

HIPAA Guide for Contractors

SECTION 1. HIPAA COMPLIANCE

The Contractor is considered a “Business Associate,” as that term is used in the Privacy Rule and Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and it shall comply with all standards applicable to a Business Associate under such rules. The Contractor and its employees and agents have an obligation to adequately safeguard the information (in whatever form it is maintained or used, including verbal communications) from inappropriate or unauthorized use or disclosure; provide individuals access to their records; and strictly limit use and disclosure of the information for only those purposes approved of by the Office of Medicaid. Copies of signed confidentiality forms must be provided to the Broker (MART).

Section 1.1 Definitions

All terms used but not otherwise defined in this contract shall be construed in a manner consistent with the Privacy Rule, the Security Rule, and other applicable state or federal confidentiality or data security laws.

- A. Commonwealth Security Information. “Commonwealth Security Information” shall mean all data that pertains to the security of the Commonwealth’s information technology, specifically, information pertaining to the manner in which the Commonwealth protects its information technology systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats.
- B. Individual. “Individual” shall mean the person who is the subject of the Protected Information, and shall include a person who qualifies as a personal representative in accord with 45 CFR § 164.502 (g).
- C. Privacy Rule. “Privacy Rule” shall mean the Standards of Privacy of Individually Identifiable Health Information, at 45 CFR Parts 160 and 164.
- D. Protected Information. “Protected Information” shall mean any “Personal Data” defined in Mass. Gen. Laws ch. 66A and any “Protected Health Information” as defined in the Privacy Rule, that the Contractor creates, receives, obtains, uses, maintains, or discloses under this Contract.
- E. Secretary. “Secretary” shall mean the Secretary of the US Department of Health and Human Services or the Secretary’s designee.
- F. Security Incident. “Security Incident” shall have the same meaning as used in the Security Rule.
- G. Security Rule. “Security Rule” shall mean the Security Standards for the Protections of Electronic Protected Health Information, at 45 CFR Parts 160, 162, and 164.

Section 1.2 Contractor’s Obligations

- A. The Contractor acknowledges that in the performance of this Contract it will become a “Holder” of “Personal Data,” as such terms are used within Mass. Gen. Laws ch. 66A. The Contractor agrees that, in a manner consistent with the Privacy Rule and the Security Rule, as applicable, it shall comply with Mass. Gen. Laws ch. 66A and any other applicable state or federal law governing the privacy or security of any data created, received, obtained, used, maintained, or disclosed under this Contract.

- B. The Contractor acknowledges that in the performance of this Contract it is MART's Business Associate, as that term is used in the Privacy Rule and Security Rule, and that it shall comply with all standards applicable to a Business Associate under such rules.
- C. At all times, the Contractor shall recognize MART's right to control access, use, disclosure, and disposition of all data created, obtained, received, used, maintained, or disclosed under this Contract, including all PI, and any data derived or extracted from such data.
- D. The Contractor shall not use or disclose PI other than as permitted or required by this **Section 8** or as Required By Law, consistent with the restrictions of 42 CFR 431.306 (f), Mass. Gen. Laws ch. 66A, any other applicable federal or state privacy or security law.
- E. The Contractor shall ensure that any agent or subcontractor to whom it provides PI received from, or created or received by it on behalf of MART agrees in writing to the same restrictions and conditions that apply to the Contractor under this **Section 8** with respect to such information, including but not limited to implementing reasonable safeguards to protect such information. The Contractor is solely responsible for its agents' and subcontractors' compliance with all provisions of this **Section 8**. The Contractor is not relieved of any obligation under this **Section 8** because PI was in the hands of its agent or subcontractor or because its agent or subcontractor failed to fulfill any reporting obligation to it necessary for the Contractor to fulfill its reporting obligations hereunder.
- F. The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PI, and that meet, at a minimum, all standards set in the Privacy and Security Rules, as applicable to a business associate. The Contractor's safeguards must include a prohibition restricting all employees and agents from transmitting PI in non-secure transmissions over the Internet or any wireless communication device. The Contractor shall comply with all security mechanisms and processes established for access to any of MART's databases, as well as all Commonwealth security and information technology resource policies, processes and mechanisms established for access to PI. The Contractor shall protect from inappropriate use or disclosure any password, user ID, or other mechanism or code permitting access to any database containing MART PI, and shall give MART prior notice of any change in personnel whenever the change requires a termination or modification of any such password, user ID, or other security mechanism or code to maintain the integrity of the database. Upon MART's request, the Contractor shall permit representatives of MART or EOHHS access to premises where PI is maintained, created, used, or disclosed for the purpose of inspecting privacy and security arrangements.
- G. Immediately upon becoming aware of any use or disclosure of PI not permitted under this Contract or of any Security Incident, the Contractor shall take all appropriate action necessary to: 1) retrieve, to the extent practicable, any PI used or disclosed in the non-permitted manner or involved in the Security Incident, 2) mitigate, to the extent practicable, any harmful effect of the non-permitted use or disclosure of the PI or of the Security Incident known to the Contractor, and 3) take such further action as may be required by any applicable state or federal law concerning the privacy and security of such PI. Within two business days of becoming aware of the non-permitted use or disclosure, the Contractor shall report to MART, both verbally and in writing, the nature of the non-permitted use or disclosure, the harmful effects known to the Contractor, all actions it has taken or plans to take in accord with this paragraph, and the results of all mitigation actions already taken by it under this paragraph. Upon MART request, the Contractor shall take such further actions as deemed appropriate by MART to mitigate, to the extent practicable, any harmful effect of the non-permitted use or disclosure. Any actions to mitigate harmful effects of privacy or security violations undertaken by the Contractor on its own initiative or pursuant to MART's request under this paragraph shall not relieve the Contractor of its obligations to report such violations as set forth in other provisions of this Contract.

