



Privacy Impact Assessment
for
H1N1 Medical Care for
DHS Employees

December 1, 2009

Contact Point

Kathryn Brinsfield

Associate Chief Medical Officer, Component Services

Office of Health Affairs

202-254-6479

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Department of Homeland Security (DHS) Office of Health Affairs (OHA) is issuing Standard Operating Procedures (SOP) to set forth requirements for DHS Components to provide medical care to DHS Mission Critical and Emergency Essential employees located in remote or medically austere environments who either present with influenza-like symptoms, or have been exposed to a probable case of H1N1 Influenza. The SOP will remain in effect for the duration of the Department of Health and Human Services (HHS) -declared public health emergency with respect to H1N1. OHA is conducting this PIA because the SOP involves the collection of personally identifiable information (PII).

Overview

DHS OHA is issuing SOPs entitled “Guidelines for Administration of Antivirals” to set forth requirements for Department of Homeland Security (DHS) Components to provide medical care to designated Mission Critical and/or Emergency Essential individuals who either present with influenza-like symptoms or have been exposed to a probable case of H1N1 influenza, and whose location in a remote or medically austere environment makes the pursuit of medical care by a physician incompatible with mission-critical operational effectiveness (e.g., the employee is unable to leave his/her duty station without compromising his/her mission or safety). The SOP will remain in effect for the duration of the Department of Health and Human Services (HHS)-declared public health emergency with respect to H1N1. The SOP requires the collection of personally identifiable information (PII) from DHS Mission Critical and/or Emergency Essential Employees (hereinafter “eligible employees”) who voluntarily seek and consent to receive medical treatment in the form of antiviral pharmaceuticals, such as Tamiflu, from designated DHS medical professionals. This SOP also establishes that Components send certain health-related information for eligible employees treated, with PII redacted, to OHA and the Chief Administrative Officer’s Office of Occupational Safety and Environmental Programs (OSEP) so that DHS is able to track reports of adverse effects of antiviral pharmaceuticals dispensed by DHS medical providers.

The SOP provides direction to DHS federal employees whose official duties include the provision of medical care, who are authorized by their Component to provide medical care, and who are credentialed by the Assistant Secretary for Health Affairs/Chief Medical Officer (ASHA/CMO) (hereinafter referred to as “designated DHS medical care providers”). Specifically, this SOP provides guidance to designated DHS medical care providers on: (1) recognizing symptoms of influenza; (2) implementing the decision to recommend and/or administer/dispense post-exposure prophylaxis; (3) administering/dispensing treatment and post-exposure prophylaxis medication; (4) recognizing potential side effects of treatment and post-exposure prophylaxis medications; and (5) establishing a tracking mechanism to record DHS cases of probable H1N1 infection in remote or medically austere environments and whether those treated experience any adverse effects from that medication.



This SOP and its implementation require Components rendering H1N1-related medical care to collect health information from those eligible employees who voluntarily seek evaluation and treatment (where appropriate) from designated DHS medical care providers, to record the results of those evaluations and to document treatment when provided. In addition, eligible employees seeking treatment are required to sign DHS Form 5201, Antiviral Medication Consent – Declination, which states that the employee is aware of his/her right to decline treatment (before any treatment is administered). Designated DHS medical care providers shall document treatment using Standard Form 558 (SF 558), Emergency Care and Treatment Medical Record, or an equivalent form. These forms shall be considered occupational medical records which Component providers shall maintain in Employee Medical Folders (EMFs). These forms will not be duplicated or stored centrally within DHS unless PII in the form has been redacted.

This information will be transmitted, with PII such as names, direct phone numbers, and signature redacted, to OHA and OSEP every 24 hours to enable the Department to track the spread of the H1N1 virus in its workforce in medically austere environments, improve its delivery of medical care to and protect the health of this segment of the DHS workforce, and to report any adverse effects of treatment to the FDA's MedWatch Program, which monitors the safety of human medical products.¹

