Privacy Impact Assessment

for the

Medical and Public Health Information Sharing Environment (MPHISE)

DHS Reference No. DHS/CWMD/PIA-001

July 24, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Countering Weapons of Mass Destruction Office (CWMD) maintains the Medical and Public Health Information Sharing Environment (MPHISE) system. MPHISE is designed to provide a secure networking capability between DHS personnel and designated federal, state, local, territorial, tribal, and private sector medical and public health partners. This Privacy Impact Assessment (PIA) supports MPHISE to be used as a platform to enable information sharing across the extended medical and public health community in response to any chemical, biological, radiologic, and/or nuclear threat. Standard sharing includes anonymized health information, but in some cases, to be defined below, non-anonymized health data and sensitive personally identifiable information (SPII) will be shared.

Overview

The CWMD mission is to prevent attacks against the United States using weapons of mass destruction through timely, responsive support to operational partners.[1] CWMD is also chartered to work with its interagency and private sector partners to protect the nation from medical issues related to natural disasters, acts of terrorism, and other man-made disasters.[2] The DHS Chief Medical Officer sits within CWMD and is responsible for (1) serving as the principal advisor on medical and public health issues to the Secretary of Homeland Security; (2) providing operational medical support to all Components of the Department; (3) providing medical liaisons to the Components of the Department; and (4) coordinating on medical and public health matters with federal, state, local, and tribal governments, the medical community, and others within and outside the Department, including the Centers for Disease Control and Prevention (CDC) and the Office of the Assistant Secretary for Preparedness and Response of the Department of Health and Human Services (HHS).

To assist with these responsibilities, CWMD has developed MPHISE. MPHISE is a user-driven sharing platform that supports the dissemination of medical and public health information between DHS and other federal, state, county, local, tribal, private sector commercial, and other non-governmental organizations involved in identifying and preventing health incidents as well as in undertaking incident management activities. CWMD mission partners rely on MPHISE as a trusted environment that supports DHS missions by: (1) providing timely and accurate information related to detecting, preventing, responding to, and recovering from terrorist attacks and natural disasters; (2) providing timely and accurate information regarding vulnerabilities and threats, managing incidents to mitigate risks, and reducing post-incident loss of life and property; (3)

[1] *See* 6 U.S.C. § 591(g).
[2] *See* 6 U.S.C. § 597.

providing near-real time collaboration and incident management; (4) facilitating information exchange for emergency management response and recovery operations; and (5) connecting disparate information users in a dynamic and diverse information exchange environment.

MPHISE enables approved users to prepare for and respond to emerging medical and public health issues in support of homeland security operations through information sharing. In the past, technical limitations and disjointed, siloed processes have presented historic challenges for federal leadership to make rapid, informed decisions. For example, as the initial wave of 2009-H1N1 hit the United States, the Nation's ability to locate, compile, and communicate timely and accurate medical and public health information from a myriad of sources was hampered by confusion about authoritative sources, the absence of a single aggregating capability, and the lack of a coherent process to distill the mass of data into useful information for decision-making. Similar examples can be found in the management of Hurricane Katrina in 2005, the ongoing opioid crisis, and as far back as the Tylenol tampering event of the 1980s. During these events, there was a lack of coordination around obtaining reliable, timely, high-value information within agencies, as well as across federal agencies, state and local partners, and the private sector.

To remedy these past challenges, MPHISE allows for all necessary parties to engage and share necessary information. The platform is populated with information from:

- DHS medical and public health professionals;
- DHS medical and public health partners from federal, state, local, tribal, and territorial agencies; and
- Private sector and international medical and public health subject matter experts.

MPHISE will place information in a controlled location with proper access controls and archiving and auditing capabilities and will allow review of lessons learned from relatively short-lived events, which will in turn contribute to improving processes and communications channels for future events. The data in MPHISE allows for understanding of context and possible contrast of regional data, and the platform makes it possible for DHS to conduct analysis across different issue areas to identify national health concerns from regional discussion or other trends.

MPHISE has three content sharing areas: Groups, Spaces, and Projects. Groups provide default locations that separate the content of different issue areas. Individuals can elect to join Groups based on their interest in various topics. Groups can be created by any MPHISE member, but all information in Groups is anonymized. Spaces require an invitation to join, and there are two types of Spaces: Limited and Controlled. Limited Spaces are open to the entire population of MPHISE. Limited Spaces do not involve SPII or Protected Health Information (PHI), and have no criteria for the participants except that they be relevant to the discussion and invited. Controlled Spaces allow sharing for SPII, PHI, or other Specified Controlled Unclassified Information. All

Spaces have a description of the space which includes whether the space is Limited and Controlled, and if Controlled, by whom it is controlled. Sponsors (described later) establish access controls for a Controlled Space, and individuals who are invited must have the appropriate attributes to join. Projects are subsets of either Groups or Spaces with the same characteristics. Projects can be created by any member within a Group or Space, but that project can only include individuals already within that respective Group or Space.

