



Privacy Impact Assessment

for the

Preventing Infectious Disease at DHS Facilities During Declared Public Health Emergencies

DHS Reference No. DHS/ALL/PIA-088

December 21, 2020



**Homeland
Security**



Abstract

The U.S. Department of Homeland Security (DHS) has issued discretionary guidance to its Components designed to prevent the spread of infectious disease or illness among its workforce in the event of a declared public health emergency. These processes include workforce accountability tracking, basic health screening of individuals attempting to enter to DHS facilities, laboratory testing of personnel and visitors scheduled to occupy or visit certain DHS facilities, and contact tracing to identify members of the DHS workforce or visitors who might have been exposed while at a DHS worksite. DHS is conducting this Privacy Impact Assessment (PIA) because some of these processes involve the collection and use of personally identifiable information (PII).

Introduction

DHS must ensure the safety of its workforce,¹ especially when the Secretary of the Department of Health and Human Services (HHS) or a responsible designated state official declares a public health emergency.² Responses to public health emergencies vary depending on the nature of the emergency. In the context of a pandemic disease, DHS takes the extraordinary precaution of prohibiting access to its facilities by those who pose a substantial risk of infecting others. DHS³ has therefore developed discretionary guidance for its Components on the collection of certain health-related information from its personnel,⁴ as well as from visitors to DHS facilities, during an HHS- or state-declared public emergency involving infectious disease or illness. DHS may collect this information for the following purposes: 1) personnel status for workforce accountability; 2) basic health screening of individuals as a condition to entering DHS facilities; 3) contact tracing efforts; and 4) laboratory testing of individuals scheduled to occupy certain DHS facilities or fulfill certain DHS missions. This PIA discusses DHS guidance regarding these types of collections. Individual DHS Components may describe in an appendix if their efforts in these areas differ due to their unique mission needs and responsibilities.

¹ See, e.g., DHS Chief Medical Officer's authorities pursuant to 6 U.S.C. § 350 and 6 U.S.C. § 597.

² The Secretary of HHS may, under section 319 of the Public Health Service (PHS) Act (codified at 42 U.S.C. § 247d), declare that: 1) a disease or disorder presents a public health emergency; or 2) that a public health emergency, including significant outbreaks of infectious disease or bioterrorist attacks, otherwise exists. The declaration lasts for the duration of the emergency or 90 days but may be extended by the Secretary. Congress must be notified of the declaration within 48 hours.

³ Guidance is developed based on input from all relevant offices, to include the Office of the Chief Human Capital Officer Workforce Health and Safety Division, DHS Office of General Counsel, DHS Office of the Chief Information Officer, and DHS Privacy Office, as well as input from respective Component offices, as necessary.

⁴ "DHS personnel" in this context includes DHS employees, contractors, detailees, interns, volunteers, mission support individuals, and long-term trainees.



Workforce Accountability

During a declared public health emergency, the health and safety of the DHS workforce is more important than ever; to ensure both continuity of operations and the well-being of DHS personnel and their families. Workforce accountability allows the Department to properly staff resources, manage and distribute personal protective equipment (PPE), and coordinate Department response efforts. Further, the DHS Chief Medical Officer is responsible for providing consultation to and coordination with Component medical operators on issues that might affect individuals' fitness for duty.⁵

In order to fulfill these responsibilities and provide continued guidance allowing implementation of appropriate safeguarding measures, DHS and Component leadership require data on employee workforce status, potentially requiring the creation of a tracking system. A tracking system allows management to track employee status and cases, providing leadership with a centralized view of cases across the agency.⁶ DHS may use pre-existing workforce accountability systems, or develop incident-specific systems, that allow for personnel and supervisors to input their status or those that they supervise directly into a tracker.

If there is believed to be a known or possible encounter with the disease or illness, a DHS employee or supervisor may be able to log on to a tracker and submit a case. Information maintained as part of the case would include contact information about the impacted individual (e.g., name, email address), duty location information (e.g., work address, organization), and other case-related information (e.g., possible contact/contraction dates; test result; other medical responses, such as hospitalization or quarantine; work status, such as teleworking or unable to perform duties). It may also be necessary for personnel to provide their status absent a confirmed case or connection to the disease or illness. For example, it may be necessary for managers and supervisors to know of their direct reports' statuses or the potential impact return-to-work efforts may have. In the later phases of a declared public health emergency response, this could include additional information such as an individual's vaccine status.

Access to this individual-level data would be limited to those with a need-to-know, such as first- and second-line supervisors (and other appropriate parties, such as a Component's Pandemic Response Team) to allow for effective management of their personnel.

⁵ See 6 U.S.C. § 597(c), which states that, "The 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 - (1) 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; (2) providing operational medical support to all components of the Department; ..."

⁶ DHS uses these types of trackers to display data for other incidents affecting the workforce, such as hurricanes.



Analytics and Decision Making

Information collected by workforce accountability trackers may be used to inform return-to-work models, areas requiring deep cleaning and sanitizing after an exposure, potential building closures, areas for cross-training to avoid work stoppage, other general policy guidance, needed resources and tools, and the effectiveness of specific interventions. PII can be aggregated and displayed for DHS and Component leadership, providing a valuable tool to analyze response and workforce problem areas. These aggregated reports should not contain PII but would contain metrics such as personnel cases/deaths by jurisdiction, cases/hospitalizations by Component/Office, or number of individuals currently quarantined or unable to perform their duties.

Facilities Screening

DHS requires procedures for employees, contractors, and visitors to be screened prior to entering any DHS facility that remains open during a declared public health emergency involving infectious disease or illness. Due to the unique mission needs and responsibilities of Components, these procedures may be developed independently. However, DHS recommends the following procedures be incorporated into these screenings: 1) temperature checks at facility entrances to assess if the individual's body temperature is at a level potentially indicative of infection, and 2) asking individuals a series of questions to assess their recent exposure risk.

Temperature Checks

Components should grant facility access to employees, contractors, or visitors if they have a body temperature below that which could indicate infection with the disease or illness that is the subject of the declared public health emergency. DHS encourages use of no-touch infrared thermometers or thermal camera kiosks/stations for all on-site temperature checks to avoid the need for physical contact. If the employee, contractor, or visitor has a body temperature above the recommended threshold, as determined by the appropriate DHS workforce health and safety offices, Components may deny the individual entry to the facility. No records should be collected pertaining to the individual's identity since the only function of the temperature check is to determine whether entry is appropriate at that specific time. Affirmation of passing the temperature check may be required and can be documented through creation of a badge/sticker with no PII. Access denial on any given day does not mean access is automatically denied for any time period. Individuals who decline to be screened may be denied entry to the DHS facility.

Screening Questions

Components may ask individuals seeking access to DHS facilities during a declared public health emergency questions which might reasonably help determine whether the individual poses a significant risk to the health or safety of others. Typical questions include:



1. Are you experiencing any symptoms of the disease (list symptoms if needed)?
2. Within the past *<however many days the disease might be present prior to manifestation of symptoms>* have you been within *<whatever distance public health officials have determined the disease is easily communicable>* of any person who you know to have had an active or suspected case of laboratory-confirmed *<whatever disease is the subject of the public health emergency>*?
3. In the last *<however many days the disease might be present prior to manifestation of symptoms>*, have you received instructions from a public health authority to self-observe, self-isolate, or self-quarantine?
4. Have you recently returned from travel to any location known to have a high number of confirmed cases or sustained community transmission, such as *<list regions, countries, states, provinces as appropriate>*?

