Department of Defense (DoD) Business Associate Agreement (BAA)

Introduction

In accordance with 45 CFR §§164.502(e)(2), 164.504(e); the Health Information Technology for Economic and Clinical Health (HITECH) Act; and paragraph 3.3.c. of Department of Defense Manual (DoDM) 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, and Chapter 1, Section 5 of the TRICARE Operations Manual, this document serves as a Business Associate Agreement (BAA) between the executing parties for purposes of the Health Insurance Portability and Accountability Act (HIPAA) as implemented by the HIPAA Rules and Department of Defense (DoD) HIPAA Issuances (as defined below). The parties are a DoD Component, acting as a HIPAA Covered Entity, and a Business Associate (i.e., a DoD Contractor creates, receives, maintains, and/or transmits protected health information (PHI) for the purpose of performing covered functions on behalf of the DoD Component). The HIPAA Rules (as defined below) require BAAs between covered entities and business associates. As such, this BAA implements and incorporates the applicable DoD HIPAA Issuances (including DoDI 6025.18 and the authorities incorporated therein) and provides the Business Associate requirements which apply to the relevant Business Associates contract or other agreement between the parties.

(a) **Catchall Definition**:: Except as otherwise provided in this BAA, the following terms used in this BAA shall have the same meaning as those terms in the DoD HIPAA Issuances : Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), PHI,, Required by Law, Secretary of HHS, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(b) **Specific definitions**:

Agreement means this BAA together with the documents and/or other arrangements under which the Business Associate signatory performs services involving access to PHI on behalf of the DoD component signatory.

Breach means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses personally identifiable information; or (2) an authorized user accesses or potentially accesses Personally Identifiable Information (PII) for an other than authorized purpose. The foregoing definition is based on the definition of breach in Office of Management and Budget (OMB) Memorandum M-17-12.

Business Associate shall generally have the same meaning as the term "Business Associate" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean *[insert name of the non-federal Business Associate entity/signatory to this BAA]*.

Covered Entity shall generally have the same meaning as the term "covered entity" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean *[insert name of the DoD Component entity/DoD signatory to this BAA].*

Covered Functions are functions of a covered entity, the performance of which makes the entity a health plan or health care provider as outlined in DoDM 6025.18.

Defense Health Agency (DHA) Privacy Office means the DHA Privacy and Civil Liberties Office, with the responsibilities and authorities as outlined in DoDM 6025.18. The Chief of the DHA Privacy Office is the HIPAA Privacy and Security Officer for DHA.

DoD HIPAA Issuances means all DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances include DoDM 6025.18 (2019), Department of Defense Instruction (DoDI) 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019; and DoDI 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015.

DoD Privacy Program Issuances means the current DoD issuances implementing within DoD the Privacy Act and certain privacy-related authorities, as identified by DHA Privacy Office Guidance. These issuances are DoDI 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, DoDM 5400.11, Volume 2 "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021 and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007. These issuances are available on the Washington Headquarters Services DoD Directives website (https://www.esd.whs.mil/DD/) or upon request.

Department of Health and Human Services (HHS) Breach means a breach that satisfies the HIPAA Breach Rule definition of breach found in 45 CFR §164.402.

HIPAA Rules means the regulations issued by HHS pursuant to its authority to issue regulations on health information privacy, as provided by Section 264(c) of HIPAA. The HIPAA Rules, as amended by the Omnibus Final Rule, include the HIPAA Privacy Rule, the HIPAA Breach Rule, the HIPAA Security Rule, and the HIPAA Enforcement Rule.

I. Obligations and Activities of the Business Associate

(a) The Business Associate shall not use or disclose PHI other than as permitted or required by the Agreement or as required by law.

(b) The Business Associate shall use appropriate safeguards, and comply with the HIPAA Rules and DoD HIPAA Issuances incorporated by reference in this document Issuances with respect to PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement.

(c) The Business Associate shall report to the Covered Entity any breach of which it

becomes aware, and shall proceed with breach response steps as required by Part V of this agreement. With respect to electronic PHI, the Business Associate shall also respond to any security incident of which it becomes aware in accordance with any cybersecurity provisions of the Agreement. If at any point the Business Associate becomes aware that a security incident involves a breach, the Business Associate shall immediately initiate breach response as required by PartV of this BAA.

(d) In accordance with DoDM 6025.18, paragraph 3.3.c.(3)(b)4, 45 CFR §164.502(e)(1)(ii)) and §164.308(b)(2),the Business Associate shall ensure that any (and all) subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to PHI, specifically the responsibilities laid out in the DoD HIPAA Issuances incorporated by reference in this agreement. PHI.

(e) The 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, in accordance with DoDM 6025.18, paragraph 4.5.e.(1), that the subcontractor will appropriately safeguard the information.

(f) The Business Associate shall make available PHI in a Designated Record Set, to the Covered Entity or, as directed by the Covered Entity, to an Individual, as necessary to satisfy the Covered Entity obligations under 45 CFR §164.524 and DoDM 6025.18, paragraph 5.3.c.