- H. If during the term of this Contract, the Contractor obtains access to any Commonwealth Security Information, the Contractor is prohibited from making any disclosures of or about such information, unless in accord with the express written instructions of MART. If the Contractor is granted access to such information in order to perform its obligations under this Contract, the Contractor may only use such information for the purposes for which it obtained access. In using the information for such permitted purposes, the Contractor shall limit access to the information only to staff or agents necessary to perform the permitted purposes. While in possession of such information, the Contractor shall apply all privacy and security requirements set forth in this **Section 8**, as applicable to maintain the confidentiality, security, integrity, and availability of such information. Notwithstanding any other provision in this **Section 8**, the Contractor shall report any non-permitted use or disclosure of such information to MART immediately within twenty-four hours. The Contractor shall immediately take all reasonable and legal actions to retrieve such information if disclosed to any non-permitted individual or entity; shall include a summary of such retrieval actions in its required report of the non-permitted disclosure; and shall take such further retrieval action as MART or EOHHS shall require. Notwithstanding **Section 8.6** below, the Contractor may not retain any Commonwealth Security Information upon termination of this Contract, unless such information is expressly identified in any retention permission granted in accord with **Section 8.6.B**. If retention is expressly permitted, all data protections stated herein survive termination of this Contract and shall apply for as long as the Contractor retains the information.
- I. The Contractor shall immediately report to MART, both verbally and in writing, any instance where PI or any other data obtained under this Contract is requested, subpoenaed, or becomes the subject of a court or administrative order or other legal process. If MART directs the Contractor to respond to such requests, the Contractor shall take all necessary legal steps to comply with Mass. Gen. Laws ch. 66A, Medicaid regulations including 42 CFR 431.306 (f), and any other applicable federal and state law. If MART determines that it shall respond or challenge such requests directly, the Contractor shall fully cooperate and assist MART in its response or challenge. In no event shall the Contractor's immediate reporting obligations under this paragraph be delayed beyond the return date in such request or two business days from obtaining such knowledge or request for data, whichever is shorter.
- J. The Contractor shall provide MART, or upon MART's request, the Individual, with access to or copies of any PI maintained by it, as shall be necessary for MART to meet its obligation under 45 CFR § 164.524 to provide an Individual with access to certain PI pertaining to the Individual. Such access or copies shall be provided to MART or to the Individual at a reasonable time and manner to be specified by MART in the request and as shall be necessary for MART to meet all time and other requirements set forth in 45 CFR § 164.524. In the event the Contractor receives a request for access directly from an Individual, the Contractor shall, within two business days of receipt of such request, notify MART and proceed in accord with this paragraph.
- K. The Contractor shall make any amendment(s) to PI that MART requests in order for MART to meet its obligations under 45 CFR § 164.526. Such amendments shall be made promptly in a manner specified in, and in accord with any time requirement under, 45 CFR § 164.526. In the event the Contractor receives a request for amendment directly from the Individual, the Contractor shall, within two business days of receipt of such request, notify MART, and shall only make any amendment in accord with MART's instructions.
- L. The Contractor shall document all disclosures of PI, and required information related to such disclosures, as would be necessary for MART to respond to a request by an Individual for an accounting of disclosures of PI and related information in accord with 45 CFR § 164.528. In the event the Contractor receives a request for an accounting directly from an Individual, the Contractor shall, within two business days of receipt of such request, notify MART and proceed in accord with this paragraph. Within 10 business days of MART's request, the Contractor shall make a listing of

such disclosures and related information available to MART or upon MART's direction to the Individual.

- M. The Contractor shall make its internal practices, books, and records, including policies and procedures and PI, relating to the use and disclosure of PI received from, or created or received by it on behalf of MART, available to MART in a time and manner designated by MART for purposes of determining MART's compliance with the Privacy Rule.
- N. The Contractor shall designate a person, who shall act as custodian of PI and all other data obtained under this Contract, and who shall oversee the Contractor's compliance with this **Section 8**. The Contractor shall provide MART with the name of such custodian within fifteen days of the effective date of this **Section 8**, and thereafter within fifteen days of any transfer of this duty to another person within its organization.