DHS/Components should pose all questions before requesting whether the individual's answer to any of them is affirmative. In turn, individuals should only indicate if their answer to any one of the questions is affirmative without answering each question individually or identifying the specific question to which they are responding. If the individual answers affirmatively after all questions are asked, he or she should be denied access. As with temperature checks, no records should be collected pertaining to the person's identity since the sole purpose is to turn away individuals who might pose a risk at that specific time.

Health Screening Privacy Notice

Upon attempting to enter a DHS facility, the individual should be provided with a hardcopy privacy notice and other notices at the entrance of these facilities where screening will occur. The notice should explain that the individual will be screened by a designated DHS representative or other technology (e.g., thermal camera kiosks/stations) for symptoms of the disease, which may include a temperature check. The notice should explicitly state the specific temperature threshold that would result in denial of entry. The notice should also contain a printed version of the questions to be asked, and it should explain that the DHS representative may ask all the questions as a condition to entry. The notice should specifically instruct the individual to answer "yes" or "no" only once and only after the DHS representative has asked all questions. The notice should further explain that if the individual answers yes, he or she may be denied entry and no further questions or answers would be provided. Finally, the notice should indicate that no information will be recorded, and that refusal to submit to the temperature check or to answer the questions may result in denial of entry.



Contact Tracing

Contact tracing is a process recommended by public health experts during pandemics that involves determining who has contracted or may have been exposed to a suspected or confirmed communicable disease, and then determining who recently interacted physically with that individual. Typically, when a person receives a laboratory-confirmed diagnosis (a “confirmed case”), a trained individual known as a “contact tracer” interviews the confirmed case to ensure he or she is successfully quarantining and to ask with whom he or she has come into close enough and recent contact to potentially transmit the disease. The contact tracer then documents this information and subsequently reaches out to anyone the confirmed case reported as potentially exposed (an “exposed contact”) to request they also quarantine and to ask they provide notification back if any symptoms develop. If any symptoms do develop, the contact tracer will ask the exposed contact for information about close and recent physical contacts, and these secondary exposed contacts may also be interviewed. This process continues until everyone who might have been exposed downstream from a confirmed case is promptly and successfully quarantined—the idea being that if all exposed contacts are quarantined quickly enough, the virus identified in the confirmed case will have nowhere else to spread.

Contact tracing programs at DHS are instituted in response to an HHS - or state-declared public health emergency involving infectious disease or illness. The intent is to quickly identify, isolate, track, alert, and prevent facility outbreaks and exposures. Contact tracing informs implementation of administrative and workplace controls aimed at keeping the DHS workforce safe, protecting mission readiness, and preventing the spread of the disease.

Specific contact tracing efforts are initiated at DHS in response to receiving a report of a confirmed case during the public health emergency. DHS will not contact trace family, personal friends and acquaintances, or other individuals its personnel might have engaged with while outside the workplace; however, contact tracing may involve visitors to DHS facilities.⁷ Furthermore, although participation in DHS’s contact tracing program is strongly encouraged, it is nonetheless completely voluntary, and personnel can always opt not to participate without fear of negative consequences.

⁷ Contact tracing on visitors, who are not DHS personnel, is necessary to protect those individuals, but also DHS personnel. However, a smaller subset of information is required to be collected from visitors, which includes: name; phone number; email address; date(s) and time(s) of entrance and exit from DHS workspaces, facilities, and grounds; name(s) of all individuals encountered; and information indicating plans on entering a DHS workspace, facility, or grounds in the near future. More specific information about this distinction is available in DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records, 85 Fed. Reg. 80127 (December 11, 2020), available at <https://www.dhs.gov/system-records-notice-sorns>.



DHS recommends each Component assign a team of contact tracers to build and sustain a contact tracing network within their organization. These contact tracers receive appropriate information on contract tracing training, their responsibilities, use of appropriate tools, and managing case load and workflow. Additional training requirements may include privacy awareness, IT security awareness, handling medical and other sensitive information, and telephone customer service.

DHS recommends contact tracers perform the following duties:

- Conduct telephone interviews with confirmed cases following pre-approved protocols and scripts;
- Collect and record information from confirmed cases and input this information into specialized contact tracing forms or online contact tracing reporting tools;
- Conduct telephone interviews with exposed contacts following pre-approved interview scripts and protocols and provide pre-approved information about isolation/quarantine;
- Provide a tracking worksheet for exposed contacts to self-monitor their symptoms over the relevant period during which the disease could develop;⁸
- Maintain daily communications with supervisory contact tracers, who will review a percentage of all interviews to ensure compliance with program objectives and requirements; and
- Conduct in-person investigations into congregate settings, as needed, to determine the risk that DHS personnel might infect others in those settings.

All DHS personnel should be actively encouraged, but are not required, to inform their supervisors or Contracting Officer Representatives (COR) if they receive a laboratory-confirmed positive test result for the disease or illness that is the subject of the declared public health emergency. Supervisors and CORs who receive such reports will direct the confirmed case to isolate from the rest of the workforce, typically by working remotely or by taking sick leave. The supervisor or COR also asks the confirmed case if he or she consents to being contacted and interviewed by a contact tracer. If permission is granted, the supervisor or COR provides the contact tracer with information about the confirmed case.

Contact Tracing Interviews – Confirmed Case

Assuming the confirmed case grants permission to the supervisor or COR to share their contact information with a contact tracer, the contact tracer calls the individual to conduct an interview. The main purpose of the interview is to check on the health status of the confirmed case,

⁸ Use of the worksheet is optional, and the contact tracer instructs the interviewee that it should not be submitted back to DHS.



to obtain a list of exposed contacts who should also be interviewed, and to provide resources describing public health recommendations on quarantine and self-care.

Interviews follow an established script specifically tailored to confirmed cases. The script explains the purpose of the call and includes a detailed privacy notice, which the contact tracer reads verbatim. The privacy notice explicitly states that the collection is voluntary and that no PII will generally be shared outside of DHS,⁹ or with anyone in DHS other than the confirmed case's direct supervisor/COR and a supervisory contact tracer. The script also includes questions to determine whether the confirmed case was at a DHS worksite at any period during which he or she could have transmitted the disease to others. If the confirmed case indicates he or she was at a DHS worksite, the contact tracer then asks the confirmed case to validate information relating to the dates, office locations, and the names of other personnel that were in close enough contact to have potentially been exposed.¹⁰ The contact tracer records this information either on a contact tracing form or in an online contact tracing reporting tool specifically tailored to the epidemiology of the disease.

Regardless of whether the confirmed case was at a DHS worksite while contagious, the contact tracer provides the confirmed case with information to access online training regarding contact tracing, successful quarantine, self-care, and other useful information tailored to the specific disease at issue to assist as necessary. The contact tracer ends the call by reiterating that any information collected will only be used to notify individuals who may have been exposed while at a DHS worksite, and that neither the confirmed case's name nor any other identifiable information will be shared with anyone other than the direct supervisor/COR and a supervisory contact tracer. The contact tracer also requests that the confirmed case call the contact tracer back if he or she remembers other individuals, or DHS locations potentially impacting other unnamed individuals, not mentioned on the call that could have been exposed.