To become a MPHISE user, an individual must have a valid public health role as determined by Approvers and Sponsors (outlined below) in federal, state, local, tribal, or territorial government. Personnel from Non-Governmental Organizations and industry and academia with an existing Memorandum of Understanding (MOU) with DHS will also be accepted as users. DHS may also request specific individuals who it deems relevant to specific areas of interest (e.g., the foremost expert on a specific type of medical issue). Users register with their professional email to allow validation of membership with their organizations.[3]

MPHISE uses role-based access controls based on five types of users in the system, and each user signs and adheres to a user agreement specific to his or her user type.

User Type	**Role**
Approvers	DHS personnel who can invite others to the system and establish their roles. Must approve all users not invited by a Sponsor. Approvers can also be Community Managers.
Community Managers	This is a sub-role of Approvers. Community Managers are the only role that can create Spaces and invite users into a given Space.
Analyst	DHS personnel who can access and review all system data.
Sponsors	Lead individuals in organizations designated by DHS. Can invite users which need not be approved by an Approver.
Users	Can enter Spaces to which they are invited. Can recommend other users to the MPHISE self-registration portal.

[3] So far, this process has been ad-hoc, but it will be developed into a more formal process as the MPHISE userbase grows.

Approvers are DHS personnel managing the system. A subset of Approvers is Community Managers who have the authority to start a Space and invite Users into the Space. Approvers designate Analysts to monitor the system, including all Spaces. These Analysts review the information in the system but have no other system privileges and no ability to contribute. Their purpose is to identify trends or issue-spot across the different Groups, Spaces, and Projects. For example, a Space created for a specific geographical region experiencing an event or particular medical challenge may not realize another Space is dealing with the same concerns. The role of the Analyst is to then connect these Spaces to ensure collaboration of appropriate information.

Approvers also establish Sponsors. A Sponsor is an individual who DHS has designated as a trusted partner. Sponsors can vouch for individuals to be invited to the system. For example, this may be the Chief Medical Officer at Johns Hopkins Hospital who could then invite other Johns Hopkins personnel.

All other MPHISE members are Users, who, when approved through the self-registration portal, are initially granted access to a general Group. Users only have access to the Spaces to which they are invited. A new MPHISE member is created through three methods:

1. Approver-identified personnel
    - During the initial MPHISE development, a bulk load of users was granted access. These users included known and verified users (DHS personnel and limited external organization personnel, such as Southwest Border state and local representatives).
    - Moving forward, MPHISE Approvers can provide access to known individual users on an individual basis for those who support the collaboration.
2. Individual invites from MPHISE Sponsors
    - Sponsors can invite other members of their organization into MPHISE. The individuals would still have to be appropriately granted access to Groups, Spaces, and Projects by Community Managers, for example. This process is designed to spur organic userbase growth.
3. Self-Registration
    - If an individual is invited by another User, that individual is pointed to the self-registration process which occurs through a portal. This process will allow additional userbase growth but requires official approval from an Approver.

The system enforces least privilege (i.e., you must be granted access to data and do not get it by default). The system also has strong audit capabilities to reconstruct what actions were conducted in the system. MPHISE has system administrators and system auditors (i.e., system monitors) who can monitor and assess whether rules are being followed by monitoring membership and content,

specifically for Spaces. The MPHISE Program Management Office (PMO) is responsible for enforcing the guidelines, controls, and management of all users and content in MPHISE.

MPHISE is an information-sharing platform, although new data may be created through collaboration in Groups, Spaces, and Projects. Any data that is shared from a source system by a MPHISE member (data content owner) remains under the stewardship of that individual. The data content owners are responsible for marking their data correctly (e.g., retention, re-dissemination limitations) prior to uploading it and sharing it in the appropriate Groups, Spaces, and Projects. User agreements outline that all users must have the authority to share the data they share on MPHISE and that all sharing restrictions (to include retention and re-dissemination) need to be marked as a banner on the document itself. In addition, it is noted that before any actions are taken based on the data within MPHISE, the data should be confirmed by the data owner.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

As defined in 6 U.S.C. § 597, CWMD is chartered to work with its federal and private sector partners as follows:

- 6 U.S.C. § 597(c)(1): Responsibilities – The DHS Chief Medical Officer shall have the responsibility within the Department for medical issues related to natural disasters, acts of terrorism, and other man-made disasters, including serving as the principal advisor on medical and public health issues to the Secretary, the Administrator of the Federal Emergency Management Agency, the Assistant Secretary, and other Department officials.
- 6 U.S.C. § 597(c)(2): Responsibilities – Providing operational medical support to all Components of the Department.
- 6 U.S.C. § 597(c)(4): Responsibilities – The DHS Chief Medical Officer shall have the responsibility within the Department for medical issues related to natural disasters, acts of terrorism, and other man-made disasters, including coordinating with federal, state, local, and tribal governments, the medical community, and others within and outside the Department, including the Centers for Disease Control and Prevention and the Office of the Assistant Secretary for Preparedness and Response of the Department of Health and Human Services, with respect to medical and public health matters.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

MPHISE Registration Data: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[4] covers the collection and maintenance of information in order to provide authorized individuals access to DHS information technology resources.

DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System[5] covers the collection and maintenance of information for the purpose of creating contact lists and facilitating communication within MPHISE.

MPHISE Content: MPHISE is a tool for information sharing within the homeland security enterprise. The information contained within MPHISE is covered by the applicable SORN(s) depending on the source of the record for federal records. Non-federal records contained in MPHISE are governed by the laws and regulations applicable to the relevant state, local, or public/private agencies that participate in MPHISE and by relevant state, local, or public/private agencies that are the stewards of the information.

As an example, DHS medical records would be covered under the following SORNs:[6]

- OPM/GOVT-10 Employee Medical File System Records[7] covers records related to current and former federal civilian employees and their medical records related to pre-employment and employment.
- DHS/ALL-034 Emergency Care Medical Records System[8] allows DHS to collect and maintain records on individuals who receive emergency care from Department Emergency Medical Services providers. Individuals in this system include anyone who experiences a medical emergency and is treated by an on-duty Departmental Emergency Medical Services medical care provider.
- Forthcoming DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency System of Records[9] will cover DHS's collection, use, and maintenance of records

[4] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[5] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (November 25, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[6] Other DHS Component-specific SORNs covering medical information may also be applicable depending on the information shared on MPHISE.
[7] OPM/GOVT-10 Employee Medical File System Records, 75 Fed. Reg. 35099 (June 21, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.
[8] DHS/ALL-034 Emergency Care Medical Records System of Records Notice, 76 Fed. Reg. 53921 (August 30, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.
[9] The forthcoming DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and

on individuals associated with DHS and its facilities during a declared public health emergency, such as during contact tracing.

Any new data created on MPHISE through collaboration efforts would not require additional SORN coverage. That content may contain personally identifiable information (PII), but that information would not need to be based on an individual and retrieved by that individual's personal records.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

MPHISE is categorized as "moderate" under Federal Information Processing Standards Publication 199. A current iteration of MPHISE that does not share SPII and PHI is already in use with an Authority to Operate (ATO) granted March 27, 2020. The System Security Plan (SSP) is being updated concurrently to this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The MPHISE PMO is working with the National Archives and Records Administration (NARA) to develop appropriate records disposition schedules for any data created on MPHISE. CWMD is proposing a retention schedule of 10 years from the time of inclusion in MPHISE. Other data content owner information shared on or maintained in MPHISE is subject to its source record retention policy, as discussed in Section 5.1, including deference to the records management rules and procedures of specific data content owners.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act (PRA) does not apply to MPHISE because this is a collaboration tool and is not engaging in a "collection of information" as defined under the PRA.[10]

Visitors During a Declared Public Health Emergency System of Records will be available in the Federal Register and DHS Privacy Office website once completed, *available at* https://www.dhs.gov/system-records-notices-sorns.

[10] *See* 44 U.S.C. § 3502(3).

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

MPHISE Registration Data: MPHISE collects user registration information for the purpose of processing and validating the registrant's identity and ensuring the user's relevance to data within MPHISE and/or the qualifications of entry into a particular MPHISE Space. Information that is collected and stored on MPHISE from a member includes: Name, Email Address, Affiliation, Agency/Company, Organization, Functional Area, Background Investigation Level, Security Question, Security Answer. In addition, for access to SPII and PHI Controlled Spaces, additional attributes may be collected, such as: Medical Role, Facilities over which the individual has oversight, and other medical-related qualifications.

MPHISE General Content: MPHISE members may generate structured and unstructured data, including content, data visualizations, and reports, in order to support the evaluation of potential medical and public health threats, as well as to detect trends related to potential and ongoing events of interest. Users may also share content that originated from external source systems.

An example of this type of data would be deidentified geolocated COVID-19 case data. The information could include relevant clinical care information about each case, including the diagnoses, medications, and allergies for each case. MPHISE generally focuses on event data rather than individual-level information. For example, the sharing of this information is to allow collaboration on what individuals have observed that is out-of-the-ordinary based upon their judgment/experience and the circumstance of their observation, and solicit guidance and assistance in some cases. Identifying individuals is not the purpose of the information sharing or collaboration and not needed in most cases (other cases described below).