(g) The Business Associate shall make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR § and DoDM 6025.18, paragraph 5.4.

(h) The Business Associate shall maintain and make available the information required to provide an accounting of disclosures to the Covered Entity or an individual as necessary to satisfy the Covered Entity’s obligations under 45 CFR §164.528 and DoDM 6025.18, paragraph 5.5.

(i) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the HIPAA Privacy Rule and DoDM 6025.18, the Business Associate shall comply with the requirements of the HIPAA Privacy Rule and DoDM 6025.18, that apply to the Covered Entity in the performance of such obligation(s); and

(j) The Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI from, or created or received by the Business Associate on behalf of, the DoD Component available to the Secretary of HHS and to the Director, DHA, or their designee for purposes of determining compliance with the HIPAA Rules.

II. Permitted Uses and Disclosures by Business Associate

(a) The Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Agreement or as required by law. The Business Associate is not permitted

to de-identify PHI, nor is it permitted to use or disclose de-identified PHI, except as provided by the Agreement or directed by the Covered Entity with written approval from DHA's HIPAA Privacy Officer.

(b) The Business Associate agrees to use, disclose, and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances.

(c) The Business Associate shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances if done by the Covered Entity.

(d) Except as otherwise limited in the Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

(e) Except as otherwise limited in the Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f) Except as otherwise limited in the Agreement, the Business Associate may use PHI to provide Data Aggregation services relating to the Covered Entity's health care operations.

III. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) The Covered Entity shall provide the Business Associate with NoPP that the Covered Entity produces in accordance with 45 CFR §164.520 and DoDM 6025.18, paragraph 5.1.

(b) The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes affect the Business Associate's use or disclosure of PHI.

(c) The Covered Entity shall notify the Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR §164.522 and DoDM 6025.18, paragraph 5.2, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

IV. Permissible Requests by Covered Entity

The Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule or any applicable Federal regulations (including without limitation, DoD HIPAA Issuances) if done by the Covered Entity.

V. Breach Response

(a) In general.

In the event of a breach of PII/PHI held by the Business Associate, the Business Associate shall follow the breach response requirements set forth in this Part V, which is designed to satisfy both the Privacy Act and HIPAA breach response requirements, as applicable. If a breach involves PII without PHI, then the Business Associate shall comply with DoD Privacy Program Issuances breach response requirements only. If a breach involves PHI (a subset of PII), then the Business Associate shall comply with DoD Privacy Program Issuances breach response requirements. A breach involving PHI may or may not constitute a HHS Breach. If a breach is not an HHS Breach, then the Business Associate has no HIPAA breach response obligations. In such cases, the Business Associate must still comply with breach response requirements under the DoD Privacy Program Issuances.

If the DHA Privacy Office determines that a breach is an HHS Breach, then the Business Associate shall comply with both the HIPAA Breach Rule and DoD Privacy Program Issuances, as directed by the DHA Privacy Office. If the DHA Privacy Office determines that the breach does not constitute an HHS Breach, then the Business Associate shall comply with DoD Privacy Program Issuances. The following provisions of Part V set forth the Business Associate's Privacy Act and HIPAA breach response requirements for all breaches, including but not limited to HHS breaches.

In general, for breach response, the Business Associate shall report the breach to the Covered Entity. Such breach shall be reported to the DHA Privacy Office within 24 hours at 703-275-6363 or dha.privacyofficer@mail.mil. If such breach is a cybersecurity incident, an incident involving damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, electronic communication, including information contained therein, ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of data, as defined in Committee on National Security Systems Instruction (CNSSI) 4009 https://www.cnss.gov/CNSS/issuances/Instructions.cfm, the discovering party shall report the breach to the DHA NIWC CSSP Watchdesk by dialing 1.866.786.4432 Cybersecurity and Infrastructure Security Agency potential-CERT) within one hour of the potential cybersecurity incident. The DHA NIWC CSSP Watchdesk reports, and report to USCYBERCOM within 48 hours of being notified of the occurrence of a breach, and complete the breach response actions as required by DHA guidance https://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI?type=Policies#RefFeed.

The Business Associate is deemed to have discovered a breach as of the first day a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the Business Associate.

The Business Associate shall submit a report to the U.S. Computer Emergency Readiness Team (US-CERT), using the US-CERT report online form at https://us-cert.cisa.gov/forms/reporthttps://us-cert.cisa.gov/forms/report. Before submission to US-CERT, the Business Associate shall save a copy of the on-line report. After submission, the Business Associate shall record the US-CERT Reporting Number. Although only limited information about the breach may be available as of the one-hour deadline for submission, the Business Associate shall submit the US-CERT report by the deadline. The Business Associate shall e-mail updated information to the Covered Entity as it is obtained. The Business Associate shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office. Business Associate general questions about US-CERT reporting shall be directed to the DHA Privacy Office not the US-CERT office.