Contact Tracing Interview – Exposed Contact

Once the interview with the confirmed case is complete, the contact tracer begins calling each exposed contact identified by the confirmed case using a pre-approved script tailored to exposed contacts. As before, the contact tracer explains the purpose of the call, reads the same detailed privacy notice, and asks for consent to be interviewed. If the contact declines to give their consent to be interviewed, the contact tracer ends the call. If consent to be interviewed is granted, the contact tracer asks the exposed contact to confirm he or she was at the location or event

⁹ There are circumstances when DHS might be required to share contact tracing records outside of DHS. These are noted in the routine uses listed in DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records, 85 Fed. Reg. 80127 (December 11, 2020), available at <https://www.dhs.gov/system-records-notice-sorn>.

¹⁰ The exact physical proximity will depend on the nature of the disease at issue and should be explicitly referenced in the questioning.



described by the confirmed case. If the exposed contact replies he or she was not at the location or event, the contact tracer ends the call.

However, if the exposed contact confirms he or she was at the relevant location or event, the contact tracer informs the individual that personnel he or she may have been in contact with tested positive for the disease.¹¹ If the exposed contact asks for the identity of the confirmed case, the contact tracer replies by stating that the information cannot be shared to protect the individual's privacy, and instead reiterates the date and approximate time during which the possible exposure occurred. The contact tracer provides the same contact tracer training and information regarding successful quarantine and self-care that was referenced on the call to the confirmed case.

Additionally, the contact tracer asks the exposed contact for information about other personnel who were present with him or her at the exposure location or event, including first and last name, specific locations, contact information, and dates of last potential exposure. Again, this information is recorded either on a contact tracing form or in an online contact tracing reporting tool in preparation for further interviews.

The contact tracer also asks if the exposed contact reported to a DHS worksite at any time after the location or event identified by the confirmed case. If the exposed contact answers yes, the contact tracer collects and records information about any exposed contacts at these subsequent appearances so they can also be interviewed. The contact tracer further asks if the employee anticipates coming to a DHS worksite at any point in the future when they could potentially still be contagious. If the exposed contact answers yes to this question, the contact tracer directs the exposed contact to discuss alternative work options and other remediation strategies to avoid needing to physically access DHS facilities.

The contact tracer also asks the exposed contact if he or she is currently experiencing any symptoms associated with the disease. If the exposed contact answers yes, the contact tracer provides additional information related to managing the symptoms and offers resources relevant to tracking the progression of the disease, including a symptom self-monitoring worksheet to assist with identifying any symptoms not yet experienced that might manifest during the relevant isolation period. The contact tracer explicitly states that the worksheet is optional and should not be returned to DHS.

The contact tracer ends the call by specifying the exact dates of the employee's isolation period based on last possible exposure date at a DHS worksite. The exposed contact should not be allowed to physically return to work at a DHS facility until the isolation period ends.

¹¹ In some cases, an individual confirmed positive may consent to having their information shared to these exposed contacts.



Online Contact Tracing Reporting Tools

DHS is also using and making available to Components an online contact tracing reporting tool that supports the DHS Contact Tracing Program. The online contact tracing reporting tool allows employees to submit exposure-related information about themselves, supervisors to submit exposure-related information about their employees, and CORs to submit exposure-related information about their contractors. A privacy notice prominently appears on the landing page of the tool explaining the authorities permitting the collection, the purpose of the collection, routine uses, and consequences for failing to provide information.¹² Users must validate they have read and understand the privacy notice before proceeding to use the tool. The contact tracing tool collects the following information:

- Confirmed Case (to be completed by the confirmed case or their supervisor/COR):
 - Name (last, first);
 - Work email;
 - Work phone;
 - Best phone number and phone type (business, home, mobile);
 - Supervisor/COR name (last, first);
 - Supervisor/COR work phone;
 - Supervisor/COR work email;
 - Reporting experiencing symptoms (Y/N);
 - Confirmed positive case (Y/N);
 - Current work status (e.g., administrative leave, sick leave, teleworking, in the office, deployed to the field) and affiliated leave status information;
 - Last day in DHS facility (YYYY-MM-DD); and
 - Date of symptoms onset (YYYY-MM-DD).
- Return to work (to be completed by the confirmed case and validated by their supervisor/COR):¹³
 - Required period has elapsed since recovery (Y/N);

¹² In this case, there are no consequences for failing to provide information since the DHS Contact Tracing Program is completely voluntary, albeit strongly encouraged.

¹³ In some cases, a supervisor may request that an employee (for example, a high-risk individual as defined by the CDC) provide medical documentation that he or she is cleared to return to work. Prior to doing so, supervisors consult with their respective human resources and legal offices.



- Has a return to work plan been submitted to your supervisor/COR? (Y/N);
- Has required period elapsed since symptoms first appeared? (Y/N); and
- Date of planned return (YYYY-MM-DD).
- Phone log (to be completed by contact tracers):
 - Date/time of call; and
 - Notes from call.
- Work location activity (to be completed by the contact tracer, the confirmed case, or the confirmed case's supervisor/COR):
 - Date of activity (YYYY-MM-DD);
 - Number of days before onset; and
 - Location(s) of activity (e.g., DHS duty location, building/floor/conference room, desk, or common area).
- Exposed individuals in close contact (to be completed by the contact tracer, the confirmed case, or the confirmed case's supervisor/COR):
 - Name (last, first);
 - Work email;
 - Phone number and phone type (business/home/mobile);
 - Contact type (confirmed case/exposed contact);
 - Location(s) of contact (building/floor/desk); and
 - Date of last exposure to DHS personnel (YYYY-MM-DD).

Components that decide not to use some configuration of the HQ online contact tracing reporting tool have the option of developing their own online contact tracing reporting tools. These tools are vetted and approved by the DHS Privacy Office, and other appropriate oversight offices, to ensure their architecture and use will adequately reflect the DHS Fair Information Practice Principles (FIPPs).¹⁴

Access and Information Sharing

Contact tracers will only have access to records of the cases they handle, whether they be contact tracing forms or records contained in online contact tracing reporting tools. Access by

¹⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), available at <https://www.dhs.gov/privacy-policy-guidance>.



supervisory contact tracers will be limited to all records handled by any of the contact tracers that report to them. First-line supervisors and CORs will only have access to paper or online records of their direct reports. DHS management officials should only be able to access anonymized data within the online tools for analytics and decision making. In all cases, anyone with permissions within the online contact tracing reporting tools will only have access and edit rights to data for which they have a valid need-to-know. PII on contact tracing forms and online contact tracing reporting tools is never shared outside of DHS except for circumstances specified in the applicable system of records notice (SORN): DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records.¹⁵

Analytics and Decision Making

Information collected by contact tracers during interviews and entered onto contact tracing forms or in online contact tracing reporting tools may be used to inform return-to-work models, areas requiring deep cleaning and sanitizing after an exposure, potential building closures, areas for cross-training to avoid work stoppage, other general policy guidance, needed resources and tools, and the effectiveness of specific interventions. PII may also be aggregated into metrics to aid in program evaluation and decision making such as time to interview from symptom onset and from diagnosis, proportion of contacts interviewed, median number of contacts elicited, proportion with no contacts elicited, proportion of contacts notified, time from first potential exposure to notification, daily proportion of contacts whose status is evaluated, proportion of contacts reporting symptoms within 24 hours of initial onset, proportion of contacts who complete their full self-monitoring period, and percentage of new cases arising among contacts during the self-monitoring period. Unaggregated PII should not be used or shared for any purposes related to analytics and decision making.