Section 1.3 Permitted Uses and Disclosures by the Contractor

Except as otherwise limited in this Contract, the Contractor may only use or disclose PI to perform functions, activities, or services for, or on behalf of, MART as specified in this Contract, provided such use or disclosure would not violate the Privacy Rule if done by MART or not violate the minimum necessary policies and procedures of MART. In performing functions, activities, or services for or on behalf of MART, the Contractor represents that it will only request from MART an amount of PI that it reasonably believes is the minimally necessary to perform the function, activity, or service for which it is needed under this Contract and to the extent this Contract authorizes the Contractor to request PI from other covered entities on MART's behalf, the Contractor shall only request an amount of PI that it reasonably believes is the minimally necessary to perform the function, activity, or service for which the PI is needed under this Contract.

Section 1.4 Obligations of MART

- A. MART shall notify the Contractor of any limitation(s) in its notice of privacy practices issued in accord with 45 CFR § 164.520, to the extent that such limitation may affect the Contractor's use or disclosure of PI.
- B. MART shall notify the Contractor of any changes in, or revocation of, permission by Individual to use or disclose PI, to the extent that such changes may affect the Contractor's use or disclosure of PI.
- C. MART shall notify the Contractor of any restriction to the use or disclosure of PI that it has agreed to in accord with 45 CFR § 164.522, to the extent that such restriction may affect Contractor's use or disclosure of PI.

Section 1.5 Termination

- A. Notwithstanding any other provision in this Contract, MART may terminate this Contract, immediately upon written notice, if MART determines, in its sole discretion, that the Contractor has materially breached any of its obligations set forth in this **Section 8** or any other provision of this Contract pertaining to the security and privacy of any PI provided to the Contractor under this Contract.
- B. Prior to terminating this Contract as permitted above, MART **may** provide an opportunity for the Contractor to cure the breach or end the violation. If such an opportunity is provided, but cure is not feasible, or the Contractor fails to cure the breach or end the violation within a time period set by MART, MART may terminate the Contract immediately upon written notice.

- C. In the event that termination of this Contract for a material breach of any obligation regarding PI is not feasible, or if cure is not feasible, MART shall report such breach or violation to EOHHS.

Section 1.6 Effect of Termination

- A. Except as provided immediately below in subsection (B), upon termination of this Contract for any reason whatsoever, the Contractor shall, at MART's option, either return or destroy all PI and other data obtained or created in any form under this Contract, and the Contractor shall not retain any copies of all such PI and data in any form. This provision shall apply to all PI and other data in the possession of the Contractor's subcontractors or agents, and the Contractor shall ensure that all such PI and data in the possession of its subcontractors or agents has been returned or destroyed and that no subcontractor or agent retains any copies of such PI and data in any form. In no event shall the Contractor destroy any PI or other data without first obtaining MART's approval.
- B. If the Contractor determines that returning or destroying PI or other data is not feasible, the Contractor shall provide MART with written notification of the conditions that make return or destruction not feasible. If based on the Contractor's representations, MART concurs that return or destruction is not feasible and permits the Contractor to retain such data, the Contractor shall extend all protections set forth in this Contract to all such PI or data and shall limit further uses and disclosures of such data to those purposes that make the return or destruction of such data not feasible, for as long as the Contractor maintains the PI and other data.
- C. Notwithstanding any other provision concerning the term of this Contract, all protections pertaining to any PI or other data covered by this Contract shall continue to apply until such time as all such PI and data is returned to MART or destroyed, or if return or destruction is not feasible, protections are applied to such PI and data in accord with subsection (b) immediately above.

Section 1.7 Miscellaneous Provisions

- A. **Regulatory References.** Any reference in this Contract to a section in the Privacy or Security Rules or other regulation or law refers to that section as in effect or as amended.
- B. **Amendment.** The Contractor agrees to take such action as is necessary to amend this Contract in order for MART to comply with any requirements of the Privacy or Security Rules, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA), and any other applicable law pertaining to the privacy, confidentiality, or security of PI or other data. Upon MART's request, the Contractor agrees to enter promptly into negotiations for any amendment as MART, in its sole discretion deems necessary for MART's compliance with any such laws. The Contractor agrees that, notwithstanding any other provision in this Contract, MART may terminate this Contract immediately upon written notice, in the event the Contractor fails to enter into negotiations for, and to execute, any such amendment.
- C. **Waiver.** Nothing in this Contract shall be construed to waive or limit any of MART's legal rights or remedies which may arise from the Contractor's unauthorized use or disclosure of any PI or other data received by it under this Contract. MART's exercise or non-exercise of any authority under this Contract, including for example any rights of inspection or approval of privacy or security practices or approval of subcontractors, shall not relieve the Contractor of any obligations set forth herein, nor be construed as a waiver of any of the Contractor's obligations or as an acceptance of any unsatisfactory practices or privacy or security failures or breaches by the Contractor.
- D. **Interpretation.** Any ambiguity in this Contract shall be resolved to permit MART to comply with the Privacy or Security Rules, HIPAA, and any other applicable law pertaining to the privacy, confidentiality, or security of PI or other data.