Much of the MPHISE data is sourced from source systems. The data is being used to evaluate the overall situation or event, not to take individual-level actions. The system is used to conduct analysis to assist with validation of data, analyze outcomes, and manage resources.

MPHISE Sensitive PII and PHI Content: Individual-level data is shared on the system for limited use cases and is only shared in Controlled Spaces. Sensitive content introduced into the system is marked in accordance with guidance from the respective CWMD mission partner, agency, or private sector organization, as required. The following use cases are examples that illustrate the uses of sensitive data on the system.

- Use Case 1: A specific set of symptoms that requires a group of MPHISE members to discuss and see if there is similar symptomology across care sites. The information would still be anonymized but likely identifiable due to the extremity or uniqueness of the cases.

The discussion would be limited to researchers and caregivers in the Controlled Space. The outcomes (trends and analysis without SPII and PHI) of this analysis may be shared outside the Controlled Space when learned.

- Use Case 2: A specific set of facilities would use MPHISE to transition either patient data, test sample data, contact tracing information, or other sensitive data from one facility to the other. This could be in a situation where DHS had control or care over one of the facilities that patients were being transferred to or from, in order to facilitate patient care. After transition of the data, the data would be removed from MPHISE. The Controlled Space in this use case would be limited to the two facilities. MPHISE allows for a more secure means of transferring this information between these stove-piped groups than email or other conventional methods.
- Use Case 3: Data concerning people in detention, people being cared for, or personnel in a specific facility or set of facilities and their disease/illness or vaccine status. This is used in locations of hotspots to communicate to DHS medical and senior personnel and is not a standing analysis of all facilities. For example, it is necessary to know the overall status of a facility if an individual that enters that facility has a disease or illness. If a detainee comes into a U.S. Customs and Border Protection (CBP) detention center and has a disease, it is necessary for DHS medical and senior personnel to see the vaccine status for all CBP personnel in that facility to account for workforce accountability, medical response, and other responsibilities. For example, this data may be used in a heat-map to assist DHS medical personnel and leadership in understanding health risks in specific locations in CBP detention centers. The information used for this use case is generally deidentified, but could be re-identifiable (likely by the recipients of the data) due to the small population. The Controlled Space would be limited to those with authority over the facility and need-to-know.
- Use Case 4: Similar to the previous use case, this use case would be for workforce health data collected on DHS personnel that would be analyzed for fitness for duty. The DHS Chief Medical Officer is required to provide consultation to and coordination with Component medical operations on issues such as infectious disease exposures that might affect fitness for duty. This could also include data regarding job role, vaccines, diagnoses, medications and allergies, and job requirements. The Controlled Space would be limited to those with authority over the personnel. This would be shared for coordination with CWMD for advisory support, to show aggregate issues across facilities, and to address resourcing or other concerns at the organizational level.
- Use Case 5: Data on a specific individual or group of individuals that creates specific difficulty in contract tracing. This is not to replace the contact tracing being done by individual Components but to augment these efforts to manage resources, identify trends,

and validate ongoing analysis, as required by the DHS Chief Medical Officer's responsibility to provide consultation to and coordination with Component medical operations. This may include sharing consistent elements of multiple cases to identify or verify an overlapping connection. This may be sharing between two contact tracing personnel obtaining contact tracing data for a given facility or locale. The Controlled Space would be limited to contact tracers and those with authority over the facility or locale in which contact tracing collaboration is required.

MPHISE sharing of SPII or PHI is limited to those with access permissions needed for sharing in their user accounts/profiles. The introduction of SPII or PHI requires a Controlled Space established by a Community Manager with specific access limitations supported through user account attributes.

2.2 What are the sources of the information and how is the information collected for the project?

MPHISE Registration Information: Information is collected directly from individuals who are registering for MPHISE, or from their Sponsor during the onboarding process.

MPHISE Content: MPHISE members may share content with other MPHISE members that originated from external source systems as long as they have the authority themselves to share the information. Sources of the information collected, used, and maintained within MPHISE also include publicly available and open source information, such as news reports and social media; finished products, such as locality health data or public health products; meeting notices; information bulletins; and federal, state, local, tribal and territorial information and notices.

Additionally, MPHISE members may generate structured and unstructured data, including content, data visualizations, and reports, in order to support the evaluation of potential medical and public health threats, as well as to detect trends related to potential and ongoing events of interest.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. MPHISE content may be sourced from commercial sources or publicly available data. For example, MPHISE may use commercial geolocation data, or publicly available data from states/localities identifying medical cases by ZIP code.