Workforce and Visitor Testing

In order to maintain a strong mission readiness posture, some Components may conduct focused or ongoing laboratory testing of the workforce (to include visitors to DHS facilities) for the disease that is the subject of a public health emergency. In these cases, DHS issues guidance to Components on how to procure test kits and how to conduct the testing. Whether laboratory testing is appropriate in a specific situation will depend on factors associated with the specific disease, including the accuracy and availability of test kits, the length of time the disease is communicable before symptoms arise, the proximity of individuals who will be occupying the facility, and whether the disease is treatable in the event of a positive test result.

¹⁵ See DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records, 85 Fed. Reg. 80127 (December 11, 2020), available at <https://www.dhs.gov/system-records-notice-sorns>.



Any laboratory testing guidance is collaborated among the responsible workforce health and safety offices and appropriate oversight office (e.g., legal, privacy). However, any guidance DHS issues includes the following at a minimum:¹⁶

- Tests may only be administered to the DHS workforce under the advice and consent of a physician and only by individuals with proper training and certification;
- All DHS Components must obtain medical clearance by a DHS Medical Officer, in concert with senior officials, prior to procuring test kits for the DHS workforce;
- Component requests for clearance to procure test kits must describe a testing plan; results notification plan, staffing impact considerations; plan for aggregate reporting of results to HQ;¹⁷ records management and retention capabilities; and appropriate physical and security controls;
- Test subjects must complete a consent form prior to taking a test. The consent form should contain a detailed privacy notice explaining the authorities, purpose, and routine uses of the collection, as well as any consequences that would result from refusal to take the test;
- Test results of personnel should be stored in the person's medical file, and under no circumstances should the test results be stored or recorded in the individual's regular personnel file;
- Priority for laboratory testing should be given to occupants of DHS facilities that support national security operations, mission essential functions, and other activities essential to continuity of government;
- Subjects should be notified in a timely manner once test results are obtained;
- Personnel who test positive should be provided U.S. Centers for Disease Control and Prevention (CDC) - approved guidance and instruction for managing and treating the disease;
- Personnel should be directed to consult with their supervisor or COR on appropriate work-related flexibilities to ensure no further spread of the disease on DHS premises. This could include use of telework or sick leave until the subject is no longer contagious; and

¹⁶ These requirements may change slightly depending on the nature of the declared public health emergency. For example, other declared public health emergencies may not require procurement testing kits be cleared by DHS Headquarters or DHS Medical Officer (for example, in a localized public health emergency affecting one Component's duty location).

¹⁷ The aggregate reports should not contain PII.



- Personnel who test positive should sign a separate consent form prior to DHS dispensing any medication to treat the disease.

It may also be necessary for DHS personnel to be tested depending on their job responsibilities. The DHS mission does not stop due to a declared public health emergency. For example, U.S. Customs and Border Protection (CBP) is still responsible for securing the nation's borders, the Federal Emergency Management Agency (FEMA) still responds to and mitigates manmade and natural disasters, and the Transportation Security Administration (TSA) still safeguards the nation's transportation systems to ensure freedom of movement for people and commerce. Given DHS's dispersed workforce across the nation and its coordination with other federal, state, and local agencies, there may be instances during a declared public health emergency where DHS personnel are required to address additional requirements, or testing, before they are able to fulfill their local responsibilities.

For example, FEMA deploys personnel to disaster recovery facilities in localities that have just experienced disasters. Depending on the state and local requirements of that jurisdiction, it may be required that FEMA personnel undergo preventative testing before being deployed. In these cases, Components may conduct in-house testing or require the acquisition of the commercial services of a dedicated laboratory testing provider. As is the emergent nature with any public health emergency, the testing requirements would be developed specific to that incident. "At home" testing and sample collection kits could be provided to identified DHS personnel and the corresponding laboratory testing and result generation capability could be conducted by the third-party or DHS could facilitate personnel visiting testing locations/laboratories. Specific to the FEMA example, once the employee receives their results, they would then be able to show that result to the agency or governing body charged with allowing access to local facilities.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974¹⁸ articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.¹⁹

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.²⁰ The FIPPs account for the

¹⁸ 5 U.S.C. § 552a.

¹⁹ 6 U.S.C. § 142(a)(2).

²⁰ See *supra* note 14.



nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208²¹ and the Homeland Security Act of 2002, Section 222.²² Given that DHS's prevention efforts reflect a programmatic approach rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of DHS operations performed during declared public health emergencies involving infectious disease to protect its workforce and facilities.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

Workforce accountability trackers contain information that is input largely by the individuals themselves, or at times the individual's supervisor. The tracker should maintain a detailed privacy notice identifying the authorities, purpose, and routine uses for the collection, as well as any consequences for failing to provide information.

Individuals, to include visitors, attempting to enter a DHS facility during a declared health emergency should be shown a hardcopy privacy notice explaining the screening process, including the temperature threshold and the specific questions to be asked. The notice should also contain instructions on how and when to answer the questions and should explain that no PII will be required or recorded as part of the screening process. The notice should also explain the authorities, purpose, and routine uses of the collection, as well as the consequences of refusing to be screened. The notice should also provide information to individuals on what they should do if they are denied entry.

Contact tracers are required to read a detailed privacy notice to all individuals they interview. A detailed privacy notice also appears on online contact tracing reporting tools that confirmed cases and supervisors/CORs may use to submit information about themselves or their direct reports. These privacy notices contain the authorities, purpose, and routine uses for the collection, as well as any consequences for failing to provide information.

Individuals subject to laboratory testing receive a privacy notice printed on the test consent form, as well as on all consent forms issued prior to DHS dispensing any medication to treat the

²¹ 44 U.S.C. § 3501 note.

²² 6 U.S.C. § 142.



disease in the event of a positive test result. Again, these notices should provide the authorities, purpose, and routine uses of the collection, as well as the consequences of failing to be tested.

Notice is also provided by this PIA, as well as by DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records. Further, specific incident guidance is distributed by DHS and Component leadership during public health emergencies.

Privacy Risk: There is a risk that individuals may not know how their information is used when collected due to a declared public health emergency.

Mitigation: This risk is mitigated. DHS takes several steps to ensure transparency in its response efforts to declared public health emergencies. Systems or technical solutions used to track data related to public health emergencies generally requires information to be input by individual personnel or their first- or second-line supervisors. Those systems and technical solutions have privacy notices to inform individuals how the information will be used and guidelines to help them provide the appropriate information.

If access to DHS facilities requires additional screening, DHS provides notice to advise personnel and visitors of new requirements. This may include instructions/handouts, signage, email notification of procedural changes, and privacy notices.

DHS has developed a script for contact tracers to use when coordinating contact tracing efforts with interviewees. This script includes information about the DHS Contact Tracing Program, the purpose of the call, and a detailed privacy notice. Further, DHS has provided information resources on the DHS Contact Tracing Program, both available on internal DHS websites and directly distributed to personnel.

During testing efforts, consent forms should contain a privacy notice and other information about how the testing process works and what individuals can expect (e.g., results timeframe, medical care).

