

HMIS Privacy and Security Standards and COVID-19 Response

March 27, 2020

This document is intended to inform communities covered under HUD's [HMIS Privacy and Security Standards](#) of the ways and limitations that participant information can be shared under the HMIS Standards during an Infectious Disease Emergency Response. The HMIS Standards protect the participant's personally identifiable information (PII) but also allow for uses and disclosures for specific situations. The HMIS Standards apply to any homeless assistance organization that records, uses or processes protected personal information (PPI¹) for an HMIS and these homeless providers are referred to as a covered homeless organization (CHO).

Two primary provisions in the HMIS Standard support the disclosures discussed in this document:

Disclosures required by law: A CHO may use or disclose PPI when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

Disclosures to avert a serious threat to health or safety: Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI if:

- (1) the CHO, 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 an individual or the public; and
- (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

HMIS Information Sharing Scenarios

The following scenarios will help communities make decisions about appropriate disclosures in very specific circumstances. The following scenarios are not exhaustive, and providers should seek clarification regarding any of the below through the HUD Exchange Ask-A-Question (AAQ) portal. Furthermore, CoCs and providers should err on the side of caution. Homeless and healthcare systems are already stretched by this crisis and the stress may worsen. HUD asks that CoCs and providers think about balancing the needs of the participants with the needs of the larger system and that any disclosures are done for appropriate and legal reasons. Staff should still take steps when possible to inform participants of disclosures. The authority to make disclosures without participant consent is not unlimited.

¹ The HMIS Standards use the term Protected Personal Information or PPI. For a homeless provider subject to the standards, PPI is the same as the more commonly used Personally Identifiable Information or PII. This document uses the terms interchangeably.

Scenario 1: Disclosing information about a participant infected with or suspected of being infected with COVID-19 to a public health authority.

Providers are authorized to disclose participant PII required under any federal, state, or local law. A mandatory public health reporting law, whether federal, state, or local, qualifies. A provider may initiate a disclosure to a public health authority if the law requires the provider to report known cases.

This provision authorizes a provider to disclose participant PII under broad circumstances. The first condition is that the provider must believe, in good faith, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public in general. Any public health authority qualifies as a recipient of participant PII about exposure to or infection with COVID-19 under this provision.

The second condition is that the recipient of the information is a person reasonably able to prevent or lessen the threat, including the target of the threat. Any public health authority is reasonably able to prevent or lessen the threat from an infectious disease like COVID-19.

The authority to disclose PII is not unlimited. If a public health authority does not seek or require participant names, then the names should not be disclosed.

The two provisions discussed here are substantially similar to provisions in the health privacy rule issues by the U.S. Department of Health and Human Services under the authority of the Health Insurance Portability and Accountability Act (HIPAA). If questions arise about definitional matters (e.g., who is a public health authority), it is appropriate to look to the HIPAA health privacy rule to resolve those questions. See 45 C.F.R. Parts 160 and 164.

Scenario 2: Disclosing information about a participant infected with or suspected of being infected with COVID-19 to a health care provider.

First, if disclosure to a health care provider is required by law, the disclosure is permissible under the HMIS Standards. Providers are authorized to disclose participant PII required under any federal, state, or local law.

Second, if a provider believes in good faith that disclosure to a health care provider of information about a participant infected with or suspected of having COVID-19 is necessary to prevent or lessen a serious threat to the health and safety of an individual or the public in general, then the disclosure meets the first part of the disclosure requirements. A provider may presume that a health care provider is reasonably able to prevent or lessen the threat, so the second part of the disclosure requirements are satisfied and the disclosure is allowable.

A provider could disclose to a health care provider treating the participant infected with or suspected of being infected with COVID-19. A provider could also disclose information about one participant infected with or suspected of being infected with COVID-19 if the provider is treating a different participant, a provider staff member, or an individual in contact with a participant infected with or suspected of being infected with COVID-19.

The authority to disclose PII is not unlimited. If it is sufficient to give adequate notice to a provider without disclosing the names of one or more participants, then it would be appropriate not to disclose the names.

Scenario 3: Disclosing information about a participant infected with or suspected of being infected with COVID-19 to a shelter or other homeless provider when referring that participant or another participant.

First, if disclosure to a shelter or other homeless provider is required by law, the disclosure is permissible under the HMIS Standards. Providers are authorized to disclose participant PII required under any federal, state, or local law.

Second, if a provider believes in good faith that disclosure of information to a shelter or another homeless provider about a participant infected with or suspected of being infected with COVID-19 is necessary to prevent or lessen a serious threat to the health and safety of an individual or the public in general, then the disclosure meets the first part of disclosure requirements. Given the highly infectious nature of the COVID-19 virus, disclosure to a shelter or other provider is necessary because it allows the recipient of the information to take appropriate precautions to protect the individual, the other provider participants, and the provider staff.