2.3 Discuss how accuracy of the data is ensured.

MPHISE Registration Information: Registration data is collected directly from the individual in question, or the individual's Sponsor, and so is assumed to be accurate. Additionally, MPHISE registration information is validated by authorized Approvers/Sponsors of MPHISE prior

to initiating the registration process. Members have access to their user accounts to change an incorrect information as necessary.

MPHISE Content: MPHISE relies on the information from data content owners within the original source systems being accurate and does not collect information directly from members of the public or any other primary source. These original source systems may be federal, state, local, tribal, territorial systems, private-sector, and/or other CWMD mission partners' systems. The locality health data or public health products generated and shared by MPHISE members rely on a variety of source record systems and public records to verify the accuracy of information before it is shared within MPHISE. Ultimately, data content owners are the responsible for the accuracy of the data they share on MPHISE.

2.4 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that MPHISE will collect more information than is necessary.

Mitigation: This risk is partially mitigated. CWMD has worked with the DHS Privacy Office to minimize the areas in MPHISE in which sensitive information in shared. MPHISE content is limited to deidentified data unless it is in a Controlled Space. This ensures that any SPII or PHI is available only to those with a need-to-know and who have been appropriately provisioned access, not the entire MPHISE community. These Controlled Spaces are available to a small number of members with attributes that show their valid need and access to the data. The Controlled Spaces address a specific problem and require relevant membership to assist in the purpose of MPHISE.

Privacy Risk: There is a risk that, due to lack of data validation, information provided by users will be inaccurate or out of date.

Mitigation: This risk is not fully mitigated. However, CWMD has taken several steps to ensure data accuracy. Information presented to MPHISE is linked to the individual that provides it. If any inaccurate data is discovered, the data content owner can be notified of the error. Additionally, and by the nature of MPHISE, users on the system are looking for collaboration on issues and other concerns they need assistance with. Part of the purpose of the system for some uses cases is for experts to critically analyze and validate the data. The data is being used to evaluate the overall situation or event, not to take individual-level actions.

In additional use cases, MPHISE itself presents a more secure sharing method, preserving data integrity, than the sharing that otherwise may occur via email, over the phone, or other informal methods.

Privacy Risk: There is a risk MPHISE members may share information about individuals

who are not relevant to the immediate incident.

Mitigation: This risk is partially mitigated. In the areas that have sensitive data (i.e., Controlled Spaces), the sharing would fit the types of use cases above, such as to evaluate an anomaly or to pass information from one facility to another. The purpose of MPHISE is for information sharing and collaboration, not to make decisions about individuals. Although MPHISE itself cannot ensure that all information that is shared within a Controlled Space will be relevant to the resolution, there are mechanisms in place to limit its sharing. Individuals are responsible for their own data when it is on MPHISE and the person has the ability to remove it if it is found to be not relevant. Furthermore, the MPHISE archiving capability allows for Community Managers and other MPHISE members to archive their data if an incident is determined to have no relationship to potential or ongoing medical and public health threats.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The information collected in MPHISE enables federal, state, local, public, and private health partners to research and analyze activities in support of preparing for or responding to medical issues related to man-made and naturally occurring disasters. It allows users to draw links and patterns that might not otherwise be readily apparent. The system is used to quickly share information in an evolving environment to conduct analysis to assist with validation of data and outcomes and manage resources. As outlined in the use cases above, any sensitive data within MPHISE is being used to evaluate the overall situation or event, not to take individual-level actions.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. MPHISE Analysts can search MPHISE to identify potential medical threats to the homeland or trends requiring further analysis. MPHISE Analysts also conduct electronic queries of data to identify medical trends related to potential and ongoing natural disasters, acts of terrorism, and other man-made disasters. This includes suspected biological chemical, radiological, and nuclear threats to the homeland.

MPHISE Users do not have the ability to conduct similar system-wide searches, but may use resulting data to produce reports, visualizations, or other outcomes as required to serve the CWDM mission.

3.3 Are there other components with assigned roles and responsibilities within the system?

Other DHS Components may have a role within the system, but MPHISE is managed by CWMD through the user registration process. Given the nature of a particular emergency, other DHS Component personnel could be approved as Sponsors or Approvers. Other homeland security enterprise public health mission partners may also become Sponsors. For example, CWMD personnel may elect to share medical and public health information with CBP related to biological agents that may have entered the country. Information about biological agents related to medical events of interest may also be reported by CWMD mission partners and shared with the appropriate Group or Space (Controlled if it involves SPII or PHI).

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information may be misused or used in a manner inconsistent with the homeland security enterprise public health mission, particularly by non-DHS personnel.