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

DHS personnel and visitors attempting to access DHS facilities are provided a privacy notice explaining the authorities, purpose, and routine uses of the collection, and are explicitly informed that no PII will be collected about them from the screening process and the only negative consequence that may result from what information they provide is denied access to the facility. Their voluntary decision to submit to a temperature check and to answer health screening questions as a condition to accessing the facility is again deemed a reflection of their consent. The screening



information collected is no more sensitive than the information DHS already requires personnel and visitors to submit when accessing DHS facilities under normal circumstances. Denied access on any given day does not mean access is automatically denied for any time period. If a DHS employee or contractor is denied entry, they are provided information on contacting their supervisor or COR and what actions may be required for the workday (e.g., taking leave or teleworking).²³

Confirmed cases and exposed contacts voluntarily provide their information to contact tracers only after receiving notification that the program is voluntary and that no negative consequences will result from failing to participate. They are also informed prior to collection of the authorities, purpose, and routine uses of the information they will be asked to provide. Their decision to voluntarily provide their information is thus deemed a reflection of their prior consent. Confirmed cases and exposed contacts can reach back to the contact tracers assigned to their case at any time for access, correction, or redress regarding any PII they provided. Confirmed cases and exposed contacts in Components that use the online contract tracing reporting tools should be provided access to the online reporting tools and a direct means to correct their own information within the reporting tools. Similar consent and redress processes are in place for workforce accountability trackers. Generally, individuals themselves, or their direct supervisors, input the data and can access and correct it at any time.

Individuals required to provide specimens for laboratory testing as a condition of visiting or working in certain DHS facilities are provided a written consent form prior to supplying the specimen(s), and another written consent form prior to provision by DHS of any treatment.²⁴ These consent forms also provide the authorities, purposes, routine uses, and consequences of declining to submit specimens for testing. The subject may contact the Component workforce health and safety office that collected the specimen(s) and consent forms for correction of PII or redress.

Privacy Risk: There is a risk that individuals may not have appropriate redress opportunities related to facility access screenings or specimen testing.

Mitigation: This risk is mitigated. The DHS Privacy Office works extensively with the Federal Protective Service (FPS), workforce health and safety officials, and other appropriate offices to determine the requirements and information needed to safely and effectively process DHS personnel and visitors into DHS facilities. This includes developing Facility Entry Health Screening Privacy Notices, distributing DHS-Wide Workforce Guidance related to the restriction

²³ If an individual suffers from a chronic medical condition that causes disease or illness-like symptoms, individuals may speak with their supervisor about facility access and reasonable accommodation.

²⁴ Although most testing across DHS personnel would be voluntary, there are some situations or populations where it is mandatory. For example, U.S. Coast Guard (USCG) military personnel may be required to undergo mandatory testing in accordance with USCG authorities. Situations that deviate from what is outlined in the PIA are discussed in Component-specific appendices, as necessary.



of access or partial closure of DHS facilities, and meeting the necessary compliance requirements to ensure adherence to DHS privacy policy. Part of this work involves determining the appropriate repercussions of a denial of access or a positive test, and the ability of individuals to contest or correct those results.

Each public health emergency may be treated differently (e.g., the thresholds for denying access, the need for testing), but the general screening process remains largely the same. Access denial on any given day does not mean access is automatically denied for any time period.²⁵ Individuals who meet or exceed the screening thresholds should be advised to contact their supervisor or COR to determine how they should proceed for the workday. Information may be relayed to individuals verbally, electronically, or through a “Denied Access Information Paper.” No PII is collected during these screening processes.

With respect to testing, most scenarios are voluntary, but may be required to participate in the activity or job responsibility requesting the test (e.g., FEMA deployment, training course at the Federal Law Enforcement Training Centers (FLETC)). If an individual’s test is positive, they may not be able to participate in the activity or job responsibility. However, the individual may be retested, as false positive results can occur, or can participate when they overcome the disease or illness (which may include the individual completing a period of quarantine/self-isolation). All tested individuals are provided with consent forms and information that outlines how they should proceed depending on a positive or negative test. These individuals will generally be required to isolate from the rest of the workforce, typically by working remotely or by taking some type of leave, until such time as they are determined to be disease - or illness-free in accordance with the latest CDC, DHS, or health agency guidance. Individuals cannot be reprimanded or disciplined for testing positive.

Further, individuals seeking access or amendment to any record contained in a DHS system of records may submit a Privacy Act (for U.S. citizens and Lawful Permanent Residents) or Freedom of Information Act (FOIA) (for all individuals) request to the respective Component FOIA Office which can be found under “Contact Information” at <https://www.dhs.gov/freedom-information-act-foia>.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The privacy notices on contact tracing forms and online contact tracing reporting and workforce accountability tools, the hardcopy privacy notice provided to individuals during screening at entrances to DHS facilities, and the privacy consent forms for laboratory testing and

²⁵ Depending on the nature of the health emergency, and under the guidance of DHS workforce health and safety officials, individuals may be able to re-take a temperature reading if there is reason to believe it may be inaccurate.



provision of treatment all articulate the purposes for which PII will be used. Generally, authorities to collect this information include: Section 319 of the Public Health Service (PHS) Act (42 U.S.C. § 274d); Coronavirus Aid, Relief, and Economic Security (CARES) Act, Pub. L. No. 116-136, Div. B., Title VIII, sec. 18115, 134 Stat. 574 (codified in 42 U.S.C. § 274d note); DHS Chief Medical Officer's authorities pursuant to 6 U.S.C. § 350 and 6 U.S.C. § 597; 6 U.S.C. §464; 21 U.S.C. § 360bbb-3; 40 U.S.C. § 1315; American with Disabilities Act, including 42 U.S.C. § 12112(d)(3)(B), 29 CFR 602.14, 1630.2(r), 1630.14(b)(1), (c)(1), (d)(4); Medical Examinations for Fitness for Duty Requirements, including 5 CFR Part 339; Workforce safety federal requirements, including the Occupational Safety and Health Act of 1970, Executive Order 12196, 5 U.S.C. § 7902; 29 U.S.C. Chapter 15 (e.g., 29 U.S.C. § 668), 29 CFR Part 1904, 29 CFR 1910.1020, and 29 CFR 1960.66; Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. §§ 2000ff to ff-11, and 29 CFR Part 1635; and United States Coast Guard authorities, including 10 U.S.C. Subtitle A, Part II, Chapter 55, Medical and Dental Care, as applicable, 14 U.S.C. § 504(a)(17), 14 U.S.C. § 936, 14 U.S.C. § 3705, 42 U.S.C. § 253, 32 CFR Part 199, and 42 CFR 31.2 - 31.10.

The privacy notices contained on contact tracing forms and online contact tracing and workforce accountability reporting tools specify that DHS will collect the information for the purpose of maintaining and ensuring a healthy workforce and a safe DHS workspace. Contact tracing privacy notices also state that the information will help the Department in slowing down the spread of infectious disease by notifying those individuals who may have been exposed so they can take appropriate precautions and minimize exposure for others. The hardcopy privacy notices provided to personnel and visitors subject to screening at entrances to DHS facilities explain that the subject will be screened by a designated DHS representative for symptoms of the disease to determine whether to grant or deny access. Privacy notices appearing on laboratory testing consent forms explain that the collection will be used to determine whether the subject has the disease that is the subject of the public health emergency so that efforts can be taken in the event of a positive result to mitigate its spread in DHS facilities and to provide appropriate guidance and care.

Further, each form, tracking system, reporting tool, or testing initiative undergoes a privacy review (as well as reviews by other appropriate oversight offices) to ensure adherence to this PIA, the applicable SORN, and DHS privacy policy.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Temperature checks and screening questions at DHS facility entrances are informed by CDC guidance indicating effective strategies to identify risk of transmitting disease and illness.