Typical Transaction

In a typical transaction under the SOP, a DHS operational Component Mission Critical employee, for example, a U.S. Customs and Border Protection agent who is stationed in a remote or medically austere environment (i.e, the employee is unable to access medical care due to a particular mission-related circumstance), may voluntarily seek medical care for flu-like symptoms from the DHS medical care provider assigned to his duty station. After a determination as to whether it is appropriate to recommend administration/dispensation of post-exposure prophylaxis and receiving consent from the agent for such administration/dispensation, the designated DHS medical provider would request that the eligible employee enter his relevant information in form SF 558 and would evaluate that agent and provide antiviral medication. The designated DHS medical care provider would record the treatment plan in the SF 558 (in addition to the patient-provided information) and this form would be maintained in the agent's Employee Medical File (a hardcopy file similar to a medical chart kept by the provider) and accorded the same security protections as his other occupational medical records. The designated DHS medical care provider would then extrapolate specified information from the SF 558, which would not be PII, and provide that information to OHA and OSEP in a password protected spreadsheet. Should the agent experience any adverse effect due to the administered antiviral medication, such as severe nausea, the designated DHS medical care provider would update the spreadsheet (again not containing PII) and send it to OHA within 24 hours. OHA then forwards this non-personally identifiable information to the Food and Drug Administration's (FDA) MedWatch Program, which monitors the safety of human medical products

¹ More information about MedWatch is available at <http://www.fda.gov/Safety/MedWatch/default.htm>.



This SOP does not apply to health services provided by, for, or on behalf of the United States Coast Guard (USCG); compliant with Department of Defense, TRICARE, and USCG Commandant Directives and Instructions related to the provision of health services.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

In the course of providing H1N1-related medical care to eligible employees, as directed in the SOP, Component-designated medical care providers collect, use, maintain and disseminate (where appropriate) information from eligible employees that is necessary to render appropriate evaluation and treatment of probable H1N1 infection or exposure and to track potential adverse effects of pharmaceutical treatment administered. This information includes PII that is sensitive both in that it can be used to identify a person as an essential employee and that it contains health information about that individual. Components will collect this information using SF 558, or an equivalent form and maintain that form in the EMF like all other occupational medical files. Information entered into the SF 558 shall include the following information:

- Name, age, location
- Identification number (Social Security Number or other)
- Initial signs and symptoms presented
- Treatment modalities
 - Drug given
 - Dosage and schedule
 - Route
 - Location
 - Date and Time
 - Noted potential contraindications
 - Expiration Date
- Side effects experienced
- Prevention measures
- Disposition
- Follow-up orders

In addition, Components will enter the above listed information, PII redacted, into a password protected spreadsheet and share with OHA and OSEP, to enable the Department to track the spread of the H1N1 virus in its workforce located in remote or medically austere environments, improve its delivery of medical care to and protect the health of that DHS workforce, and to report any adverse effects of treatment to the FDA's MedWatch Program.



1.2 What are the sources of the information in the system?

The sources of the information are eligible employees who voluntarily seek medical evaluation and treatment for possible H1N1 infection or exposure. Designated DHS medical care providers collect this information in the form of SF 558s (or equivalent forms) and report treatment provided.

1.3 Why is the information being collected, used, disseminated, or maintained?

Designated DHS medical care providers collect this information, which includes PII, as part of standard patient care (generally, providers cannot treat patients who will not identify themselves or share certain sensitive health information). The information is collected to protect the health of the DHS workforce in remote or medically austere environments and ensure continuity of operations and safety of DHS personnel in the face of a pandemic by 1) facilitating the appropriate medical evaluation and treatment of eligible employees located in remote or medically austere environments who either present with influenza-like symptoms or who have been exposed to a probable case of H1N1 influenza; 2) tracking the spread of the H1N1 virus in the DHS workforce located in remote or medically austere environments; and 3) monitoring for and reporting adverse effects of treatment to the FDA's MedWatch Program. Collection of PII also enables Component DHS designated medical care providers to alert employees that have been administered/dispensed medications if safety or efficacy issues arise with the administered/dispensed medication.

1.4 How is the information collected?

Designated DHS medical care providers will collect this information in the form of SF 558s (or equivalent forms). They will enter this information into a spreadsheet, redact names, and supply the redacted information to OHA and OSEP via password protected email.

