DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

INFO MEMO

March 19, 2020

FOR: GENERAL COUNSEL, DEPARTMENT OF DEFENSE

FROM: Salvatore M. Maida, Acting General Counsel, Defense Health Agency

SUBJECT: COVID-19 and HIPAA

Given the impact of COVID-19 on the Federal workplace, the following general guidance on HIPAA and the Privacy Act is provided with respect to the issues that are most likely to present themselves. Following this guidance will ensure that the Department of Defense provides consistent advice on this subject.

- General Rule:

  The HHS HIPAA Privacy Final Rule is implemented in the Department of Defense by DoD Manual 6025.18 (March 13, 2019). In general, Protected Health Information (PHI) must not be disclosed by DoD covered entities or their business associates without patient authorization, except for specifically permitted or required purposes. A covered entity is defined as a health plan or a health care provider who transmits certain health information in electronic form. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI for a covered entity.

  HIPAA PHI release protections only apply to covered entities and their business associates. Once PHI is released to a third person or entity that is not another covered entity or a business associate, it is no longer covered by HIPAA and any subsequent release is not protected by the rule. If, however, the third person or entity receiving the information is a government entity, the information may be covered by the Privacy Act. (Refer to the below section on the Privacy Act.)

  There are very few covered entities or business associates within the Department of Defense outside of the Military Health System.

- Self-Reported Health Information:

  If an individual self-reports PHI to his or her employer, the information is not covered by HIPAA (e.g., Service member, civilian employee, or contractor employee reports to his or her supervisor that he or she has tested positive for COVID-19; it is not protected by HIPAA, but may be subject to the Privacy Act).

- Permitted Disclosures of PHI Without Patient Authorization by Covered Entities Relevant to COVID-19:

    1. Uses and Disclosures for Specialized Government Functions:

        A Department of Defense covered entity (and a covered entity not part of or affiliated with the Department of Defense) may use and disclose the PHI of individuals who are Service members for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.

        Appropriate command authorities include the Secretary of Defense, the Secretary of the Military Department responsible for the Service member, all commanders who exercise authority over the Service member, and any official delegated authority by one of the aforementioned Secretaries.

        This is very broad release authority and covers the release of COVID-19 PHI of Service members from a covered entity to a command authority. Once released to the command authority, any subsequent release by the command authority would not be covered under HIPAA. However, the subsequent release may be covered by the Privacy Act. (Refer to the below section on the Privacy Act.)

        This exception is only applicable to PHI of Service members; it does not apply to civilians in any capacity, including, but not limited to, civilian employees, contractor employees, and family members.

    2. Uses and Disclosures for Public Health Activities:

        A covered entity may use or disclose PHI for public health activities to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, including, but not limited to, the reporting of disease and the conduct of public health surveillance, public health investigations, and public health interventions. For example, if a civilian employee is tested by the covered entity, the covered entity may disclose PHI to the State Department of Health; the State Department of Health can use this information to contact those with whom the employee had close contact.

        A Department of Defense covered entity (e.g., an occupational health clinic) that provides health care to a Department of Defense civilian employee at the request of the employee's supervisor to evaluate whether the employee has a work-related illness can disclose PHI that consists of findings concerning that work-related illness or workplace-related medical surveillance.

3. Uses and Disclosures to Avert a Serious Threat to Health or Safety:

   A Department of Defense covered entity may use or disclose PHI if the Department of Defense covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat.

   This exception may be used for COVID-19 if the Department of Defense covered entity has a good faith belief that the person is positive for COVID-19 and engages in behavior that constitutes a serious and imminent threat to the health or safety of a person or the public (e.g., the person fails to follow applicable CDC guidance).

4. Disclosures of PHI must be limited to the information reasonably necessary to accomplish the purpose for which disclosure is sought.

- Privacy Act:

  1. To be subject to the Privacy Act, information must be contained within a "system of records," that is, groups of records "about individuals" under agency control that are retrieved by the individual's name or some other personal identifier. Department of Defense's system of records notices (SORNs) are available at https://dpcld.defense.gov/Privacy/SORNs/.

  2. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Privacy Act is implemented in Department of Defense by DoD 5400.11-R, Department of Defense Privacy Program (May 14, 2007), DoD Instruction 5400.11, DoD Privacy and Civil Liberties Programs (January 29, 2019), and 32 C.F.R. Part 310.

  3. Under the Privacy Act, records pertaining to an individual contained within a Department of Defense system of records may be disclosed to a Department of Defense official or employee provided the recipient has a need for the record in the performance of his or her assigned duties.

  4. In the absence of an individual's written consent, records pertaining to an individual contained within a Department of Defense system of records may only be disclosed outside of the Department of Defense if there is authority under one of the Privacy Act's other exceptions. One of the more common exceptions is a disclosure pursuant to a published routine use in the system of records notice that identifies the purpose of the disclosure and the category of recipient. Another exception (though infrequently invoked) permits disclosure outside of the agency if there has been a showing of

"compelling circumstances affecting the health or safety of an individual," provided that the record subject is also notified of the disclosure.

5. If information is not contained in a system of records, the Privacy Act would not apply.

- Best Practices:

1. Department of Defense entities informed that one of its Service members, civilian employees, or contractor employees have contracted COVID-19 (by notification from a covered entity, public health authority, or the employee directly) should only disclose personally identifiable information (PII) of the person to Department of Defense officials with a need to know. Such information should be disclosed in a secure manner (e.g., encryption).

2. If covered by the Privacy Act, disclosures outside of the Department of Defense will require either written consent of the individual or authority under one of the Privacy Act exceptions.

3. When notifying people who may have had close contact with the infected individual, Department of Defense officials must ensure proper authority exists for any release of PII (e.g., written consent of the individual, published routine use, etc. if Privacy Act applies).

This Information Paper covers the more common questions that are expected to arise. It is understood that more complex questions are likely to be presented. The Military Departments each have subject matter experts who may be contacted in that event; DoD components may contact the Defense Health Agency Office of General Counsel at (703) 681-6012 for additional guidance.

Prepared by: Salvatore M. Maida, (703) 681-6012