No PII is necessary for collection during these processes. Temperature screening tools do not require the storage of any PII or images, and screening subjects are directed to indicate a single “yes” or “no” response only after all required questions are asked so that answers cannot be tied to specific screening questions.

All information collected on contact tracing forms and the online contact tracing reporting and workforce accountability tools is relevant and necessary for identifying confirmed cases and exposed contacts; recording contact information in preparation for interviews and follow-up by contact tracers; tracking symptoms and health status for evaluating when personnel can safely return to work; and informing supervisors, CORs, facilities managers, workforce health and safety officials, and leadership of the need for deep cleaning and sanitization, the need for administrative and engineering workplace controls, areas for cross-training to avoid work stoppage, and metrics to assist with policy guidance and evaluation of specific interventions.

Information collected in preparation for laboratory testing is limited to that which is necessary to identify the test subject, conduct the test, and report results. Furthermore, testing is typically only required of a subset of personnel who physically report to facilities that support national security operations, mission essential functions, and other activities critical to continuity of government. The CDC parent agency, HHS, may require certain reporting with each administered test. For example, HHS may require laboratory entities to report specific data for all testing completed, for each individual tested, within a certain timeframe of results being known or determined, or on a daily basis to the appropriate state or local public health department based on the individual’s residence or testing location. This could include testing metadata (e.g., performing facility information, date), demographic information of the individual (e.g., age, race, gender), or identifying information of the individual (e.g., name, address, date of birth). Contact information is generally optional, and DHS should refrain from providing that information when conducting testing or procuring testing services through a third-party.

DHS is in the process of developing a records schedule for declared public health emergency records. However, to the extent applicable, and to ensure compliance with the Americans with Disabilities Act of 1990 (ADA), the Rehabilitation Act of 1973, and the Genetic Information Nondiscrimination Act of 2008 (GINA), medical information is maintained on separate forms and in separate medical files and is treated as confidential. This means that medical information and documents are stored separately from other personnel records. As such, the Department keeps medical records for at least one year from creation date. Further, any records created in response to a declared public health emergency and incorporated into an occupational individual medical file pursuant to the Occupational Safety and Health Act (OSHA) are maintained in accordance with 5 CFR Part 293.511(b) and 29 CFR 1910.1020(d), and must be destroyed 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer, in accordance with National Archives and Records Administration (NARA)



General Records Schedule (GRS) 2.7, Item 60, and NARA records retention schedule DAA-GRS-2017-0010-0009, to the extent applicable. Visitor processing records are covered by GRS 5.6, Items 110 and 111, and must be destroyed when either two or five years old, depending on security level, but may be retained longer if required for business use, pursuant to DAA-GRS-2017-0006-0014 and -0015.²⁶

Privacy Risk: There is a risk that DHS will collect more information than is necessary to effectively protect the workforce and DHS facility visitors during a declared public health emergency.

Mitigation: This risk is partially mitigated. All information collected on contact tracing forms and the online contact tracing reporting and workforce accountability tools is relevant and necessary. However, because declared public health emergencies are generally unprecedented events that can fluctuate rapidly, the information collected over the course of an emergency may change or no longer be needed. Workforce health and safety offices work with their respective Component privacy offices (and other appropriate oversight offices) to ensure that all privacy equities are met; to include adherence to DHS privacy policy, the Privacy Act, Departmental guidance, and this PIA.

No PII is maintained for facilities screening. DHS provides only the PII necessary and required, generally in accordance with HHS or other health agency requirements, to conduct testing activities.

Privacy Risk: There is a risk that information collected in response to a declared public health emergency will be retained for longer than necessary.

Mitigation: This risk cannot currently be mitigated. Because many of the records collected under a declared public health emergency and discussed above have not been scheduled, they are retained indefinitely. DHS is currently working to develop a records schedule. Once a records schedule is completed and approved by NARA, DHS will be able to implement mechanisms within its online contact tracing reporting and workforce accountability tools to ensure proper disposal and destruction of such data.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

In the context of the programs and activities described in this PIA, DHS only collects PII necessary to support its efforts to prevent the spread of infectious disease in DHS facilities and among its workforce during declared public health emergencies. These activities are conducted in

²⁶ Components may have different applicable retention schedules based on their own authorities and deviations from what is outlined in this PIA. Those differences are outlined in Component-specific appendices, as necessary.



accordance with the purposes specified in the privacy notices referenced above and the other procedures outlined in this PIA.

No PII is shared outside of the Department except in accordance with circumstances specified in DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records. For example, as contact tracing is conducted on visitors to DHS facilities; and, although the DHS Contact Tracing Program was developed to not have contact tracers disclose PII, information related to contact with a confirmed case may be shared outside the Department. Further, in accordance with state and local health requirements, DHS may be required to share testing results with appropriate federal, state, or local governmental agencies to assist in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats.

Privacy Risk: There is a risk that more information will be shared external to DHS than is necessary.

Mitigation: This risk is mitigated. The DHS Privacy Office and Component privacy offices work with workforce health and safety offices and programs to ensure that information collection and sharing is done in accordance with this PIA and the DHS/ALL-047 SORN. All forms, screening tools, contact tracing and workforce accountability trackers, and testing processes undergo review by the appropriate oversight offices. Part of this review includes the completion of a Privacy Threshold Analysis (PTA) to ensure that any new effort aligns with DHS privacy policy and the FIPPs. The PTA includes analysis on why and what information is shared externally.

Additionally, online contact tracing reporting and workforce accountability tools do not have direct external connections and any disclosures can be automatically tracked through audit logs. DHS personnel also complete Privacy and IT Security and Awareness training annually.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Information collected for purposes of screening individuals at entrances to DHS facilities is always taken directly from the data subject and is immediately used to determine whether to grant or deny access. None of this information involves PII or is recorded.

PII collected by contact tracers is collected directly from the data subjects and immediately recorded on contact tracing forms or online contact tracing reporting tools. The only third-parties capable of submitting PII into online contact tracing reporting tools are supervisors and CORs submitting information about their direct reports and contact tracers submitting information during interviews. Contact tracing forms and online contact tracing reporting tools incorporate pre-



approved templates and frameworks to help ensure that collections are relevant and complete. PII for workforce accountability tools is input directly by the individual or their supervisor or COR. Individuals will have access to their own information and can correct it as necessary and appropriate. Much of the contact and work-related information collected via online contact tracing reporting and workforce accountability tools is automatically populated from systems like DHS's Access Lifecycle Management system²⁷ to further ensure accuracy. Moreover, many of the fields in these systems are drop-down fields rather than free-text options to further ensure accuracy.

PII collected to conduct laboratory testing or to dispense medication and treatment is also collected directly from the individual and immediately recorded. Again, pre-approved forms collecting the information help ensure that data is relevant and complete.

Privacy Risk: There is a risk that inaccurate data obtained during facilities screening or testing activities, due to the nature of declared public health emergencies, could inappropriately affect an individual.

Mitigation: This risk is mitigated. Given that declared public health emergencies are generally unprecedented or novel, the appropriate response may not be fully known at the outset. DHS works with its own medical professionals and those of other agencies to ensure DHS's response aligns with the recommended practices; for example, from the CDC. Due to the uncertainty of these emergencies, DHS may not have the most accurate way to conduct facilities screening or collect/test samples. For example, facilities screening tools may not be calibrated to accurately detect individuals who pose a potential risk until more details of the disease or illness come become available. Testing samples may result in false positives or false negatives, or testing procedures may have different accuracy rates depending on the novelty of an emerging disease or illness.

