HEALTH AND PERSONAL INFORMATION PROTECTION

Rhode Island employees and contractors have an obligation to secure **protected health information (PHI)** and **personally identifiable information (PII)** about individuals.

What is PHI?

PHI is health information about an individual protected by the Health Insurance Portability and Accountability Act – commonly known as HIPAA.

PHI is any health information that can identify an individual and relates to their past, present or future physical or mental health or condition, treatment, or payment for health care, that is created or received by or on behalf of a health care provider, health plan (insurance provider), or health care clearinghouse. PHI includes an individual's:

- Name, social security number, dates of birth, dates or details of diagnosis and/or treatment, or photograph;
- Street address (or elements of it, such as a city or zip code), email address, telephone or fax number, account number, or medical record number; or
- Information that can be combined with publicly available information to identify an individual (e.g., via Google or a newspaper).

There are limited exceptions to the definition of PHI, including for employment records, but **you should assume HIPAA applies to identifiable health information.** HIPAA continues to apply **for 50 years after the individual's death**.

HIPAA Notification Requirements

- ***Privacy***: PHI can only be accessed or shared for limited purposes without patient consent, including for public health and to prevent imminent threats. You can only use and share the minimum amount of PHI necessary to carry out permitted activities.
- ***Security****:* You are obligated to take steps to keep PHI confidential.

DO: Password protect your devices, send emails securely to known recipients, use encryption if available, and report any suspicions or breaches.
DO NOT: Leave health records in public places, send PHI to unknown or unnecessary recipients, text PHI, have no password or a simple password on your device, let others use your device, or keep security concerns or breaches to yourself.

- ***Breach***: If you suspect that anyone may have accessed a device, file or record containing PHI without authorization – including a fellow employee – you should **report it to your supervisor immediately by phone**.
    - This includes if you think you may have been the target of a virus or phishing attack, or if you lose or send any files containing PHI inadvertently.
    - If you send PHI or PII by mistake, you should alert the recipient, have them delete it and not further view or share the information, and report it immediately.

What is PII and How Can I Protect It?

PII refers to any individual's name (first name or initial + last name) in combination with: the individual's social security number, driver's license or other state or tribal identification number, financial account or card number, medical or health insurance information, or email address along with any password enabling access to a personal, medical, insurance or financial account.

PII should be protected in the same manner that you protect PHI, as described above.

Report any suspected breach or theft of PII due to hacking or a lost or stolen device to the Division of Information Technology. Report any suspected breach because of lost files to the Division of Human Resources or Legal Services.

Keeping COVID-19 Information Secure

All information that you may have access to for your job function relating to a COVID-19 positive individual, an individual who is being assisted due to a positive diagnosis or symptoms, or may be in isolation or quarantine for any reason should be kept confidential and secure and should be treated as information protected by HIPAA.

Any COVID-19 information that you have access to for your job function should not be shared with any other individual, except when sharing the information is necessary to perform your job function and the individual who you are sharing the information with is both authorized to receive it and has a need to know.

Any COVID-19 information that is to be shared with others should be only the minimum amount necessary in order for the person to whom you are sharing the information to do their job.

All COVID-19 information should be considered highly confidential and should be kept secure.

Failure to secure PHI and PII may result in corrective disciplinary action up to and including termination of employment.