data Sets created therefrom, as a result of the Underlying Agreement or this BAA and McLaren is and remains the sole owner of any such PHI and the de-identified information and Limited Data Sets created therefrom, if any.

4. OBLIGATIONS OF MCLAREN.

4.1. Notice of Privacy Practices. McLaren will notify Business Associate of any limitation(s) in McLaren's Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation(s) may affect Business Associate's Use or Disclosure of PHI.

4.2. Restrictions. McLaren will notify Business Associate of any restriction to the Use or Disclosure of PHI that McLaren has agreed to or must comply with in accordance with 45 C.F.R. § 164.522 and HITECH § 13405(a), to the extent that such restriction may affect Business Associate. McLaren will notify Business Associate of any changes in, or revocation of, permission by Individuals to Use or Disclose their PHI, if such changes affect Business Associate's permitted or required Uses or Disclosures.

4.3. Compliance with Laws. McLaren will not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the Privacy Rule if done by McLaren.

4.4. Manner and Format. McLaren will provide to Business Associate, within 30 business days of McLaren executing this BAA, details regarding the manner and format that Business Associate will use to provide the information required hereunder, including, without limitation, notices pursuant to Section 3.4 (*Reporting Unauthorized Uses, Breaches, and Security Incidents*). McLaren may, in its reasonable discretion, modify such manner and format requirements at any time during the term of this BAA upon 30 calendar days' advance written notice.

5. INDEMNIFICATION AND LIMITATION OF LIABILITY. Each Party will indemnify, defend, and hold harmless the other Party and its officers, directors, trustees, employees, agents, successors and assigns, from and against any and all claims, actions, causes of action, demands, liabilities, damages, judgements, government investigations, government penalties actually incurred, reasonable costs actually incurred, and reasonable expenses actually incurred (including, but not limited to, reasonable attorneys' fees and interest) (collectively, the "**Claims**"), which the indemnified Party sustains or incurs to the extent arising out of, the indemnifying Party's or its Workforce members', agents', or Subcontractors' wrongful or negligent act, error, or omission in connection with the terms of this BAA or the Privacy Laws. In no event will either Party be liable to the other or to any third party for Claims (whether direct or indirect) caused by or incurred as a result of its own wrongful or negligent act, error, or omission or that of its Workforce members, agents, or Subcontractors in connection with this BAA or the Privacy Laws. Any limitations on liabilities or exclusions from liability agreed upon by the Parties, whether written (including in the Underlying Agreement) or oral, will not be applicable to the terms of this BAA, including the indemnification obligations contemplated in this Section 5, or the Privacy Laws.

6. TERM AND TERMINATION.

6.1. Term. The term of this BAA will be effective as of the earlier of the effective date of the Underlying Agreement or the Effective Date of this BAA and will terminate when all of the PHI provided by McLaren to Business Associate, or created, received, maintained, or transmitted by Business Associate (or its agents or Subcontractors) on behalf of McLaren, is destroyed or returned to McLaren, or, if it is infeasible to return or destroy the PHI, then protections are extended to such information in accordance with this BAA.

6.2. Termination. Upon McLaren's knowledge of a material breach of this BAA by Business Associate, McLaren will give Business Associate written notice of such breach and may provide a reasonable opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach within such time frame to McLaren's reasonable satisfaction, then, notwithstanding anything contrary in the Underlying Agreement, McLaren may terminate this BAA and the Underlying Agreement. McLaren may terminate this BAA and the Underlying Agreement immediately upon written notice if McLaren reasonably believes that cure of the material breach is not feasible. In the event this BAA is terminated by McLaren pursuant to this Section 6.2, any cancellation fees contemplated in the Underlying Agreement will be waived. McLaren may exercise any of its rights of access and inspection under Section 3.14 (*Availability of Books and Records*), and seek all other remedies at law or in equity, including but not limited to injunctive relief. McLaren's option to allow a cure of a breach of this BAA will not be construed as a waiver of any other rights McLaren has in this BAA, the Underlying Agreement, or by operation of law or in equity.

6.3. Effect of Termination. Upon the termination of this BAA or the Underlying Agreement for any reason, Business Associate will and will cause its agents and Subcontractors to return to McLaren, or, at McLaren's direction, destroy, all PHI received from McLaren that Business Associate, its agents, or Subcontractors, maintains in any form, recorded on any medium, or stored in any storage system. Business Associate will retain no copies of the PHI, including any compilations, Limited Data Sets, or de-identified data derived therefrom. Business Associate will complete such return or destruction as promptly as possible, but not more than 30 calendar days after the effective date of termination of the Underlying Agreement, and no later than on the 31st day, Business Associate will certify in writing to McLaren that such return or destruction has been completed. If Business Associate destroys PHI, it will be done with the use of technology or methodology that renders the PHI unusable, unreadable, or undecipherable to unauthorized individuals as specified in guidance provided by HHS and consistent with the guidelines set forth by the National Institute of Standards and Technology. If return or destruction is not feasible, Business Associate will explain in writing to McLaren why conditions make the return or destruction of such PHI not feasible. If McLaren, in its reasonable discretion, agrees that the return or destruction of PHI is not feasible, Business Associate will retain the PHI, subject to all of the protections of this BAA, and will make no further Use or Disclosure of such PHI. Business Associate will remain bound by the provisions of this BAA, even after termination, until such time as all of PHI has been returned or otherwise destroyed as provided in this Section.

7. GENERAL TERMS.

7.1. Regulatory References. A reference in this BAA to a section of the Privacy Laws, or the regulations issued thereunder, means the section or regulation as in effect or as amended, and for which compliance is required.

7.2. Amendment; Waiver. This BAA may be amended or supplemented only by a writing that refers explicitly to this BAA and that is signed by an authorized representative of each Party. The Parties agree to amend this BAA

as appropriate, to conform to any new or revised legislation, rules, and regulations to which McLaren is subject including, without limitation, the Privacy Laws and the Red Flags Rule. The Parties agree to make a good faith effort to amend this BAA within 90 days of either Party first providing written notice of such amendment and if the Parties are unable to mutually agree on such amended terms, then either Party may terminate this BAA upon 30 days written notice. Notwithstanding the immediately preceding sentence, if the Parties determine in good faith that amendments or alterations to the BAA are not feasible, then either Party may terminate this BAA upon 30 days prior written notice. No delay or failure of either Party to exercise any right or remedy available hereunder, at law, or in equity, will act as a waiver of such right or remedy, and any waiver will not waive any subsequent right, obligation, or default.

7.3. Relationship to Underlying Agreement. Any ambiguity in this BAA will be resolved to permit the Parties to comply with the Privacy Laws. If any express term of this BAA conflicts with the Underlying Agreement, then this BAA, if applicable, will control as to that term. The Underlying Agreement will control in all other instances, including, without limitation, governing law, venue, assignment, severability, and relationship of the Parties.

7.4. No Third Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor will anything herein confer, upon any person other than McLaren, Business Associate, or their respective successors or permitted assigns, any rights, remedies, obligations, or liabilities whatsoever.

7.5. Injunctive Relief. The Parties agree that the remedies at law for a violation of the terms of this BAA may be inadequate and that monetary damages resulting from such violation may not be readily measured. Accordingly, in the event of a violation by either Party of the terms of this BAA, the other Party will be entitled to immediate injunctive relief. Nothing herein will prohibit either Party from pursuing any other remedies that may be available to either of them for such violation.

7.6. Survival. The rights and obligations contained in Sections 3.1.2 (De-Identification), 3.4 (*Reporting Unauthorized uses, Breaches, and Security Incidents*), 3.5 (*Mitigation*), 3.8 (*Accounting of Disclosures of PHI*), 3.14 (*Availability of Books and Records*), 3.15 (*Assistance in Litigation or Administrative Proceedings*), 3.16 (*Subpoenas*), 3.18 (*Ownership*), 5 (*Indemnification and Limitation of Liability*), 6.3 (*Effect of Termination*), and 7 (*General Terms*) will survive the termination of this BAA.