1.5 How will the information be checked for accuracy?

All employees with active EMFs have access to that folder's contents, including the SF 558 (or equivalent form) which is completed by the DHS designated medical care providers who evaluate and treat the eligible employee seeking care for H1N1 (or H1N1 exposure). Components will work with employees to correct any reported inaccuracies in their EMFs.

PII collected by the designated DHS medical care provider is done in direct consultation with the DHS employee (patient) who is providing the information voluntarily, and so is assumed to be accurate at the time of collection. That PII collected is not further duplicated or shared, which prevents it being inaccurately transmitted or copied.



1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The ASHA/CMO leads OHA and has primary responsibility within the Department for “medical issues related to natural disasters.” See Section 516 (c) of the Post Katrina Emergency Management and Reform Act, P.L. 109-295, 6 U.S.C. 321e(c). In addition, the Secretary has delegated to the CMO/ASHA responsibility for providing oversight for all medical and health activities of the Department. See Delegation to the Assistant Secretary of Health Affairs and Chief Medical Officer, No. 5001 (signed July 28, 2008). OHA issues this SOP based on these authorities, as well as its CMO authority for “ensuring internal and external coordination of all medical preparedness and response activities of the Department.” See 516(c)(3) of PKEMRA.

Component-designated medical care providers collect medical information from eligible employees in accordance with and under the authorities provided in OPM/GOVT-10 System of Records Notice for Employee Medical Files and Part 293, Subpart E of Title 5 of the Code of Federal Regulations, Employee Medical File System Records (2009).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

While there are inherent privacy risks in collecting health information from employees, this collection of information is necessary to facilitate the medical evaluation and treatment of eligible employees who voluntarily seek care for H1N1 infection (or probable exposure). Receiving evaluation/treatment, and submitting information required for evaluation and treatment, is strictly voluntary, and employees are required to sign a Patient Consent form which states that the employee is aware of his/her right to decline treatment. Once collected, this information is not duplicated or transferred; only de-identified information as is minimally necessary to carry out health-related authorities is reported up to OHA and OSEP.

The SF 558s or equivalent form which captures the sensitive information provided is maintained in an employee’s EMF. EMFs are standard files kept by Components for each of their employees whose job has a fitness for duty requirement, and these are generally the same employees who would seek and receive treatment according to the SOPs. In the event that an eligible employee who does not have an EMF (e.g., because the employee does not have a fitness for duty requirement) requests medical care from a designated DHS medical care provider for H1N1, the medical care provider shall create an EMF for that employee consistent with the Component’s process for creating EMFs.

The PII collected according to these SOPs will be stored in hard copy format and kept in the same manner as all other existing medical records. The EMF is kept separate from general employee personnel files and is accorded the necessary protections to ensure that this information



is maintained confidentially. Generally, these protections include that the files are kept in hard copy in a locked file cabinet with limited access inside a secured DHS facility.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Designated DHS medical care providers use the information provided by eligible employees seeking treatment for probable H1N1 infection or exposure and captured in the SF 558 (or equivalent form) to review and evaluate employees' medical complaints and help make decisions about what kind of treatment to provide employees (if any). Designated DHS medical care providers collect this information, which includes PII, as part of standard patient care (generally, providers cannot treat patients who will not identify themselves or share certain sensitive health information). The information is collected to protect the health of the DHS workforce in remote or medically austere environments. Collection of PII also enables Component DHS designated medical care providers to alert employees that have been administered/dispensed medications if safety or efficacy issues arise with the administered/dispensed medication.

The designated DHS medical care provider describes the treatment recommended and/or administered on the SF 558. This information is then retained by the Component as an occupational medical record within the EMF during the employee's federal service. Information described in Section 1.1, with the exception of PII, is entered into a password protected spreadsheet. This spreadsheet is shared with OHA and OSEP, enabling the Department to track the spread of the H1N1 virus in its workforce, improve its delivery of medical care, protect the health of the DHS workforce and to report any adverse effects of treatment to the FDA's MedWatch Program.

2.2 What types of tools are used to analyze data and what type of data may be produced?

There are no data analysis tools associated with the issuance of this SOP or the collection of SOP associated information. OHA, OSEP, and the FDA will be given non-personally identifiable aggregate data to track outbreaks and adverse reactions, which may be used in pattern-recognition and mapping tools to aid in analysis. None of these activities would be traceable back to an individual.



