Privacy Protection of COVID-19 Information

Everyone's health and safety are paramount during this evolving COVID-19 situation.

All personally identifiable information (PII), including health information protected under the Privacy Act, maintained on DoD personnel and affiliated individuals, should be collected, used, and disclosed only as necessary to safeguard public health and safety in accordance with relevant privacy laws, regulations, and policies.

As a guiding principle, only collect and disclose the minimum amount of PII regarding COVID-19 necessary to persons with an authorized need to know. You should also actively seek to minimize the amount of data sharing so as to safeguard the PII for access by those persons with a need to know.

An example of PII is information contained on recall roster lists, such as names that are linked with phone numbers and email addresses. Another example of PII is an instance in which an employee reports a positive test result for COVID-19 to his or her supervisor. For these uses, this is not patient information, but is considered employment- and readiness-related information. Therefore, this information is not protected health information under the Health Insurance Portability and Accountability Act (HIPAA), but should be protected as PII consistent with the Privacy Act.

As we respond to COVID-19, employ best practices when handling PII to avoid privacy incidents, including the following:

- Limit distribution of PII to <u>those who have a valid, need to know</u>. For example:
    - If a DoD employee (military member or civilian) tests positive for COVID-19, they should <u>inform their supervisor immediately</u>. The supervisor will then notify the appropriate persons within the chain of command designated as need to know for COVID-19. This information along with any other related details, such as quarantine date(s), exposure date(s), duty status date(s), etc., will be provided only to persons with an authorized need to know
    - If a DoD employee self-identifies with a higher risk susceptibility to COVID-19, in accordance with CDC guidelines, the information should be reported to the supervisor and reporting limited to only those who have a <u>need to know</u>.
- Employ good data security practices, such as <u>encrypting email transmission of PII</u> on all classification systems (NIPR, SIPR, or JWICs). For example, a supervisor should not transmit names, social security numbers, personal phone numbers, or health or readiness status via unencrypted email.
- <u>Do not use personal email accounts to transmit PII</u>.
- <u>Do not use collaboration platforms to communicate PII</u>. For example, do not discuss or disclose an individual's current or potential COVID-19 status on a work-related blog or instant message system.
- <u>Do not post</u> recall rosters or excel spreadsheets with PII to internal shared drives, Share Point, or similar sites without proper safeguards and role-based access restrictions. This

will ensure only individuals within the designated chain of command with a need to know will be able to access the PII.

- HIPAA Rules do not apply to employment records, even if the information in those records is health-related, as the HIPAA does not apply to the actions of an employer. To the extent that you have questions about applicable law, consult your counsel.

If you have further questions or concerns about collecting, maintaining, processing, or disseminating PII (to include health information) please contact your Component Privacy Office.