7.7. Counterparts. This BAA may be executed in one or more counterparts, all of which together will constitute one agreement.

7.8. Reports to Privacy Officer. Business Associate will submit reports of Security Incidents and Breaches of Unsecured Protected Health Information to the McLaren Privacy Officer via email or by mail to:

«Privacy_Officer»

Effective Date: _____, __20__ (if none provided, then the last date indicated below)

By their signatures below, the undersigned, being an authorized representative of the applicable Party, agree that the terms and conditions of this BUSINESS ASSOCIATE ADDENDUM will be effective as of the Effective Date.

McLaren Health Care Corporation	**«Company_Name»**
_____	_____
«McLaren_Signer» «Title_MHC_Signer»	«Co_Leader» «Co_Leader_Title»
Date:_____	Date:_____

Business Associate Agreement

THIS BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into and effective on the date signed below, between **«Company_Name»** ("Cover Entity"), and Business Associate, **«Subsidiaries_Included»**, ("McLaren").

SERVICES

McLaren will provide the following services in accordance with this Agreement:

«Description_of_Contract_Services»

RECITALS

WHEREAS, McLaren performs on behalf of Covered Entity functions or activities involving the use and/or disclosure of Individually Identifiable Health Information;

WHEREAS, McLaren's provision of the services may require the disclosure by Covered Entity or creation, use or disclosure by McLaren of Individually Identifiable Health Information;

WHEREAS, McLaren is considered a "business associate" of Covered Entity under the HIPAA regulations; and

WHEREAS, this Agreement is intended to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and implementing regulations, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"), Standards for Electronic Transactions, and the privacy, security and Breach Notification regulations of the Health Information Technology for Economic and Clinical Health Act ("HITECH Rules") and HIPAA Omnibus final rule, (collectively "HIPAA Rules"). Any term not otherwise defined in this Agreement shall have the same meaning as given in the HIPAA Rules, as applicable, unless the context requires otherwise.

NOW THEREFORE, in consideration of the mutual promises contained in this Agreement, the parties agree as follows:

1. Definitions.

1.1. **General Statement**. The following terms used in this BAA will have the same meaning as those terms in the HIPAA Rules: Administrative Safeguards, Availability, Breach, Business Associate, Code Set, Confidentiality, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information ("EPHI"), Health Care Operations, Individual, Integrity, Minimum Necessary, Physical Safeguards, Protected Health Information ("PHI"), Required by Law, Secretary, Security Incident, Standard Transaction, Subcontractor, Technical Safeguards, Unsecured PHI, Uses and Disclosures, and Workforce. A change to the Privacy Laws which modifies any defined term, or which alters the regulatory citation for the definition will be deemed incorporated into this BAA.

1.2. **"Breach Notification Rule"** means Part 2, Subtitle D of HITECH and Notification in the Case of Breach of Unsecured Protected Health Information at 45 C.F.R. Part 164 Subpart D.

1.3. **"Privacy Rule"** means the standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

1.4. **"Security Rule"** means the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part 164.

2. Obligations and Activities of McLaren.

2.1. **Access, Uses and Disclosures.** McLaren agrees to Access, Use or Disclose, and shall ensure that its directors, officers, employees, contractors and agents Access, Use or Disclose, PHI only as permitted or required by this Agreement, or as required by law. Furthermore, McLaren shall not permit access to any PHI by any unauthorized person or Use an access code or authorization in an unauthorized manner. McLaren shall not

Access, Use or Disclose PHI in any manner that would constitute a violation of the HIPAA Rules, or other laws, if done by Covered Entity.

2.2. **Minimum Necessary.** McLaren agrees to make Uses, Disclosures, and requests for PHI consistent with the Minimum Necessary standard. In addition, McLaren agrees that it will institute and implement policies and practices to limit Uses and Disclosures to that which is minimally necessary to perform its services under this Agreement.

2.3. **Permitted Uses.** Except as otherwise limited in this Agreement or by law, McLaren may Access, Use or Disclose PHI provided to McLaren by Covered Entity:

2.3.1. To perform the functions, activities, or services for or on behalf of Covered Entity that are specified in this Agreement, provided that such Access, Use or Disclosure would not violate the HIPAA Rules, or other laws, if done by Covered Entity; and

2.3.2. For the proper management and administration of McLaren or to carry out the legal responsibilities of McLaren.

2.3.3. To report a violation of law to appropriate Federal and/or State authorities, consistent with 45 CFR §164.502(j)(1).

2.4. **Subcontractors and Agents**. McLaren agrees that it shall execute a written agreement that complies with all the requirements specified in §164.504(e)(2), and imposes the same restrictions and conditions that apply through this Agreement, to McLaren, with any Agent, including a Subcontractor, to whom McLaren provides PHI. McLaren agrees that, consistent with Section 13405(b) of the HITECH Act, it shall only provide said Agents and/or subcontractors with Limited Data Sets or the Minimum Necessary PHI required to perform services. Further, McLaren agrees to provide copies of said written agreements to Covered Entity within ten (10) business days of a request for same.

2.5. **Safeguards.** McLaren agrees to use reasonable and appropriate safeguards to prevent Access, Use or Disclosure of PHI other than as specifically authorized by this Agreement. Such safeguards shall at a minimum include:

2.5.1. A comprehensive written information privacy and security policy addressing the requirements of the HIPAA Rules, that are directly applicable to McLaren;

2.5.2. Periodic and mandatory privacy and security training and awareness for members of McLaren's Workforce; and

2.5.3. Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any electronic PHI, as provided for in the Security Rule and as mandated by Section 13401 of the HITECH Act and the safe harbor guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website, including documentation of all implemented Safeguards.

2.6. **Reporting Unauthorized Disclosures, Security Incidents and Breaches.** Except for unsuccessful security incidents defined in 2.6.1., McLaren agrees to promptly, and in no event later than five (5) business days upon becoming aware, report to Covered Entity's Privacy Officer any disclosure not provided for by this Agreement, security incident, or known or potential breach related to PHI, whether by McLaren (or the McLaren's employee, officer, agent or Subcontractor). McLaren further agrees, consistent with Section 13402 of the HITECH Act, to provide Covered Entity with information necessary for Covered Entity to meet the requirements of said section, and in a manner and format specified by Covered Entity.

2.6.1. **Unsuccessful Security Incidents.** Covered Entity and McLaren hereby agree that attempted Security Incidents that fail to be successful and consequently fail to result in the unauthorized use or disclosure of EPHI, such as pings and other broadcast attacks on the McLaren's firewall, port scans, unsuccessful log-on attempts, and denials of service occur, and that this constitutes McLaren's report and notification to Covered Entity of such events, and that no further reporting of such unsuccessful Security Incidents is required under this BAA.

2.6.2. **Discovery.** A security incident or Breach involving PHI shall be treated as "Discovered" as of the first day on which such occurrence is known to the McLaren (or the McLaren's employee, officer, agent or Subcontractor), or, by exercising reasonable diligence would have been known to the McLaren (or the McLaren's employee, officer, agent or Subcontractor).

2.6.3. **Investigation and Reports.** The McLaren shall immediately conduct an investigation and report, to Covered Entity's Privacy Officer, in writing within ten (10) business days the following information:

2.6.3.1. Each Individual whose PHI has been or is reasonably believed to have been Accessed, acquired, or Disclosed during the occurrence;

2.6.3.2. A brief description of what happened, including the date of the occurrence and the date of the discovery of the occurrence, if known;

2.6.3.3. A description of the types of PHI that were involved in the occurrence (such as full name, social security number, date of birth, home address, account number, etc.);

2.6.3.4. A brief description of what the McLaren is doing to investigate the occurrence, to mitigate losses and to protect against further occurrences;

2.6.3.5. The actions the McLaren has undertaken or will undertake to mitigate any harmful effect of the occurrence;

2.6.3.6. A corrective action plan that includes the steps the McLaren has taken or shall take to prevent future similar occurrences; and

2.6.3.7. Any additional information reasonably requested by Covered Entity for purposes of investigating a Breach of Unsecured PHI.