2.3 If the system uses commercial or publicly available data please explain why and how it is used.

There is no commercial or publicly available data associated with the issuance of this SOP of the collection of SOP associated information. OHA, OSEP, and the FDA will be given non-personally identifiable aggregate data to track outbreaks and adverse reactions, which may be used in pattern-recognition and mapping tools to aid in analysis. None of these activities would be traceable back to an individual.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The primary privacy risk associated with administering medical care to DHS employees is the possibility of information being improperly used beyond the reason for which it was collected. The major mitigation of this risk is the fact that these records are kept in hard copy at provider sites separate from the employee's general personnel file(s). Designated DHS medical care providers record PII on the hard copy SF 558 as part of their standard patient care practices and forward on to OHA and OSEP only non-PII information. Component providers and their staffs keep this PII in paper form in secure facilities and only medical personnel and their administrative staffs have access to these files.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

All information recorded in the SF 558s (described in 1.1) is retained by Components in EMFs. The password protected spreadsheets containing this information, with the exception of PII, are retained by OHA and OSEP.

3.2 How long is information retained?

Pursuant to OPM/GOVT 10, the EMF, which contains the SF 558 information and the Patient Consent form, is maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center for storage, or as appropriate, to the next employing federal agency.



Within 90 days after the individual separates from the federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-1(21).

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Information collected pursuant to the SOP is covered under General Schedule 1, Civilian Personnel Files, Section 21, Employee Medical Folder.²

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The length of time associated with the retention of information collected pursuant to this SOP is determined by General Records Schedule 21. Privacy risks associated with the retention of information in EMFs are minimal, and DHS seeks to mitigate these risks by maintaining these records in secured facilities and ensuring that only those personnel providing medical treatment, and their administrative staffs, have access to these files.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The de-identified information (described in 1.1) is shared with OHA and OSEP to enable the Department to track the spread of the H1N1 virus in its workforce, improve its delivery of medical care, protect the health of the DHS workforce and to report any adverse effects of treatment to FDA's MedWatch Program, which monitors the safety of human medical products.

4.2 How is the information transmitted or disclosed?

The subject information is generally shared via a password protected spreadsheet, with PII not included.

² More information on the Employee Medical Folder is available at <http://www.archives.gov/records-mgmt/ardor/grs01.html>



4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

There are risks inherent in sharing health related information. Seeking medical care for H1N1 infection or exposure is voluntary, and therefore supplying information needed to facilitate evaluation and treatment is also voluntary. Internal sharing of this health information is minimal (only to OHA and OSEP) and information supplied does not include PII. The privacy risks of collecting and retaining health information to facilitate treatment of H1N1 related cases are outweighed by the risks of not providing such treatment in the face of a pandemic which has the potential to interrupt continuity of operations.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information described in Section 1.1, with the exception of PII, may be shared with FDA's MedWatch Program, which monitors the safety of human medical products.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Sharing of PII outside of the Department is not necessary. The only instance in which the PII collected via this SOP would be shared outside the Department would be when the EMF is shared with or transferred to another Department, such as at the employee's request if he were to work for another agency that requires EMFs.



5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information described in Section 1.1, with the exception of PII, may be shared with FDA's MedWatch program. This sharing will generally be conducted via email with password protected attachments.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The information (described in Section 1.1) is shared only with FDA's MedWatch program to track potential adverse effects of H1N1 treatment. The privacy risks inherent in sharing this information, which are minimal because PII is not shared, are outweighed by the risks of not tracking potential adverse effects of treatment for H1N1.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Eligible employees seeking treatment for H1N1 infection and/or exposure are notified of their right to decline treatment and are required to sign DHS Form 5201, Antiviral Medication Consent – Declination, which verifies that they understand this right. In addition, prior to any evaluation taking place, eligible employees requesting treatment shall acknowledge receipt of the attached Privacy Act Statement (in Appendix A). Eligible employees are always present at the time this information is collected and are provided the required notification by the OPM/GOVT-10 Employee Medical File System of Records Notice, DHS/ALL-002 (71 FR 3536) which covers the collection of such occupational medical records.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Eligible employees have the right to decline to give information by declining evaluation and treatment.