A provider may presume that another homeless provider is reasonably able to prevent or lessen the threat, so the second part of the disclosure requirements are satisfied and the disclosure is allowable.

The authority to disclose is not unlimited. As an example, sending a list of all infected participants to a shelter or other homeless provider may be inappropriate if only one participant is being referred.

Scenario 4: Disclosing information about a participant infected with or suspected of being infected with COVID-19 to a transportation provider, emergency worker, or first responder when referring that participant or another participant

First, if disclosure to a transportation provider, emergency worker, or first responder is required by law, the disclosure is permissible under the HMIS Standards. Providers are authorized to disclose participant PII required under any federal, state, or local law.

Second, if a provider believes in good faith that disclosure to a transportation provider, emergency worker, or first responder of information about a participant infected with or suspected of being infected with COVID-19 is necessary to prevent or lessen a serious threat to the health and safety of an individual or the public in general, then the disclosure meets the first part of the disclosure requirements. Given the highly infectious nature of the COVID-19 virus, disclosure to a transportation provider, emergency worker, or first responder is necessary because it allows the recipient of the information to take appropriate precautions to protect the individual, the other participants, the provider staff, and the workers.

A provider may presume that a transportation provider, emergency worker, or first responder is reasonably able to prevent or lessen the threat, so the second part of the disclosure requirements are satisfied and the disclosure is allowable.

The authority to disclose is not unlimited. For example, sending a list of all infected participants to a transportation provider may be inappropriate when only one participant is being referred.

Scenario 5: Disclosing information about a participant infected with or suspected of being infected with COVID-19 to a third-party quarantine/isolation facility when referring that participant or another participant

First, if disclosure to a third-party quarantine/isolation facility is required by law, the disclosure is permissible under the HMIS Standards. CHO are authorized to disclose participant PII required under any federal, state, or local law.

If a provider believes in good faith that disclosure to a third party quarantine/isolation facility of information about a participant infected with or suspected of being infected with COVID-19 is necessary to prevent or lessen a serious threat to the health and safety of an individual or the public in general, then the disclosure meets the first part of the disclosure requirements. Given the highly infectious nature of the COVID-19 virus, disclosure to any facility housing a participant infected with or suspected of having COVID-19 is necessary because it allows the recipient of the information to take appropriate precautions to protect the participant, themselves, staff, other participants, and other individuals.

A provider may presume that a third-party quarantine/isolation facility is reasonably able to prevent or lessen the threat, so the second part of the disclosure requirements are satisfied and the disclosure is allowable.

The authority to disclose is not unlimited. Sending a list of all infected participants to a third-party quarantine/isolation facility may be inappropriate when only one participant is being referred.

Scenario 6: CoC discovers that the local Privacy Notice isn't up to date.

The HMIS Privacy and Security Standards require providers to include many required elements in its privacy notice. For example, local Privacy Notices should satisfy this requirement:

A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

Because this provision allowing amendment of a privacy notice at any time is a required part of a privacy notice, a provider can and should take immediately action to amend its privacy notice to comply with

the requirement. The authority to change the privacy notice at any time exists even if a privacy notice fails to include the required statement about amendment at any time.

Scenario 7: The local Privacy Notice is changed and the change applies to information collected prior to the change.

The HMIS Privacy and Security Standards specifically address the question of retroactivity:

A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

Scenario 8: The local Privacy Notice is more restrictive than the minimum required by the HMIS Privacy and Security Standards.

A CHO has the ability to adopt a notice that includes policies that are stricter than those in the HMIS Privacy and Security Standards. For example, a provider may adopt a policy for changing its privacy notice to commit to providing advance notice to participants of any change to the privacy notice. However, a privacy notice must include a statement that the notice may be amended at any time and that the amendments may affect information obtained by the providers before the date of the change.

Under urgent conditions, such as the COVID-19 emergency, a provider may find it necessary to change some elements of its notice in order to meet unexpected needs or pressing circumstances. A provider can retract a policy that said that it would give advance notice of a change to its privacy policy and make the change effective immediately. Similarly, a provider that adopted a policy requiring participant consent for disclosures that the HMIS Privacy and Security Standards allow without participant consent may change or eliminate the requirement for participant consent and make the change effective immediately.

The ability to change a privacy notice is not unlimited. The notice must still meet all the requirements of the HMIS Privacy and Security Standards. Any changed notice must be made available to participants and others as provided in the Standards.

This resource is prepared by technical assistance providers and intended only to provide guidance.

The contents of this document, except when based on statutory or regulatory authority or law, do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.