2.6.4. **Forensic Investigation, Notifications and Mitigation**. Covered Entity shall have the right to determine, with respect to a Breach:

2.6.4.1. Whether Notice is to be provided to Individuals, regulators, law enforcement agencies, consumer reporting agencies, media outlets and/or the Department of Health and Human Services, or others as required by law or regulation;

2.6.4.2. The contents of such Notice and whether McLaren or Covered Entity will be responsible for giving Notice, and if provided by McLaren, the documentation required to demonstrate notifications were made as required;

2.6.4.3. Whether any type of remediation may be offered to Individuals affected, and the nature and extent of any such remediation; and

2.6.4.4. The cost and expense of investigation, provision of Notices to affected Individuals and/or media, and any Remediation which Covered Entity determines is required or reasonably necessary, shall be the sole responsibility of the McLaren.

2.7. **PHI in Designated Record Sets.** To the extent that McLaren maintains PHI in a Designated Record Set, McLaren shall provide for the following:

2.7.1. **Confidential Communications.** McLaren shall, if directed by Covered Entity or an Individual, use alternative means or alternative locations when communicating PHI to an Individual based on the Individual's request for confidential communications.

2.7.2. **Availability of PHI for Amendment.** Within ten (10) business days of receipt of a request from Covered Entity for the amendment of an individual's PHI or a record regarding an Individual contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), McLaren will provide such information to Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 C. F. R. §164.526.

2.7.3. **Access to Information.** McLaren agrees to, within five (5) business days of request of Covered Entity, provide access to PHI in a Designated Record Set to Covered Entity or as directed by Covered Entity, to an Individual, in order to meet Covered Entity's requirements under 45 C.F.R. §164.524.

2.7.3.1. If McLaren controls access to PHI in an Electronic Health Record, McLaren agrees to provide a copy of the information in electronic format or to transmit such copy to an entity or person designated by the Individual, as required under Section 13405(c) of the HITECH Act.

2.7.3.2. In the event an Individual requests access to PHI directly from McLaren, McLaren will within two (2) business days, forward such request to Covered Entity. Covered Entity will be responsible for any denials to access to the PHI requested.

2.8. **Restricted Disclosures.** McLaren shall honor all restrictions, consistent with 45 C.F.R. §164.522, that Covered Entity or the Individual makes the McLaren aware of, including the Individual's right to restrict certain disclosures of PHI to a health plan, where the Individual pays out of pocket in full for the healthcare item or service, in accordance with HITECH Act Section 13405(a).

2.9. **Documentation and Accounting of Disclosures.** McLaren agrees to maintain necessary and sufficient documentation of Disclosures of PHI as would be required for Covered Entity to respond to a request by an Individual for an Accounting of such Disclosures, in accordance with 45 CFR §164.528.

2.9.1. McLaren agrees to provide, within ten (10) business days of receipt of a request from Covered Entity, for an Accounting of Disclosures, McLaren will provide, in a manner and format to be specified by Covered Entity, the following information:

2.9.2. Date of the Disclosure(s);

2.9.3. Name of the entity or person who received the PHI, and if known, the address of such entity or person;

2.9.4. A brief description of the PHI Disclosed; and

2.9.5. A brief statement of the purpose of and basis for such Disclosure.

2.9.6. In the event the request for an accounting is delivered directly to McLaren, McLaren will within two (2) business days forward such request to Covered Entity. It will be Covered Entity's responsibility to prepare and deliver any such Accounting requested.

2.9.7. McLaren agrees to implement an appropriate record-keeping process to enable it to comply with the requirements of this Section.

2.10. **Data Aggregation.** Business Associate shall not use PHI for Data Aggregation services. For purposes of this agreement, Data Aggregation service means the combining of PHI provided by McLaren to Business Associate, with PHI received by Business Associate in its capacity as a business associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective covered entities.

2.11. **De-Identification.** Unless specifically required by this Agreement, or otherwise agreed to in writing between the parties, McLaren shall not De-identify PHI or use De-identified PHI for any purpose, other than Permitted Uses listed above.

2.12. **Limitation on Remuneration for PHI.** With regard to its Use and/or Disclosure of PHI necessary to perform its obligations to Covered Entity and to comply with the HIPAA Rules, McLaren agrees not receive direct or indirect remuneration for any exchange of PHI not otherwise authorized under the HIPAA Rules without individual authorization, unless:

2.12.1. Specifically required for the provision of services under this Agreement,

2.12.2. For treatment purposes,

2.12.3. Providing the individual with a copy of his or her PHI; or

2.12.4. Otherwise determined by the Secretary in regulations.

2.13. **Availability of Books and Records.** Unless otherwise protected or prohibited from discovery or Disclosure by law, McLaren agrees to make internal practices, books, and records, including policies and procedures (collectively "Compliance Information"), relating to the Access, Use or Disclosure of PHI, available to Covered Entity or to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules.

3. Obligations and Activities of Covered Entity.

3.1. Covered Entity shall notify McLaren of the provisions and any limitation(s) in its Notice of Privacy Practices of Covered Entity in accordance with 45 CFR §164.520, to the extent that such provisions and limitation(s) may affect McLaren's Use or Disclosure of PHI.

3.2. Covered Entity shall notify McLaren of any changes in, or revocation of, permission by an Individual to Use or Disclose PHI, to the extent that the changes or revocation may affect McLaren's Use or Disclosure of PHI.

3.3. Covered Entity shall notify McLaren of any restriction to the Use or Disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, and also notify McLaren regarding restrictions that must be honored under section 13405(a) of the HITECH Act, to the extent that such restrictions may affect McLaren's Use or Disclosure of PHI.

3.4. Covered Entity shall notify McLaren of any modifications to accounting for Disclosures of PHI under 45 CFR §164.528, made applicable under Section 13405(c) of the HITECH Act, to the extent that such restrictions may affect McLaren's Use or Disclosure of PHI.

3.5. Covered Entity shall provide McLaren, within thirty (30) business days of Covered Entity executing this Agreement, a description and/or specification regarding the manner and format in which McLaren shall provide information to Covered Entity, wherein such information is required to be provided to Covered Entity as agreed to by McLaren. Covered Entity reserves the right to modify the manner and format in which said information is provided to Covered Entity, as long as the requested modification is reasonably required by Covered Entity to comply with the HIPAA Rules and McLaren is provided thirty (30) business days' notice before the requested modification takes effect.

4. **Indemnification**. Each party will indemnify, defend, and hold harmless the other party and its respective officers, directors or trustees, employees and agents from and against any and all claims, actions, causes of action, demands, liabilities, losses, damages, costs, and expenses (including, but not limited to, reasonable attorneys' fees and interest), which the other party or its respective officers, directors or trustees, employees, and agents sustains or incurs as a result of, in connection with, or arising out of, the indemnifying party's or its employees' or agents' negligence, malpractice, action, or failure to act, in connection with the fulfillment of this Agreement.

5. **Term and Termination.**

5.1. **Term.** The Term of this Agreement shall be effective the date signed below and shall terminate when all of the PHI provided by Covered Entity to McLaren, or created, received, maintained or transmitted by McLaren (or its Agents or Subcontractors) on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Agreement.