Additionally, the Business Associate will send to the DHA Privacy Office a completed Breach Report Form Report DD 2959 at https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2959.pdf. Encryption is not required, because Breach Report Forms must not contain PII/PHI.

If multiple individuals are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The Business Associate shall inform the DHA Privacy Office as soon as possible if it believes that a "single event" breach response is appropriate. The DHA Privacy Office will determine how the Business Associate shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Business Associate report updates, individual notification, and mitigation.

When an initially submitted Breach Report Form is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Business Associate shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions by denoting "UPDATE." Examples of updated information the Business Associate shall report include but are not limited to: confirmation on the exact data elements involved, the root cause of the incident, and any mitigation actions,, including sanctions, training, incident containment, follow-up, etc. The Business Associate shall submit these report updates promptly after the new information becomes available. Prompt reporting of updates is required to allow the DHA Privacy Office to make timely final determinations on any subsequent notifications or reports. The Business Associate shall provide updates to the same parties as required for the initial Breach Reporting Form. The Business Associate is responsible for reporting all information needed by the DHA Privacy Office to enable timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy, Civil Liberties, and Transparency Division as required by DoD Privacy Program Issuances.

(b) Individual Notification Provisions

If the DHA Privacy Office determines that individual notification is required IAW 5 CFR §§ 164.400-414, the Business Associate shall provide written notification to individuals affected by the breach as soon as possible, but no later than ten working days after the breach is discovered

and the identities of the individuals are ascertained. The ten-day period begins when the Business Associate determines the identities (including addresses) of the individuals whose records were affected.

The Business Associate's proposed notification to be issued to the affected individuals shall be submitted for approval to the DHA Privacy Office. Upon request, the Business Associate shall provide the DHA Privacy Office with the final text of the notification letter sent to the affected individuals. PII shall not be included with the text of the letter(s) provided.. Copies of further correspondence with affected individuals need not be provided unless requested by the DHA Privacy Office. Pursuant to 45 CFR §§ 164.400-414 and section 13407 of the HITECH Act, the Business Associate's notification to the individuals, at a minimum, shall include the following:

—The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual of the nature and extent of any potentially PHI data elements that have been breached. In all cases, individuals should be notified as to the nature and extent of any compromised PHI.

—The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so that the individual clearly understands how the breach occurred.

—The individual(s) must be informed of any steps the individuals should take to protect themselves from potential harm resulting from the breach.

—The individual(s) must be informed of what protective actions the Business Associate is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); Teletype (TTY):): 1-866- 653-4261.

—The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) that the Business Associate may offer affected individuals, the process to follow to obtain those services, and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information.

Business Associates shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the Business Associate and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated point of contact (POC),), phone number, email address, and postal address.

If the Business Associate determines that it cannot readily identify, or will be unable to reach, some affected individuals within the ten-day period after discovering the breach, the Business Associate shall so indicate in the initial or updated Breach Report Form. Within the 10-day period, the Business Associate shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within ten days after their identities and addresses are ascertained. The Business Associate shall consult with the DHA Privacy Office, which will determine which media notice is most likely to reach the population not otherwise identified or reached. The Business Associate shall issue a generalized media notice(s) to that population in accordance with DHA Privacy Office approval.

The Business Associate shall, at no cost to the government, bear all costs associated with a breach of PII/PHI that the Business Associate has caused or is otherwise responsible for addressing.

VI. Termination

(a) Termination. Noncompliance by the Business Associate (or any of its staff, agents, or subcontractors) with any requirement addressed in this BAA may subject the Business Associate to termination under any applicable default or other termination provision of the Agreement.

(b) Effect of Termination.

(1) If the Agreement has records management requirements, the Business Associate shall handle such records in accordance with the records management requirements. If the Agreement does not have records management requirements, the records shall be handled in accordance with paragraphs (2) and (3) below, unless the Agreement has provisions for transfer of records and PII/PHI to a successor Business Associate, or if DHA gives directions for such transfer. In the case DHA or the Agreement provides for transfer of records, the Business Associate shall handle such records and information in accordance with such Agreement provisions or DHA direction.

(2) If the Agreement does not have records management requirements, except as provided in the following paragraph (3), upon termination of the Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the PHI or its derivatives.

(3) If the Agreement does not have records management provisions and the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Covered Entity and the Business Associate that return or destruction of PHI is infeasible, the Business

Associate shall extend the protections of the Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

VII. Execution

(a) Survival. The obligations of Business Associate under the "Effect of Termination" provision of this BAA shall survive the termination of the Agreement or any part thereof.

(b) Interpretation. Any ambiguity in the Agreement shall be resolved in favor of a meaning that permits the DoD Component and the Business Associate to comply with the HIPAA Rules and the DoD HIPAA Rules.

_____	_____
[Business Associate]	[DoD Covered Entity]
_____	_____
Date	Date