Mitigation: This risk is partially mitigated. CWMD has created a number of mechanisms to limit misuse of the system and the data that it maintains. The MPHISE PMO has developed a registration and onboarding process that requires individuals to be DHS and mission partners related to CWMD authorities pursuant to 6 U.S.C. § 597. Those individuals then have to be invited into areas of MPHISE where any sensitive data may be shared (e.g., Controlled Spaces). All users are required to sign and adhere to the user agreements that are tailored to the individual's role.

Furthermore, audit logs maintain records of who shared information, who accessed information, and when the information was shared/accessed. Audits are conducted periodically by the MPHISE PMO.

However, due to the nature of this system as an information sharing platform, it is incumbent on the data content owners to use and share their information appropriately.

Privacy Risk: There is a risk personnel may have access to data about which they do not have a need-to-know.

Mitigation: This risk is mitigated. CWMD has created MPHISE as a system of least privilege (i.e., you must be granted access to data and do not get it by default). First, the registration and onboarding process requires individuals to be relevant to supporting the CWMD charter. Only predetermined users (i.e., Approvers, Sponsors) can invite individuals to MPHISE. All other individuals are required to go through the formal registration process. Second, system access is granted using multi-factor authentication. Third, access to sensitive information in Controlled Spaces is provisioned to an individual being invited by a Community Manager. Users can see the restrictions in the label of the Space and see the other users in the Space that they would be sharing

information with. This ensures that a Space is able to limit sharing information to only those with a need-to-know. MPHISE also has system monitors[11] who monitor system use, membership, and content of Spaces, Groups, and Projects.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

MPHISE provides notice to users through the registration process and appropriate user agreements. For MPHISE content, the notice given to individuals is beyond the scope of MPHISE and CWMD. All information is collected and shared in accordance with authorities of the specific data content owner. Because CWMD is not collecting information directly from individuals, it is the responsibility of the data owner to provide notice, usually at the point of collection. Any discussion or created content about the underlying data would be shared consistently with the sharing rules for that data. However, this PIA provides some degree of notice

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Use of the system is voluntary, and users can elect to not join MPHISE and therefore not provide data. For MPHISE content, there is no opportunity for individuals whose PII, SPII, or PHI is collected in MPHISE to opt out of this use of their data. However, most individuals would have the opportunity to opt out of the original collection of their data (e.g., collection while DHS or other medical partner is providing care).

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not provided adequate notice that their information will be shared within MPHISE as content.

Mitigation: This risk is not fully mitigated. MPHISE content data is predominantly persons under some DHS authority (employees, detainees, visitors to DHS facilities). However, there may be cases where non-DHS data is sourced and shared. Although individuals may not be given explicit notice that their data is in MPHISE, they are aware of DHS (or the CWMD mission partner's) use and review of their data in the underlying systems or processes.

[11] These are system administrators and system auditors conducting audit functions to ensure security requirements are being met and MPHISE polices and user agreements are being followed.

Because MPHISE is a communication and collaboration tool to discuss medical issues, some individuals will not have a relationship with DHS. In these cases, DHS is serving to facilitate the transfer of the data, the evaluation of the data, and the use of resources (e.g., hospitals, testing centers, medical personnel) to address the emergency need.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

The MPHISE PMO has requested records disposition schedules for the new content created on MPHISE. Given that most contemporary knowledge of incident planning and mitigation indicates long periods of activity, and that some seemingly innocuous activity could signal a homeland security threat, CWMD has determined a 10-year retention period is necessary. The proposed schedule is 10 years from the time of inclusion in MPHISE. Not all records will remain active during this time; rather, it is anticipated that MPHISE will maintain both active and archived records. MPHISE Community Managers are required to archive content if an incident is determined to have no relationship to potential or ongoing medical and public health threats. This would allow a Community Manager to close an event as a whole if it was not relevant to the next event. For example, an anthrax release discussion might be archived during a pandemic response given that it is not relevant to the current conversation. This ensures that the information deemed to be not relevant does not impact the current situation.

MPHISE members are also required to archive their data if an incident is determined to have no relationship to potential or ongoing medical and public health threats.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be retained longer than necessary.

Mitigation: This risk is not fully mitigated. MPHISE members are responsible for adhering to the applicable federal, state, local, territorial, and/or tribal records management laws, regulations, and policies that apply to the content they share or over which they retain custody and control. However, CWMD has taken several steps to mitigate this. As part of user agreements, individuals are made aware of their responsibility to properly provision the data they share. MPHISE also has system monitors to supervise system use, including data content owners marking the retention of their data correctly.