5.2. **Termination for Cause by Covered Entity.** Upon Covered Entity's knowledge of a material breach of this Agreement by McLaren, Covered Entity shall give McLaren written notice of such breach and provide reasonable opportunity for McLaren to cure the breach or end the violation. Covered Entity may terminate this Agreement, and McLaren agrees to such termination, if McLaren has breached a material term of this Agreement and does not cure the breach or cure is not possible. If neither termination nor cure is feasible, Covered Entity may report the violation to the Secretary. Covered Entity may exercise any of its rights of access and inspection under Section Availability of Books and Records, and seek all other remedies at law or in equity, including but not limited to injunctive relief. Covered Entity's option to allow a cure of the breach of this Agreement will not be construed as a waiver of any other rights Covered Entity has in this Agreement or by operation of law or in equity.

5.3. **Effect of Termination - Return or Destruction of PHI.** Upon the termination of this Agreement, for any reason, McLaren and its agents and subcontractors will return to Covered Entity, or, at Covered Entity's direction, destroy, all PHI received from Covered Entity that McLaren maintains in any form, recorded on any medium, or stored in any storage system, unless such information has been De-identified and is no longer PHI. This provision will apply to PHI that is in the possession of Subcontractors or agents of McLaren. McLaren will retain no copies of the PHI, including any compilations derived from and allowing identification of PHI.

5.3.1. McLaren shall complete such return or destruction as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of the Agreement. Within such thirty (30) day period, McLaren shall certify on oath in writing to Covered Entity that such return or destruction has been completed.

5.3.2. If McLaren destroys PHI, it shall be done with the use of technology or methodology that renders the PHI unusable, unreadable, or undecipherable to unauthorized individuals as specified in guidance provided by HHS. Acceptable methods for destroying PHI include:

5.3.2.1. Paper, film, or other hard copy media shredded or destroyed in order that PHI cannot be read or reconstructed; and

5.3.2.2. Electronic media cleared, purged or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST). HHS specifically excluded redaction as a method of destruction of PHI, unless the information is properly redacted so as to be fully De-identified.

5.3.3. Upon mutual agreement of the Covered Entity and McLaren, that return or destruction is not feasible, McLaren shall extend the protections of this Agreement to PHI received from or created on behalf of Covered Entity, and limit further Uses and Disclosures of such PHI, for so long as McLaren maintains the PHI. McLaren will remain bound by the provisions of this Agreement, even after termination, until such time as all of PHI has been returned, De-identified or otherwise destroyed as provided in this Section.

6. **Third Party Rights.** The terms of this Agreement are not intended, nor should they be construed, to grant any rights to any parties other than McLaren and Covered Entity.

7. **Owner of PHI.** Under no circumstances will McLaren be deemed in any respect to be the owner of any PHI Used or Disclosed by or to McLaren pursuant to the terms of this Agreement.

8. **Changes in the Law.** The parties agree to amend this Agreement as appropriate, to conform to any new or revised legislation, rules and regulations to which Covered Entity is subject now or in the future including, without limitation, the Privacy Standards, Security Standards, Transactions Standards, or Red Flags Regulations (collectively "Laws"). If within ninety (90) days of either party first providing written notice to the other of the need to amend this Agreement to comply with Laws, the parties, acting in good faith, are:

8.1. Unable to mutually agree upon and make amendments or alterations to this Agreement to meet the requirements in question; or

8.2. Alternatively, the parties determine in good faith that amendments or alterations to the requirements are not feasible then either party may terminate this Agreement upon thirty (30) days prior written notice.

9. **Reports to Privacy Officer.** Reports of Security Incidents and Breaches of Unsecured Protected Health Information shall be submitted by the McLaren to the Covered Entity Privacy Officer via email or by mail to:

Name:
Title:
Address:
Email:
Phone number:

Reports or concerns to McLaren should be made to:
«Privacy_Officer»

IN WITNESS WHEREOF, the parties have executed this Agreement the day and year last written below.

«Company_Name»:	**«Subsidiaries_Included»:**
Signed	Signed

«Co_Leader»
«Co_Leader_Title»

Date

«McLaren_Signer»
«Title_MHC_Signer»

Date

Business Associate Agreement

This Business Associate Agreement (**"Agreement"**) is entered into between McLaren Health Plan, Inc., McLaren Health Plan Community, and Health Advantage, Inc. (each referred to as a **"Covered Entity"**) and _____ (referred to as **"Business Associate"**), collectively the **"Parties"** as of _____ (**"Effective Date"**).

Recitals

A. McLaren Health Plan, Inc. and McLaren Health Plan Community are health maintenance organizations and are considered to be Covered Entities as defined under HIPAA.

B. Health Advantage Inc., is a third party administrator and is a considered to be a "Business Associate" under HIPAA.

C. For purposes of this Agreement, the parties intend that "Health Advantage, Inc." will be referred to as "Covered Entity" and Business Associate will be referred to as Business Associate throughout this Agreement even when it is performing activities as a Subcontractor for Health Advantage, Inc.

D. The Parties have a relationship where Business Associate provides functions or activities on behalf of, or provides services to Covered Entity that involve the use or disclosure of PHI.

E. The purpose of this Agreement is to comply with the requirements in HIPAA and as amended by HITECH.

F. The Parties intend for this Agreement to control as it relates to PHI if there is an inconsistency between the terms of this Agreement or the underlying agreement.

The Parties therefore agree as follows:

1. DEFINITIONS

Capitalized terms used, but not defined in this Agreement have the meaning provided in the HIPAA Privacy and Security Rules. For purposes of this Agreement, the following definitions apply:

"Electronic Protected Health Information" or "E-PHI" has the meaning given in 45 CFR §160.103, limited to the information that Business Associate creates, accesses, receives, maintains or transmits on behalf of Covered Entity in connection with the underlying agreement. E-PHI is a subset of PHI.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and any amendments.

"HIPAA Privacy and Security Rules" means HIPAA, HITECH, 45 CFR parts 160-164, and any other implementing regulations pertaining to the privacy or security of PHI.

"HITECH" means the Standards for Privacy and Security of Personal Health Information in Subtitle D (Privacy) of the Health Information Technology Economic and Clinical Health Act of 2009.

"Minimum Necessary" means a Limited Data Set or, if needed, the minimum necessary PHI to accomplish the intended purpose of a use, disclosure or request.

"Protected Health Information" or "PHI" has the meaning given in 45 CFR §160.103, limited to the information that Business Associate creates, accesses, receives, maintains or transmits on behalf of Covered Entity in connection with the underlying agreement.

"Secretary" means the Secretary of the Department of Health and Human Services or his or her designee.

"Subcontractor" means a person or entity to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of the business associate.

2. BUSINESS ASSOCIATE OBLIGATIONS, PERMITTED USES AND DISCLOSURES

2.1 Subject to the HIPAA Privacy and Security Rules. Business Associate is subject to and will comply with the requirements of the HIPAA Privacy and Security Rules. Business Associate will to the extent Business Associate carries out Covered Entity's obligations under the HIPAA Privacy and Security Rules, comply with the requirements of the HIPAA Privacy and Security Rules that apply to Covered Entity in the performance of the obligation.

2.2 Use and Disclosure of PHI. Except as otherwise expressly limited in the Agreement, Business Associate may use or disclose PHI:

A. To perform functions, activities, or services for, or on behalf of, Covered Entity in connection with the Agreement and any other agreements in effect between Covered Entity and Business Associate.

B. For the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that if Business Associate further discloses PHI:

I. The disclosure is Required by Law;

II. Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person and the person agrees to notify Business

Associate of any instances of which it is aware in which the confidentiality of the information has been Breached; or

III. To report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1)

C. Business Associate must not use or further disclose PHI other than as permitted or required by the Agreement or as Required by Law.

D. Business Associate will not de-identify PHI without Covered Entity's prior written consent.

E. Business Associate will not perform Data Aggregation services without Covered Entity's prior written consent.

2.3 Minimum Necessary. Except as permitted by 45 C.F.R. §164.502(b)(2), Business Associate must limit its use, disclosure and requests of PHI under the Agreement to the Minimum Necessary.