To mitigate these potential issues with data integrity, DHS offers redress opportunities for affected individuals. For example, individuals who do meet or exceed the screening thresholds may be allowed to re-screen depending on the nature of the disease or illness. Individuals that are denied entry are advised to contact their supervisor or COR to determine how they should proceed for the workday. Individuals may also be re-tested for the disease or illness if they receive a positive result. No testing is 100 percent infallible, especially in emergent situations such as declared public health emergencies. It is important for DHS to provide or allow for secondary measures should a positive result occur. Individuals cannot be reprimanded for testing positive for the disease or illness or for being denied entry to a DHS facility as a result of meeting or exceeding the screening thresholds established for facility access.

²⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE ACCESS LIFECYCLE MANAGEMENT (ALM), DHS/ALL/PIA-058 (2017), available at <https://www.dhs.gov/privacy-documents-department-wide-programs>.



7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Hardcopy contact tracing forms and privacy-sensitive forms associated with laboratory testing will only be made available to contact tracers, medical professionals, or others with a need-to-know; and they will always be kept in a locked drawer or other secure container when not in use. Furthermore, they will only be housed in Component workforce health and safety offices and stored separately from non-medical personnel records to ensure compliance with the ADA and the Rehabilitation Act, as appropriate. All testing samples follow Standard Operating Procedures (SOP) or Concept of Operations (CONOPs) developed to ensure adherence to testing protocols, whether for internal DHS testing or third-party testing.

Online contact tracing reporting and workforce accountability tools are architected to ensure that access to records containing PII is limited to those with a valid need-to-know. Specifically, confirmed cases and exposed contacts should only have access to their own records, supervisors and CORs should only have access to records of their direct reports, contact tracers should only have access to their assigned cases, supervisory contact tracers should only have access to records assigned to any of the contact tracers that report to them, and DHS management officials should only be able to access aggregate and anonymized data.

Privacy Risk: There is a risk that testing information or samples may be accessed or used by someone without a need-to-know.

Mitigation: This risk is mitigated. Any sensitive PII that is shared to a third-party or within DHS for testing must be password-protected or encrypted when transmitted via email, in accordance with the DHS Handbook for Protecting Sensitive Personally Identifiable Information.²⁸ Additionally, all DHS personnel complete Privacy and IT Security and Awareness training.

Testing protocols will stipulate which parties should be provided test results and how testing samples are physically handled. In some third-party testing situations, it may be the responsibility of the individual DHS employee to inform their supervisor if he or she tests positive. In other cases, DHS may be conducting the testing and processing the test results. Testing protocols ensure that results are only disclosed to those with a need-to-know. Further, contact tracing reporting and workforce accountability tools that may contain information on testing results use access controls to ensure that individuals only have access to cases, information, and permissions

²⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (2017), available at <https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information>.



that they should (e.g., supervisors can only access records/data on their direct reports rather than individuals from their entire Component).

Physical handling of testing protocols is overseen by medical professionals, or in a manner approved by those officials. These protocols are documented to maintain transparency for appropriate personnel, as well as individuals undergoing testing, and carried out to ensure efficient and accurate test results.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Designated DHS representatives who screen individuals attempting to enter DHS facilities are accountable for following guidance that DHS developed with input from the DHS Privacy Office (and other appropriate oversight offices). Since no records containing PII are generated as part of the screening process, no records management audits or logging capabilities are required. DHS enters into contracts with commercial vendors to provide the appropriate facilities screening tools. Although PII is not necessary for these tools to perform their function, they do collect statistical data (e.g., number of pass/fail results) and metadata (e.g., date/time, length of reading) for the vendor to ensure the tools are properly calibrated and performing as intended.

DHS has developed contact tracing training focused on contact tracers' responsibilities, use of appropriate tools, and managing case load and workflow. The training covers accountability issues and is meant to be completed by contact tracers across DHS. Additional training DHS recommends for contact tracers includes privacy, IT security, telephone customer service, and other publicly available contact tracing training provided by medical agencies.

Hardcopy contact tracing forms and records in online contact tracing reporting and workforce accountability tools are subject to annual records management audits. Audit logs are built into these tools and automatically track activities and changes made by users. These systems also provision initial access to users that are required to complete their job responsibilities and partition data/records available to an individual user based on their need-to-know.

Laboratory testing and medical treatment at DHS is conducted by medical professionals, or under their guidance, who must meet necessary training requirements to maintain their professional certifications. This training generally includes compliance with accountability controls mandated by the ADA, the Rehabilitation Act, OSHA, and the Health Insurance Portability and Accountability Act (HIPAA).



Conclusion

The DHS guidance on how to conduct health screenings at facility entrances, workforce accountability, contact tracing, and laboratory testing in the context of declared public health emergencies involving infectious disease is important and necessary to ensure the safety of the DHS workforce and visitors and continuity of government. All DHS guidance issued on these subjects is developed in collaboration with the DHS Privacy Office (and other appropriate oversight offices, such as the DHS Office of General Counsel) to ensure it reflects the FIPPs to the maximum extent practicable without undermining the central purpose, utility, or effectiveness of the activities. The mitigations described in this PIA reflect this balance between protecting individual privacy and protecting the health and safety of the workforce and the DHS mission. DHS will continue to work with officials throughout the Department and at other federal agencies to ensure actions it takes to contain the spread of infectious disease within its facilities adequately considers public health recommendations and its own operational realities.

Responsible Officials

Dr. Sangeeta Kaushik
Executive Director, Workforce Health and Safety
Office of the Chief Human Capital Officer
(202) 357-8478

Approval Signature

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

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



Appendix A: DHS COVID-19 Vaccination Initiative

Last updated January 8, 2021

The Secretary of Health and Human Services (HHS) declared a public health emergency on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. § 247d), in response to Coronavirus Disease 2019 (COVID-19). During a public health emergency, the U.S. Food and Drug Administration (FDA) can use its Emergency Use Authorization (EUA) authority to allow the use of unapproved medical products, or unapproved uses of approved medical products, to diagnose, treat, or prevent serious or life-threatening diseases when certain criteria are met, including when there are no adequate, approved, and available alternatives. EUA medical products to prevent serious or life-threatening diseases include vaccinations for COVID-19. There are several vaccine candidates that are or will be available pursuant to the FDA's EUA authority. Given the DHS mission of securing the homeland, it is imperative that certain DHS personnel be provided the vaccine, as appropriate, to ensure fulfillment of those mission responsibilities.

The DHS Office of the Chief Human Capital Officer (OCHCO) Workforce Health and Safety Division (WHS), in coordination with the DHS Chief Medical Officer, developed a program to ensure certain segments of the DHS workforce could be vaccinated as limited doses of COVID-19 vaccinations become available to other federal agencies. DHS has partnered with the U.S. Department of Veterans Affairs (VA), Veterans Health Administration (VHA) for administration of the vaccine. DHS and VHA entered into a Memorandum of Understanding (MOU), pursuant to the authority of the Economy Act (31 U.S.C. § 1535), to document and outline the requirements and responsibilities of this initiative.