For content created on MPHISE, a records retention schedule has not yet been approved. CWMD has proposed a 10-year retention period for this data. This risk remains unmitigated until the records retention schedule is approved and can be followed.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

MPHISE is an information-sharing tool for the homeland security medical partner enterprise. The authorities listed in Section 1.1 of this PIA assign DHS responsibility for coordinating medical and public health matters with federal, state, local, and tribal governments; the medical community; and others within and outside the Department. MPHISE is the primary platform by which DHS coordinates and shares this type of information. To become a MPHISE member, an individual must have a valid public health role in federal, state, local, public, or private health partner agency. Personnel from Non-Governmental Organizations and industry and academia with an existing MOU with DHS will also be accepted as users. DHS may also request specific individuals who they deem relevant to specific areas of interest. Individuals are permissioned onto MPHISE through several mechanisms (e.g., through Approvers, Sponsors, self-registration). From there, individuals still have to be admitted to Spaces, where issue-specific content and SPII and PHI are shared. This involves review and admittance by Community Managers to ensure a need-to-know of all individuals who access SPII and PHI.

All members must also sign and abide by user agreements specific to their user type. These user agreements discuss the appropriate actions the individual can take on MPHISE and the individual's responsibilities for the data he or she provides, shares, and accesses.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Content is shared on MPHISE across federal, state, local, tribal, territorial, private sector, international, and other non-governmental partnerships who support the homeland security medical partner enterprise. This source system data will not be owned by CWMD. Data is shared to mission partners according to data content owners' and MPHISE members' own legal and policy requirements. Because the data remains under the management of the data content owner, external sharing of data is subject to the SORN compatibility analysis on a case-by-case basis. In the case of federal mission partners' data, this sharing would be done in accordance with the SORN and applicable routine uses that apply to the data being shared. For non-federal partners, the information would be shared in accordance with an existing MOU. Additionally, the data content owner and MPHISE member agree to manage the security and privacy of their data, as provided in the appropriate MPHISE user agreement.

Any new data created on MPHISE through collaboration efforts would not require additional SORN coverage. That content may contain PII, but that information would not be

retrieved by that individual's personal records.

6.3 Does the project place limitations on re-dissemination?

MPHISE user agreements address sharing information to and from the platform. MPHISE members are required to mark all content that has dissemination limitations when sharing. All data shared within and externally from MPHISE is recorded within audit logs.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

MPHISE maintains audit logs for all information that is provided on the platform. The audit logs track system events and are reviewed weekly for indications of inappropriate or unusual activity as it relates to account usage, privileged access requests, and data access requests.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be shared in a manner inconsistent with the purpose of collection and the MPHISE mission.

Mitigation: This risk is partially mitigated. MPHISE has enacted a number of procedures to ensure sharing is limited to only those with a need-to-know. User agreements establish the rules for each user type as to their conduct on the system, that they need authority to share information on the system, and that they can only share PII, SPII, and PHI within a Controlled Space. The system has been set up, through least privilege, to have stringent onboarding processes and Controlled Space accessibility. System monitors audit Groups, Spaces, and Projects to ensure that they are being used correctly.

The nature of MPHISE as an information sharing platform still requires MPHISE members to initially share information appropriately to the system.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

MPHISE members submit their own registration information and have the opportunity to access their user accounts at any point.

For the content that MPHISE does not own, it relies on the data provision of its mission partners. Because MPHISE does not own the data, the ability of individuals to access their information lies with the data content owner. Each data owner may have different procedures that allow for individuals to access their information depending on the applicable SORN, for federal

agencies, and applicable handling requirements for other non-federal agencies, such as local law enforcement. Individuals seeking access to any record contained within a DHS source system of records may submit a Privacy Act or Freedom of Information Act (FOIA) request in writing to the Headquarters or Component FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts". If an individual believes more than one Component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA, Privacy Office, Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, DC 20528-0628.

Any content that is created as part of the collaboration process can also be accessed as described above by submitting a Privacy Act or FOIA request in writing to the Headquarters or Component FOIA Officer.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

MPHISE members have the opportunity to make changes to their user accounts at any point.

For the content that MPHISE does not own, the ability of individuals to correct inaccurate or erroneous information lies with the data content owner. Each data content owner may have different procedures that allow for individuals to correct their information. Individuals seeking correction of any DHS record contained in a source system of records may submit a request in writing to the Headquarters or Component FOIA Officer as described in Section 7.1.

For any content that is created as part of the collaboration process on MPHISE, an individual may also submit a request in writing to the Headquarters or Component FOIA Officer as described in Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

MPHISE members are made aware of their user accounts and procedures for correcting their information during the registration process.

For the content that MPHISE does not own and that which is created on MPHISE, CWMD cannot notify individuals directly about the procedures for correcting their information. This PIA serves as notice that individuals must contact the data owner or follow the data owner's process if they seek to correct their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not have sufficient redress opportunities for their information maintained in MPHISE.