2.4 Safeguards. Business Associate must use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement and will implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and E-PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the HIPAA Privacy and Security Rules.

2.5 Mitigation. Business Associate must immediately report to Covered Entity any use or disclosure of PHI not provided for by this Agreement. Business Associate must promptly mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident, Breach, or a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement or the HIPAA Privacy and Security Rules.

2.6 Reporting of Breaches. Business Associate must immediately report to Covered Entity as soon as practicable, but not later than five (5) business days, after becoming aware of any Breach or reasonably suspected Breach of Unsecured Protected Health Information. Notwithstanding the foregoing, for a Covered Entity that contracts with CMS to provide Qualified Health Plan(s), Business Associate must report to the Covered Entity any Breach or reasonably suspected Breach of Unsecured Protected Health Information in the time periods necessary for Covered Entity to report the matter to CMS in accordance with the Covered Entity's agreement with CMS. In all cases, Business Associate will provide Covered Entity with all information related to the Breach or suspected Breach, including but not limited to the content requirements in 45 CFR §164.410. Business Associate will make members of its Workforce available and will cooperate with Covered Entity in any investigation related to a Breach.

2.7 Reporting of Security Incidents. Business Associate must immediately report to Covered Entity as soon as practicable, but not later than five (5) business days, after becoming aware of any Security Incident. Business Associate will provide Covered Entity with all information related to

the Security Incident, including but not limited to the content requirements in 45 CFR §164.410. Business Associate will make members of its Workforce available and will cooperate with Covered Entity in any investigation related to a Security Incident. All incidents of ransomware that involve PHI will be considered a Security Incident that is reportable to Covered Entity.

2.8 Agent and Subcontractor Requirements. Business Associate must ensure that any agent, including a Subcontractor, to whom it provides PHI received from or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to the information. Moreover, Business Associate must ensure that any agent or Subcontractor agrees to implement reasonable and appropriate safeguards to protect Covered Entity's E-PHI as required by the HIPAA Privacy and Security Rules. Business Associate shall disclose to its Subcontractors only the Minimum Necessary to perform the Services as are delegated to the Subcontractor by Business Associate.

2.9 Accounting of Disclosures. Business Associate must document disclosures of PHI and information related to the disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528. Business Associate must provide to Covered Entity or an individual, in time and manner reasonably designated by Covered Entity, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an individual for an accounting of disclosures of their PHI in accordance with 45 CFR §164.528.

2.10 Access to PHI. If Business Associate maintains PHI in a Designated Record Set for Covered Entity, Business Associate must provide access, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524.

2.11 Amendments to PHI. If Business Associate maintains PHI in a Designated Record Set for Covered Entity, Business Associate must make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to in accordance with 45 CFR §164.526 at the request of Covered Entity or an Individual, and in the time and manner reasonably designated by Covered Entity.

2.12 Books and Records. Business Associate must make its internal practices, books, and records related to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to Covered Entity, or at the request of Covered Entity to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Privacy and Security Rules. Covered Entity has the right to audit, investigate, monitor, access, review and report on Business Associate's use of any Covered Entity's PHI, with or without advance notice from Covered Entity.

2.13 Prohibition on Sale of PHI. Business Associate must not sell PHI or receive any direct or indirect remuneration, compensation, or other consideration in exchange for PHI. Business Associate must not transmit to any Individual any communication about a product or service that

encourages the recipient of the communication to purchase that product or service unless permitted to do so by HITECH Section 13405 and any implementing regulations.

2.14 Part 2 Requirements. If Business Associate uses, discloses, maintains, or transmits PHI that is protected by Part 2, Business Associate is bound by the Part 2 regulations. Any information Business Associate receives from Covered Entity that is protected by Part 2 is subject to protections that prohibit Business Associate from disclosing information protected by Part 2 without written consent of the individual, as required by Part 2. Business Associate acknowledges that any unauthorized disclosure of information under this section is a federal criminal offense.

2.15 Prohibition on Session Replay Scripts. Business Associate's website(s) will not contain analytics tools such as session replay scripts. Business Associate will redact, and abstain from gathering, data fields containing HIPAA information upon original configuration and each subsequent website update.

2.16 Assistance in Litigation or Administrative Proceedings. Business Associate will, at its cost, make itself, its Workforce members, agents, and Subcontractors, available to Covered Entity to testify as witnesses, or otherwise, if litigation or administrative proceedings are commenced against Covered Entity, its directors, officers, or Workforce members based upon a claimed violation of this Agreement or the HIPAA Privacy and Security Rules, except where Business Associate is named as an adverse party.

2.17 Training. Business Associate will provide training to its workforce and its Subcontractors and their workforce in accordance with HIPAA requirements. Business Associate will provide the training and evidence that the training was completed to Covered Entity upon Covered Entity's request.

2.18 Ownership. Business Associate has no ownership rights related to PHI, including any de-identified information or Limited Data Sets. Covered Entity is and remains the sole owner of all PHI and the de-identified information and Limited Data Sets created, if any.

2.19 Red Flags Rule. If Business Associate provides any billing, revenue cycle, or related services, Business Associate will: (a) use reasonable efforts to implement safeguards, policies, and procedures to prevent identity theft in accordance with the Red Flags Rule; (b) notify Covered Entity within two (2) business days of any 'red flag' or identity theft incident of which Business Associate becomes aware; (c) reasonably cooperate with Covered Entity to investigate and provide notice to victim(s) if required; and (d) mitigate, to the extent practicable, harm related to any identity theft incident related to Business Associate's services.

3. COVERED ENTITY OBLIGATIONS

3.1 Restrictions. Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy and Security Rules if done by Covered Entity. Except as provided in 45 CFR §164.502(b)(2), Covered Entity will limit its use, disclosure and requests of PHI under the Agreement to the Minimum Necessary.

3.2 Notifications to Business Associate. Covered Entity will provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI, if the changes affect Business Associate's permitted or required uses and disclosures. Covered Entity will also notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522.

3.3 Breach Notification. Covered Entity will be responsible for complying with the Breach notification rules in HITECH §13402 and implementing regulations.

4. TERM AND TERMINATION

4.1 Term. This Agreement will remain in effect until all other agreements between Covered Entity and Business Associate are terminated, unless terminated earlier as provided in this Agreement.

4.2 Termination. Upon one party's knowledge of a material violation of this Agreement by the other party, the non-violating party must either: (a) provide an opportunity for the violating party to cure the violation or end the violation and terminate this Agreement (and any underlying agreement) if the violating party does not cure the violation or end the violation within ten (10) business days; (b) immediately terminate this Agreement (and any underlying agreement) if cure is not possible; or (c) if neither termination nor cure are feasible, the non-violating party must report the violation to the Secretary.

4.3 Obligations of Business Associate upon Termination.

A. Except as provided in Section 4.3(B), upon termination of this Agreement, for any reason, Business Associate must return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision applies to PHI that is in the possession of Business Associate's Subcontractors or agents. Business Associate, its Subcontractors and agents must not retain any copies of PHI.

B. If Business Associate determines that returning or destroying the PHI is not feasible, Business Associate must provide to Covered Entity notification of the conditions that make return or destruction unfeasible. Upon mutual agreement of the Parties that return or destruction of PHI is not feasible, Business Associate must extend the protections of this Agreement to PHI and limit further uses and disclosures of PHI to those purposes that make the return or destruction unfeasible, for as long as Business Associate maintains the PHI.

4.5 Injunctive Relief. The Parties agree that the remedies at law for a violation of the terms of this Agreement may be inadequate and that monetary damages resulting from a violation may not be readily measured. Accordingly, in the event of a violation by either Party of the terms of this Agreement, the other Party will be entitled to immediate injunctive relief. Nothing in this Agreement will prohibit either Party from pursuing any other remedies that may be available to either of them.