Eligible DHS employees will be permitted to receive the vaccine that is administered by VHA on a strictly voluntary basis; and eligibility will be based on relevant priority groups established by the Centers for Disease Control and Prevention (CDC) Advisory Committee on Immunization Practices (ACIP).²⁹ DHS and its Components will identify their own employees who fall within the ACIP priority groups and inform them of their eligibility to receive the vaccine. Those who wish to participate will then initiate the DHS opt-in process and VHA registration processes, which are detailed further below.

In accordance with the CDC ACIP priority groups, Components will create a list of eligible employees (with their names and email addresses) and deliver it to OCHCO WHS. This list will be used later in the registration process to confirm eligibility. In order to inform individuals about this initiative and their individual eligibility, DHS and its Components will contact personnel by email or through verbal communication depending on the nature of their duty location. This communication will inform employees about the overall effort, that participation is strictly

²⁹ See CENTERS FOR DISEASE CONTROL AND PREVENTION, ADVISORY COMMITTEE ON IMMUNIZATION PRACTICES (ACIP), available at <https://www.cdc.gov/vaccines/acip/index.html>.



voluntary, and that no adverse action will be taken against employees who refuse it. The communication will also explain what PII and medical information will be obtained, how it will be used, who will receive it, and restrictions on disclosure. Eligible employees interested in receiving the vaccine will be directed to the DHS ServiceNow website, where they can opt-in to the program. When an employee agrees to receive the vaccine via the opt-in site, he or she will be asked to submit directly into the site: full name, duty location by zip code, work email, and a “best contact phone number” at which VHA can reach the individual. The employee will then be confirmed as eligible by associating their information to the names and work emails previously received in the eligibility list provided by Components.

DHS will send this information to VHA in order for VHA to (1) contact the DHS employee using his or her best contact phone number to register and enroll the individual for the vaccine and to schedule the appointment for the first dose³⁰ and to (2) verify that it is the correct DHS employee that has deemed to be eligible by the Department when he or she arrives for the vaccine. VHA registration requires the collection of additional data, per VHA policies and processes. This may include Social Security number (SSN), date of birth, sex/gender, home address, or other PII shared to VHA, either provided by DHS or the employee. All information needed for VHA registration purposes is not shared back with DHS.³¹

DHS has determined that a phased approach is the most effective method for vaccinating its personnel based on the limited quantities of the vaccine available and the differing priority groups (as explained below). During Phase 1A of this initiative, only full name, duty location by zip code, work email, and a “best contact phone number” were provided directly from DHS to VHA, with the remaining PII provided directly by the DHS employee when contacted by VHA. During Phase 1B, and due to the increased number of eligible participants in the priority groups and vaccine quantities, in addition to the information provided by DHS as part of Phase 1A, DHS will share SSN, date of birth, home address, and other PII directly to VHA at the same time to expedite registration and verification. For those that opt-in, DHS will provide to VHA via Secure File Transfer Protocol (SFTP) information received from the DHS employee in the DHS ServiceNow website, as well as information sourced from the Department’s Human Capital Enterprise Integration Environment (EIE),³² which includes the employee’s SSN, date of birth, sex/gender, and home address.

³⁰ The duty location by zip code will be used by VHA to determine which of their administering facilities should reach out to the employee and also to anticipate quantities of vaccines needed at each facility.

³¹ All data submitted to VHA, whether directly by the individual employee or by DHS, will be retained in accordance with U.S. DEPARTMENT OF VETERANS AFFAIRS, RECORDS CONTROL SCHEDULE 10-1, ITEM 6000.2: ELECTRONIC HEALTH RECORDS, available at <https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>.

³² EIE is a secure data repository and segregated information-sharing environment managed by OCHCO that houses personnel data on every employee in the Department. See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR WORKFORCE ANALYTICS AND EMPLOYEE RECORDS, DHS/ALL/PIA-075 (2020), available at <https://www.dhs.gov/privacy-documents-department-wide-programs>.



When the employee arrives for the first dose, VHA will provide the employee with an EUA patient fact sheet and will enroll the employee in its Veterans Information Systems Technology Architecture (VistA) system.³³ VHA will then administer the first dose of the vaccine. Once the first dose is administered, the employee will schedule an appointment for the second dose in 21-28 days, and the employee will receive a printed vaccination card as a record of proof of receiving the first dose. When the employee returns for the second dose, he or she will present the vaccination card from the first dose appointment, in order to confirm eligibility. Once the employee receives the second dose, VHA will update the vaccination card and VistA accordingly.

VHA will provide the PII collected by DHS and the PII it collected as part of the registration and enrollment process, as well as other data elements related to administering the vaccine, for each administered vaccine, to the CDC per CDC's Immunization Information Systems (IIS) guidance (including "required data elements" and "optional data elements," as necessary).³⁴ DHS will not receive any PII back from VHA, but VHA may provide DHS with de-identified statistical vaccination information not linked to an individual.

Privacy Risks

Privacy Risk: There is a risk that employees will not be provided sufficient notice about the program, such as its voluntary nature or how their information will be used.

Mitigation: This risk is mitigated. During the initial communication outreach to personnel, they are informed of what PII will be collected, how that information will be used, who will receive the information, and restrictions on disclosure. When opting-in to the program through the DHS ServiceNow website, employees are required to acknowledge a Privacy Act Statement that outlines purpose of the collection, the authorities to collect the information, routine uses, and the consequences of refusing to receive a vaccine (in this case, no adverse action whatsoever will be taken against employees who refuse it). Further, the DHS ServiceNow website will direct employees to this PIA and a Frequently Asked Questions (FAQ) page if further information is needed.

Privacy Risk: There is a risk that more information is being collected to administer the vaccine to DHS employees.

Mitigation: This risk is mitigated. OCHCO WHS worked with the DHS Privacy Office, and other oversight offices, such as the DHS Office of the General Counsel, to determine the necessary information required to carry out this initiative. DHS only provides VHA PII on

³³ VistA is a health information system deployed across all veteran care sites in the United States. VistA provides clinical, administrative, and financial functions for all of the 1700+ hospitals and clinics of the Veterans Health Administration.

³⁴ See CENTERS FOR DISEASE CONTROL AND PREVENTION, COVID-19 VACCINATION REPORTING SYSTEMS TECHNICAL STANDARDS & REPORTING DATA TO CDC, APPENDIX C, *available at* <https://www.cdc.gov/vaccines/covid-19/reporting/requirements/index.html>.



individuals who opt-in to the program, and collects from those individuals the minimal amount necessary to allow VHA to contact and subsequently register those individuals.

VHA only collects the information necessary to register and enroll individuals in Vista and in accordance with CDC IIS guidance. This information is not shared back to DHS in identifiable form.

Privacy Risk: There is a risk that SPII is not be securely shared between DHS and VHA.

Mitigation: This risk is mitigated. During Phase 1A of this initiative, DHS only shared basic contact information with VHA to allow for VHA to contact the DHS employee. All other information, to include SSN and date of birth, was collected by VHA for registration purposes directly from the individual after he or she opted in. For Phase 1B, DHS has developed a SFTP process to itself securely transfer this SPII to VHA. This will remove the requirement for DHS personnel to have to relay this information to VHA over the phone during the registration process and ensure data integrity as this information is sourced directly from EIE, DHS's consolidated authoritative source for human capital information across the Department. Only information on individuals who opt-in will be transferred via SFTP to VHA during Phase 1B.