6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Although an eligible employee who received medical treatment from a designated DHS medical care provider may not consent to particular uses of the information collected, the information which contains PII is kept on file within the Component in secure facilities and is retrieved only in the event that DHS learns of a problem with the administered medication which requires notification of the affected employee.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Eligible employees seeking treatment for H1N1 infection and/or exposure are notified of their right to decline treatment, and therefore their right to decline to provide health information. The Department reduces the privacy risks associated with the collection of this information by keeping all PII collected secured by locking file cabinets or locked file rooms within the Component medical facility that directly collects the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

All employees have access to their EMFs through their respective personnel departments.

In addition, the Freedom of Information Act (FOIA) and the Privacy Act allow individuals to gain access to their own information. Specific information on how to do so is posted on the DHS public-facing website at www.dhs.gov/foia under "How to Submit a FOIA Request."

7.2 What are the procedures for correcting inaccurate or erroneous information?

There are no standardized DHS procedures for correcting inaccuracies in EMFs. Employees may periodically review their EMFs and work with their respective personnel departments to resolve any perceived inaccuracies in their file. As noted above, employees can also file requests under the FOIA and the Privacy Act to gain access to their own information.



Specific information on how to do so is posted on the DHS public-facing website at dhs.gov/foia under "How to Submit a FOIA Request."

7.3 How are individuals notified of the procedures for correcting their information?

N/A

7.4 If no formal redress is provided, what alternatives are available to the individual?

Formal redress is provided as outlined above. Employees may periodically review their EMFs and work with their respective personnel departments to resolve any perceived inaccuracies in their file.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There are no privacy risks associated with the redress available to individuals.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Those who have access to eligible employees' EMFs (i.e., medical care providers and their staffs) have access to the information collected pursuant to the SOP.

8.2 Will Department contractors have access to the system?

Contractors who have a role in the medical evaluation and treatment of employees (and administrative aspects of that care) may have access to this information.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS personnel are required to participate in annual privacy training.



8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

No. The SOPs and collection do not involve an IT system and so are not subject to IT security requirements.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The technical safeguards that components use to safeguard EMFs are in place to protect this information.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Since eligible employees already have EMFs which contain sensitive PII, the implementation of OHA's SOP does not create additional privacy risks.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

Components maintain EMFs in paper form, and these documents are kept in locked facilities at all times.

9.2 What stage of development is the system in and what project development lifecycle was used?

N/A



9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Responsible Officials

Colleen O'Keefe, Privacy Officer
Office of Health Affairs
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security



Appendix A

Privacy Act Statement: DHS's Use of Your Information

Principal Purposes: When you are treated by a designated DHS medical care provider for influenza-like symptoms or probable exposure to H1N1 influenza, the designated DHS medical care provider collects your full name, duty or home address, employee identification number (which may be your Social Security number), signature, and details about your condition and treatment. The designated DHS medical care provider uses this information to identify you and may use it to follow up with you regarding your treatment.

Routine Uses and Sharing: In general, your provider will not use this information for any purpose other than the *Principal Purposes*, and will not share this information within or outside their facility. Only de-identified, aggregate data may be shared within the Department and other agencies to track adverse effects to treatment. In addition, in certain circumstances DHS may share this information on a case-by-case basis as required by law or necessary for a specific purpose, as described in the OPM/GOVT-10 Employee Medical File System of Records Notice, DHS/ALL-002 (71 FR 3536).

DHS Authority to Collect This Information: DHS requests that you voluntarily submit this information under its following authorities: Subpart E of Title 5 of the Code of Federal Regulations, Employee Medical File System Records (2009).

Effects of Not Providing Information: You may opt not to provide the requested information or to provide only some of the information the provider requests. If you opt not to provide some or all of the requested information, the provider may not be able to administer your treatment.

Accessing and Correcting Information: If for any reason you wish to access or correct the information provided to the designated DHS medical care provider, you may go to the designated DHS medical care provider to request access. If you are unable to access the information from the designated DHS medical care provider, then you may direct your request in writing to the appropriate FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." Additional instructions are available at that website and in the OPM/GOVT-10 System of Records Notice, referenced above.