5. GENERAL

5.1 Regulatory References. A reference in this Agreement to a section in the HIPAA Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.

5.2 Amendment. The parties mutually agree to enter into good faith negotiations to amend this Agreement from time to time in order for Covered Entity or Business Associate to comply with the requirements of HIPAA and HITECH, as they may be amended from time to time, and any implementing regulations that may be promulgated or revised from time to time.

5.3 Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Privacy and Security Rules.

5.4 Headings. The headings of articles and sections contained in this Agreement are for reference only and do not affect in any way the meaning or interpretation of this Agreement.

5.5 No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement, including but not limited to individuals whose PHI is created, received, used and/or disclosed by Business Associate in its role as business associate.

5.6 No Assignment. Covered Entity and Business Associate agree that this Agreement will not be assignable by either party except as expressly provided in this Agreement.

5.7 Binding Effect. This Agreement is binding upon the Parties and their successors and assigns.

5.8 Survival. The respective rights and obligations of Business Associate, including without limitation, the obligations of Business Associate under the termination section above, indemnification, ownership of PHI, reporting of Breaches and Security Incidents, will survive termination of this Agreement to the extent necessary to fulfill their purposes.

5.9 Notice. Any notices that may be required to be provided to each party under the terms of this agreement must be provided in writing by certified mail or through a nationally recognized overnight courier to the following addresses:

For Covered Entities:	**For Business Associate:**
McLaren Health Plan Attn: Privacy Officer G-3245 Beecher Road Flint, MI 48532	Attn:

5.10 Entire Agreement. This Agreement is the entire agreement between Covered Entity and Business Associate with respect to the matters covered in this Agreement. Covered Entity and Business Associate agree that there were no inducements or representations leading to the

execution of this Agreement, nor any other agreements between them, other than those contained in this Agreement.

5.11 Counterparts. This Agreement may be executed in any number of counterparts, each of which is an original and all of which taken together form one single document. If any signature is delivered by facsimile or by email delivery of a ".pdf", the signature creates a binding obligation of the Party signing with the same effect as if it were an original.

5.12 Indemnification. Business Associate must defend and hold harmless Covered Entity and any Covered Entity affiliate, officer, director, employee, subcontractor, agent or other members of its workforce, from all claims, liabilities, damages, fines, penalties, costs, expenses (including without limitation, reasonable attorney fees, and costs related to notifications under 45 CFR 164.400 – 164.408), or judgments which arise as a result of Business Associate's failure to meet any of its obligations under this Agreement.

5.13 Insurance. Business Associate represents and warrants that Business Associate has, and will maintain, at Business Associate's own expense, cyber liability insurance in the amount of at least $3,000,000 annual aggregate and liability insurance covering breach of Business Associate's requirements under this Agreement and Business Associate's negligent or intentional disclosure or Breach of PHI covered by this Agreement. At the request of Covered Entity, Business Associate must provide to Covered Entity proof of insurance coverage required by this Section.

5.14 Prohibition of Offshore Disclosure. Business Associate must not access, store, share, maintain, transmit or use or disclose PHI in any form through any medium with any entity or person, including Business Associate's employees and Subcontractors, beyond the boundaries and jurisdiction of the United States.

5.15 Governing Law and Venue. For McLaren Health Plan, Inc., McLaren Health Plan Community and Health Advantage, Inc., this Agreement, the rights of the Parties, and all actions arising in whole or in part under or in connection with it, will be governed by and construed in accordance with the laws of the state of Michigan, without giving effect to any choice or conflict-of-law provision or rule that would cause the application of the laws of any other jurisdiction. A final judgment in any action will be conclusive and may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

5.16 Several Liability. All representations, warranties, covenants, liabilities and obligations of a Covered Entity under this Agreement are several, and not joint, to each Covered Entity. No Covered Entity will be liable for any breach, default, liability or other obligation of another Covered Entity.

5.17 Conflict. If there is an inconsistency between the provisions of this Agreement and the HIPAA Privacy and Security Rules, as may be amended from time to time by the Secretary or as a result of interpretations by HHS, a court, or another regulatory agency, the HIPAA Privacy and Security Rules will prevail. If there is a conflict among the interpretation of these entities, the conflict will be resolved in accordance with rules of precedence. If there is an inconsistency between the provisions of this Agreement and the underlying agreement, this Agreement will prevail as it relates to the subject matter of this Agreement.

MCLAREN HEALTH PLAN, INC., MCLAREN HEALTH PLAN COMMUNITY, INC., AND HEALTH ADVANTAGE, INC.	_____
Covered Entity	**Business Associate**
By: _____ Nancy Jenkins On behalf of the above named entities	By: _____
Its: President and CEO	Its:
Date: _____	Date: _____

McLAREN HEALTH CARE

NOTIFICATION OF SECURITY INCIDENT AND/OR BREACH OF UNSECURED PROTECTION HEALTH INFORMATION

The sections below should be completed for a breach of unsecured protected health information.

Identify each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach, and a description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or disability code, diagnosis, or other types of information breached. If more space is needed, add more rows to the table below.

Individual (Last, First MI)	DOB (00/00/0000)	Medical Record #	Describe Type(s) of Information Breached

Describe how the unsecured PHI was breached:

Describe the recipient(s) of the unsecured PHI (i.e. another employee, a third-party that is considered a covered entity under HIPAA, a third-party who is not a covered entity, unknown, etc.):

Describe the steps the affected individuals should take to protect themselves from potential harm resulting from the breach:

Describe what is being done to mitigate losses to the individual, and to protect against any further breach (i.e. corrective action to prevent future occurrences):

McLAREN HEALTH CARE

NOTIFICATION OF SECURITY INCIDENT AND/OR BREACH OF UNSECURED PROTECTION HEALTH INFORMATION

Directions: Complete this form electronically and email it to Privacy@mclaren.org within ten (10) business days of discovering a breach of unsecured PHI or security incident.

Business Associate HIPAA Privacy/Security Contact:	
Name:	
Title:	
Address:	
Email Address:	
Phone Number:	
Website/Other:	

BREACH INFORMATION	
Total Number of Individuals Affected by the Breach:	
Date of Breach:	
Date of Discovery:	
Date of Breach Notification to HHS:	
Date of Breach Notification to Individuals:	

SECURITY INCIDENT REPORT (NO BREACH)	
Date of Security Incident:	
Date of Discovery:	
Type of Data:	

Describe the investigation of the breach or security incident:

Describe the risk assessment process and outcome of the risk assessment related to the breach or security incident:

Describe the individual(s) who committed the breach or security incident (i.e. employee, independent contractor, subcontractor, or unknown):

McLaren Security Risk Assessment Project Initiation:

Email completed survey and any questions to:

#	Question
1	Project Name:
2	POB Ticket#(if available):
3	MHC System/Project Contact:
4	MHC Sites Involved:
5	Vendor Name:
6	System Name:
7	System Description/Functionality:
8	Vendor Contact:
9	Vendor Phone:
10	Vendor Email:

securityriskassessment@mclaren.org

Anwser

Comments

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:	

McLaren Health Care
Business Associate Breach Notification Risk Assessment Tool

--- 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**

MDwise Business Associate Addendum

This Business Associate Addendum (this "Addendum") is made part of the Contract for Services and/or SOW of even date with this Addendum (the "Agreement") by and between _____ ("Business Associate") and MDwise, Inc. ("MDwise"), and is effective as of the Effective Date of the Agreement.

In order to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-64) ("HIPAA"), and in consideration of the mutual promises and obligations set forth in this Addendum and the Agreement, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Business Associate and MDwise agree as follows:

Business Associate shall comply with each and every obligation imposed upon business associates under the Health Information Technology for Economic and Clinical Health Act, Division A of Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005 ("HITECH Act") as if it is as Covered Entity under HIPAA and/or HITECH, and each of those obligations is hereby incorporated by reference into this Addendum, with the understanding that compliance with each of those obligations is required under this Addendum only as of the date upon which compliance with each of those obligations is required under the HITECH Act.

