COVID-19 PHI Access Policy

This policy covers “Protected Health Information” (“PHI”) at Clark University as it specifically relates to COVID-19.

“PHI” is any information about health status, provision of health care, or payment for health care regarding a specific individual that is created or collected by a “Covered Entity” (or a “Business Associate” of a Covered Entity) as those terms are defined under the Health Insurance Portability and Accessibility Act “HIPAA”). Clark is a Covered Entity. PHI for students at Clark is considered part of their educational record and is covered under FERPA.

At Clark, PHI is considered confidential information under our Data Classification Policy and must be treated as such (https://www2.clarku.edu/offices/its/policies/data_classification.cfm). Confidential information at Clark should be shared with authorized users on a “need-to-know” basis, should be stored only in authorized locations, and not be transmitted via email or other text messaging system(s). Systems like CareEvolve and CoVerified are designed and authorized to store PHI related to COVID-19.

For reference, the following are some examples of how Clark may obtain PHI related to COVID-19 and what federal policies/legislation are in effect.

- **COVID Test Results**: Results of these tests should be considered Confidential under Clark’s Data Classification Policy and handled as such.
- **Daily Screening Checks**: This health information should be considered Confidential under Clark’s Data Classification Policy and handled as such.
- **Other health information provided by Health Services**: Health Services at Clark would be considered a Covered Entity under HIPAA. Information provided to Clark about a student from Health Services would be considered part of their student record and protected under FERPA. If Health Services provides any information to Clark about anyone other than a student, that information would be protected under HIPAA.

It is permitted under FERPA and HIPAA to disclose PHI without a patient authorization during a public health emergency (not indefinitely):

- as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment.
- to the CDC or local health department including Worcester DPH.
- to another person at risk of contracting or spreading the disease. (Although HIPAA permits this, specific state law may prohibit it.)
- to a student’s parent(s) if the student is a “dependent” as that term is defined. If the student is not a dependent, then it is still allowed in an emergency.

It is NOT permitted (under FERPA or HIPAA) to disclose PHI about an individual to the media.

Access to COVID related PHI in CareEvolve and CoVerified will be authorized by the Director of COVID Testing & Operations.

PHI related to COVID-19 will be retained for no longer than one year from the end of the Massachusetts state of emergency.

GDPR was enacted in 2018, and case law is still working through providing clarification. The
scope of GDPR is such that it applies to data collected about individuals while they are in the EU or
data collected about EU citizens through a service that targets EU residents (offers shipping to an
EU country, has a domain suffix for an EU country, provides translation of the web site to an EU
language, etc…). Clarifications have been issued stating that processing of GDPR covered data
(COVID test results and health checks would be covered) is allowed in the interest of protecting
public health.

The California Consumer Privacy Act (CCPA) has an exemption and does not apply to PHI that is
covered under HIPAA.

In summary, COVID test results and health screening information can be shared with other Clark
staff, Worcester DPH, or other medical professionals involved in the treatment of a patient on a need
to know basis. This information should be stored only in CareEvolve or CoVerified unless
explicitly approved by the VP for IT. PHI associated with an individual should not be shared via
email or text/instant messaging. It is permitted to email someone that a positive case has been found
without any identifying information, directing them to an appropriate location to obtain the
identifying information. Identifying information can be shared via a real-time voice/video call,
including audio/video in Microsoft Teams or Zoom using your Clark provided credentials (as these
methods of communication are encrypted).

Created on: July 25, 2020
Last Reviewed: July 30, 2020

Authored by: VP for Information Technology and CIO
Reviewed by: Human Resources (July 29, 2020) & Registrar’s Office (July 27, 2020)
Approved by: Information Security and Privacy Council – July 30, 2020