Mitigation: This risk is not fully mitigated. Redress for the SPII and PHI that are shared on MPHISE should occur with the source system owner. MPHISE is a system based on either transferring data or collaborating about the information. This PIA provides some notice of the redress process, but the individual whose data is being shared will likely have to relay on the redress processes afforded by the source system.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The MPHISE PMO will use a number of mechanisms to ensure that the information presented to MPHISE is used in accordance with this PIA. Additionally, CWMD will continue to work with the DHS Privacy Office to ensure all privacy responsibilities are being adhered to and all privacy requirements are being met as the system continues to develop.

Mechanism	Description
User Validation	Approvers validate that all users are individuals who have a valid public health role (support to the CWMD charter as designated in 6 U.S.C. § 597) in federal, state, local, tribal, or territorial government, or other appropriate health partner.
User Agreement	User agreements establishes the MPHISE sharing and conduct rules. This includes the following: • PII, SPII, and PHI can only be shared within a Controlled Space. • Users must have authority to share all information that they share on MPHISE and must share in accordance with their organization's sharing rules. • Users must mark all sharing requirements on documents shared within MPHISE before uploading documents.

	User Agreements for Sponsors define their responsibility in sponsoring others to MPHISE. User Agreements for Community Managers define their responsibilities in establishing Controlled Spaces and describing their limitations.
Controlled Spaces	Controlled Spaces are the only place that PII, SPII, and PHI may be shared, and access is limited based on attributes of the individuals in the Controlled Space.
Controlled Space Labeling	In the description of the Controlled Space, the restriction is described as controlled and the restrictions are identified. (For example: This is a controlled space limited to personnel with patient oversight at facility X and Y.)
Training	The MPHISE PMO is developing training to assist members in more fully understanding the uses of the system, including the sharing rules and requirements.
System Audit and Monitoring	The system has both automated audit features and manual monitors. System monitors can evaluate whether personnel are following the sharing rules and correct their behavior if they find material is being shared inappropriately.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project?

The MPHISE PMO provides training to use the data content controls correctly and provides fact sheets on the correct use of the collaboration tools (e.g., Groups, Spaces, Projects). DHS personnel complete annual privacy training. Other government agency users of MPHISE also receive training in the protection of personal information from their home organizations. Medical personnel who join MPHISE will also have Health Insurance Portability and Accountability Act (HIPAA) training as part of their background.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to MPHISE is strictly managed by Approvers authorized by the MPHISE PMO. Sponsors can add personnel in their organizations. Invitations are limited to individuals at DHS and mission partners who are required to support the CWMD charter, as designated in 6 U.S.C. § 597. Following registration, individuals are only permitted to access information openly shared by DHS or other mission partners unless they are provisioned access to Limited or Controlled Spaces by a Community Manager.

MPHISE access controls involve three basic components in addition to a general audit protocol designed to identify and sanction inappropriate access:

Role-Based Access Controls: The first of these controls are limitations based upon a user's administratively assigned categories and roles. Users will only have access to default areas where sensitive data is restricted unless they are invited to a Space that is addressing sensitive data. If that is the case, the Community Manager must ensure that they meet the Space criteria (i.e., have the correct attributes and have a need-to-know the information) before providing access. As an example of the role-based access, only a medical and public health professional will have access to PHI about a patient to address anomalous symptomology. This attribute (available to the Community Managers) would be validated and maintained as part of the individual's user account.

Data Content Owner Access Limitations: Data content owners placing information that they deem to be sensitive into MPHISE may also place restrictions on the data. For example, an agency may identify that a particular piece of information is of such sensitivity to an ongoing medical or public health event that it may be viewed for situational awareness but may not be officially used or referenced without contacting that agency. Similarly, a private medical company may restrict access or use of commercial proprietary information so that particular agencies may access it, but may not release it publicly or distribute it to regulatory entities unless it demonstrates a violation of law relevant to a federal, state, municipal, or tribal law enforcement agency.

Audit Controls: All data will remain linked with records of who/when that information was accessed and is subject to a periodic audit to ensure that information in MPHISE is used in accordance with the above described policies.

System access is also protected using a multi-factor authentication.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The MPHISE PMO will review all information sharing agreements and MOU to ensure that they follow the guidance with this PIA. The criteria are that the individual/organization have a valid public health role in federal, state, local, tribal, or territorial government, who are required to support the CWMD charter, as designated in 6 U.S.C. § 597. These reviews will be conducted in coordination with the DHS Privacy Office.

Responsible Officials

Scott T. Bjorge
Lt Col, USAF
Rapid Capabilities Division
Countering Weapons of Mass Destruction
U.S. Department of Homeland Security
(202) 254-7180

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717