1. **Privacy of Protected Health Information**.
    a. **Permitted Uses and Disclosures.** Business Associate is permitted or required to use or disclose Protected Health Information it creates or receives for or from MDwise only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 C.F.R. § 164.504(e) and as follows:
        i. Functions and Activities on MDwise's Behalf. Business Associate is permitted to use and disclose Protected Health Information it creates or receives for or from MDwise as required to perform and provide the functions, activities and services described in the Agreement.
        ii. Business Associate's Operations. Business Associate may use Protected Health Information it creates or receives for or from MDwise as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities. Business Associate may disclose Protected Health Information as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities only if:
            A. The disclosure is required by law; or
            B. Business Associate obtains reasonable assurance, evidenced by written contract, from any person or organization to which Business Associate will disclose the Protected Health Information that the person or organization will:
                i. Hold the Protected Health Information in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as required by law; and
                ii. Notify promptly Business Associate (who will in turn notify promptly MDwise) in accordance with this Addendum and

applicable law, including, but not limited to, Section 13402 of the HITECH Act, of any instance of which the person or organization becomes aware in which the confidentiality of such Protected Health Information was breached.

b. **Additional Requirements; Prohibition on Unauthorized Use or Disclosure.** The additional requirements of Subtitle D of the HITECH Act that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to Business Associate and by this reference are hereby incorporated into this Addendum. Business Associate will neither use nor disclose Protected Health Information it creates or receives for or from MDwise or from another business associate of MDwise, except as permitted or required by this Addendum, as required by law or as otherwise permitted in writing by MDwise. This Addendum does not authorize Business Associate to use or disclose Protected Health Information in a manner that would violate the Privacy Standards, the Security Standards or the HITECH Act if done by MDwise.

c. **Information Safeguards.**

i. **Administrative, Technical and Physical Safeguards.** Business Associate will develop, implement, maintain and use appropriate administrative, technical and physical safeguards, in compliance with the Privacy Standards, the Security Standards and any other implementing regulations issued by the U.S. Department of Health and Human Services ("HHS"), to preserve the integrity and confidentiality of and to prevent non-permitted or violating use or disclosure of Protected Health Information created or received for or from MDwise. Business Associate will document and keep these safeguards current.

ii. **Application of Security Standards.** 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 shall apply to Business Associate in the same manner that such sections apply to covered entities. The additional requirements of Subtitle D of the HITECH Act that relate to security and that are made applicable with respect to covered entities shall also be applicable to Business Associate and by this reference are hereby incorporated into this Addendum.

iii. **Technology to Secure Protected Health Information**. Business Associate shall secure all Protected Health Information by a technology standard that renders Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute and is consistent with guidance issued by the Secretary of HHS specifying the technologies and methodologies that render Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals, including the use of standards developed under Section 2002(b)(2)(B)(vi) of the Public Health Service Act, as added by Section 13101 of the HITECH Act. Business Associate shall comply will all relevant guidance published by HHS relating to the most appropriate technical safeguards for use in complying with the Security Standards.

d. **Subcontractors and Agents.** Business Associate will require any of its subcontractors and agents, to which Business Associate is permitted by this Addendum or in writing by MDwise to disclose any of the Protected Health

Information Business Associate creates or receives for or from MDwise, to provide reasonable assurance, evidenced by written contract, that subcontractor or agent will comply with the same privacy and security obligations as Business Associate with respect to the Protected Health Information, including but not limited to the provisions of Section 4(b)(ii)(A) of this Addendum. In particular, and at a minimum, Business Associate shall maintain a current business associate agreement with all subcontractors, agents, or others that possess of have access to the Protected Health Information of MDwise members, which is compliant with the HIPAA and HITECH regulations that are in effect at any given time, and which are amended from time to time.

e. **Minimum Necessary.** Business Associate will, in its performance of the functions, activities, services and operations specified in Section 1(a)(i) above, make reasonable efforts to use, to disclose and to request only the minimum amount of Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request (including, to the extent practicable, limiting such use, disclosure or request to a limited data set, in accordance with 45 C.F.R. § 164.514(e) and Section 13405(b) of the HITECH Act and all guidance issued by HHS), except that Business Associate will not be obligated to comply with this minimum necessary limitation with respect to the following, as appropriate and applicable:
   i. Disclosure to or request by a health care provider for treatment;
   ii. Use with or disclosure to an individual who is the subject of the Protected Health Information, or that individual's personal representative;
   iii. Use or disclosure made pursuant to an authorization compliant with 45 C.F.R. § 164.508 that is signed by an individual who is the subject of the Protected Health Information to be used or disclosed, or by that individual's personal representative;
   iv. Disclosure to HHS in accordance with Section 3(e) of this Addendum;
   v. Use or disclosure that is required by law; or
   vi. Any other use or disclosure that is excepted from the minimum necessary limitation as specified in 45 C.F.R. § 164.502(b)(2).

2. **Compliance with Standard Transactions.** If Business Associate conducts, in whole or part, Standard Transactions for or on behalf of MDwise, Business Associate will comply, and will require any subcontractor or agent involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 C.F.R. Part 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of MDwise that:
   a. Changes the definition, data condition or use of a data element or segment in a Standard Transaction;
   b. Adds any data elements or segments to the maximum defined data set;
   c. Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or
   d. Changes the meaning or intent of the Standard Transaction's implementation specification.

3. **Protected Health Information Access, Amendment and Disclosure Accounting.**

a. **Access.** Business Associate will promptly, upon MDwise's request, make available to MDwise or, at MDwise's direction, to the individual (or the individual's personal representative) for inspection and obtaining copies any Protected Health Information about the individual (in a format, electronic or otherwise, designated by MDwise) that Business Associate created or received for or from MDwise and that is in Business Associate's custody or control, so that MDwise may meet its access obligations under 45 C.F.R. § 164.524 and Section 13405(e) of the HITECH Act, as applicable.

b. **Amendment.** Business Associate will, upon receipt of notice from MDwise, promptly amend or permit MDwise access to amend any portion of the Protected Health Information which Business Associate created or received for or from MDwise, so that MDwise may meet its amendment obligations under 45 C.F.R. § 164.526.

c. **Disclosure Accounting.** So that MDwise may meet its disclosure accounting obligations under 45 C.F.R. § 164.528 and Section 13405(c) of the HITECH Act, as applicable:

i. Disclosure Tracking. Business Associate will record for each disclosure, not excepted from disclosure accounting under Section 3(c)(ii) below, that Business Associate makes to MDwise or a third party of Protected Health Information that Business Associate creates or receives for or from MDwise, (A) the disclosure date, (B) the name and (if known) address of the person or entity to whom Business Associate made the disclosure, (C) a brief description of the Protected Health Information disclosed and (D) a brief statement of the purpose of the disclosure (items A-D, collectively, the "disclosure information"). For repetitive disclosures Business Associate makes to the same person or entity (including MDwise) for a single purpose, Business Associate may provide (X) the disclosure information for the first of these repetitive disclosures, (Y) the frequency, periodicity or number of these repetitive disclosures and (Z) the date of the last of these repetitive disclosures. Business Associate will, upon MDwise's request, promptly make this disclosure information available to MDwise or, at MDwise's direction or as required under Section 13405(c)(3) of the HITECH Act, to the individual (or the individual's personal representative).

ii. Exceptions from Disclosure Tracking. Business Associate need not record disclosure information or otherwise account for disclosures of Protected Health Information that this Addendum or MDwise in writing permits or requires made (A) for the purpose of MDwise's treatment activities, payment activities or health care operations, unless MDwise is required to account for such information under Section 13405(c) of the HITECH Act, (B) to the individual who is the subject of the Protected Health Information disclosed or to that individual's personal representative; (C) to persons involved in that individual's health care or payment for health care; (D) for notification for disaster relief purposes, (E) for national security or intelligence purposes, (F) to law enforcement officials or correctional institutions regarding inmates, (G) incident to use or disclosure otherwise permitted or required in 45 Code of Federal Regulations § 164.502, (H) pursuant to an authorization as provided in 45 C.F.R. § 164.502 or (I) as part of a limited data set in accordance with 45 C.F.R. § 164.514(e).

iii. Disclosure Tracking Time Periods. Business Associate must have available for MDwise the disclosure information required by Section 3(c)(i) for the six (6) years preceding MDwise's request for the disclosure information, or such other time period as prescribed by applicable law.

d. **Restriction Agreements and Confidential Communications.** Business Associate will comply with any agreement that MDwise makes that either (i) restricts use or disclosure of Protected Health Information pursuant to 45 C.F.R. § 164.522(a) or Section 13405(a) of the HITECH Act or (ii) requires confidential communication about Protected Health Information pursuant to 45 C.F.R. § 164.522(b), provided that MDwise notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. MDwise will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of MDwise's Protected Health Information will remain subject to the terms of the restriction agreement.

e. **Inspection of Books and Records.** Business Associate will make its internal practices, books and records, relating to its use and disclosure of the Protected Health Information it creates or receives for or from MDwise, available to MDwise and to the U.S. Department of Health and Human Services to determine compliance with 45 C.F.R. Parts 160-164 or this Addendum.

4. **Breach of Privacy and Security Obligations.**

a. **Reporting.** Business Associate will report to MDwise in writing any acquisition, access, use or disclosure of Protected Health Information not permitted by this Addendum (a "Breach"), and shall otherwise take such necessary actions as required by 45 C.F.R. 164.510. Business Associate will make the report to MDwise within 24 hours after Business Associate knows or should have reasonably known of such Breach. Business Associate will cooperate promptly with MDwise as is reasonably required in order for MDwise to comply with applicable breach reporting and notification laws, including, but not limited to, applicable Sections of HIPAA and Section 13402 of the HITECH Act (collectively, "Breach Notification Laws"). Business Associate shall reimburse MDwise for all costs incurred by MDwise to comply with Breach Notification Laws as a result of Business Associate's failure to comply with any provision of this Addendum or applicable law, including, but not limited to fines, outside counsel fees related to dealing with the Breach and any related inquiries by regulators, remediation efforts, public relations costs, judgments, settlements, and enforcement and inspection costs. Further, at MDwise's sole discretion, Business Associate shall be liable for all costs and expenses related to obtaining and providing twelve (12) months of credit monitoring services from a vendor approved by MDwise for every individual impacted by the Breach. Business Associate's report will at least:

i. Identify the nature of the Breach;

ii. Identify the individuals (by full name and address) whose Protected Health Information was subject to the Breach and the total number of affected individuals;

iii. Identify the Protected Health Information subject to the Breach;

iv. Identify who committed the Breach and who acquired, accessed, used or received Protected Health Information that was subject to the Breach;

v. Identify what corrective action Business Associate took or will take to prevent further Breaches;

vi. Identify what Business Associate did or will do to mitigate any deleterious effect of the Breach; and

vii. Provide such other information as MDwise may reasonably request.

b. **Termination of Agreement.**

i. Right to Terminate for Breach. MDwise may terminate the Agreement and this Addendum if it determines, in its sole discretion, that Business Associate has breached any provision of this Addendum. MDwise may exercise this right to terminate the Agreement and this Addendum by providing Business Associate written notice of termination, stating the breach of the Addendum that provides the basis for the termination. Any such termination will be effective immediately or at such other date specified in the notice of termination.

ii. Obligations upon Termination.

A. Return or Destruction. Upon termination, cancellation, expiration or other conclusion of the Agreement and this Addendum, Business Associate will, if feasible, return to MDwise or destroy all Protected Health Information, in whatever form or medium (including in any electronic medium under Business Associate's custody or control), that Business Associate created or received for or from MDwise, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the Protected Health Information. Business Associate will complete such return or destruction as promptly as possible, but not later than thirty (30) days after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement and this Addendum. Business Associate will identify any Protected Health Information that Business Associate created or received for or from MDwise that cannot feasibly be returned to MDwise or destroyed, and will limit its further use or disclosure of that Protected Health Information to those purposes that make return or destruction of that Protected Health Information infeasible. Within thirty (30) days after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement and this Addendum, Business Associate will certify on oath in writing to MDwise that such return or destruction has been completed, will deliver to MDwise the identification of any Protected Health Information for which return or destruction is infeasible and, for that Protected Health Information, will certify that it will only use or disclose such Protected Health Information for those purposes that make return or destruction infeasible.

B. Continuing Privacy Obligation. Business Associate's obligation to protect the privacy of the Protected Health Information it created or received for or from MDwise will be continuous and survive termination, cancellation, expiration or other conclusion of the Agreement and this Addendum.

C. Other Obligations and Rights. Business Associate's other obligations and MDwise's other rights upon termination, cancellation, expiration or other conclusion of the Agreement will be those set forth in the Agreement.

c. **Indemnity.** Business Associate will indemnify and hold harmless MDwise and any MDwise affiliate, officer, director, employee or agent from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted or violating use or disclosure of Protected Health Information or other breach of this Addendum by Business Associate or any subcontractor, agent, person or entity under Business Associate's control or acting at Business Associate's request.

i. Right to Tender or Undertake Defense. If MDwise is named a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or violating use or disclosure of Protected Health Information or other breach of this Addendum by Business Associate or any subcontractor, agent, person or entity under Business Associate's control or acting at Business Associate's request, MDwise will have the option at any time either (A) to tender its defense to Business Associate, in which case Business Associate will provide qualified attorneys, consultants and other appropriate professionals to represent MDwise's interests at Business Associate's expense or (B) undertake its own defense, choosing the attorneys, consultants and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants and other professionals as those fees are incurred.

ii. Right to Control Resolution. MDwise will have the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that MDwise may have tendered its defense to Business Associate. Any such resolution, or MDwise's failure to consent to any proposed settlement, compromise or other resolution, will not relieve Business Associate of its obligation to indemnify MDwise as provided in this Addendum.

5. **General Provisions.**

a. **Definitions.** The capitalized terms "Privacy Standards" and "Security Standards" shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for Health Information set out in 45 C.F.R. Parts 160 and 164, as amended. The capitalized terms "Protected Health Information," "Standard" and "Transaction" have the meanings set out in 45 C.F.R. § 160.103. Terms used, but not otherwise defined, in this Addendum shall have the same meanings as those terms in the Privacy Standards, the Security Standards or the HITECH Act. The parties recognize that the enactment of the HITECH Act and planned implementing regulations and guidance could change the definitions of the defined terms used in the Addendum. It is the parties' intent to comply with such revised or amended definitions as of the applicable compliance date specified in any amending regulations.

b. **Amendment to Agreement.** Upon the effective date of any final regulation or amendment to final regulations promulgated by HHS with respect to Protected

Health Information or Standard Transactions, this Addendum and the Agreement of which it is part will automatically amend the obligations they impose on Business Associate to remain in compliance with these regulations.

6. **Conflicts.** The terms and conditions of this Addendum will override and control any conflicting term or condition of the Agreement. All non-conflicting terms and conditions of the Agreement remain in full force and effect.

[REMAINDER OF PAGE INTENTIONALLY BLANK;
SIGNATURES ON FOLLOWING PAGE]

IN WITNESS WHEREOF, MDwise and Business Associate have caused this Addendum to be signed and delivered by their authorized representatives, effective as of the Effective Date of the Agreement.

Business Associate	**MDwise, Inc.**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____