Privacy Impact Assessment Update
for the

electronic Health Records (eHR) System

DHS/ICE/PIA-037(a)

April 26, 2018

Contact Point
Dr. Stewart D. Smith
Assistant Director
ICE Health Service Corps
U.S. Immigration and Customs Enforcement
(202) 732-3524

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The electronic Health Records system (eHR) is a U.S. Immigration and Customs Enforcement (ICE) case management system for maintaining records of medical treatment provided to individuals detained by ICE. ICE detainees receive medical, dental, and mental health evaluations and treatment necessary and appropriate for the individual's medical condition and length of stay. The Privacy Impact Assessment (PIA) for eHR was conducted in 2013.[1] This update describes ICE's development of an online Patient Medical Record Portal, whereby former detainees can access an electronic copy of their medical records.

Overview

ICE is responsible for identifying, apprehending, detaining, and removing aliens who are eligible for removal under the Immigration and Nationality Act (INA). The ICE Health Services Corps (IHSC) provides health evaluations, treatment, and services to ICE detainees held in detention facilities across the country. IHSC personnel use the eHR to document health care provided to these detainees. The eHR is an integrated healthcare information system comprised of several components, which record and manage detainee healthcare evaluation and treatment information as well as process claims for payments to external healthcare providers.[2]

IHSC has now partnered with a vendor to develop a website called the Patient Medical Record Portal (the "Portal"). The Portal, part of the eClinicalWorks (eCW) component of the eHR system, permits individuals discharged from IHSC-staffed detention facilities (hereafter "former detainees") to access a read-only PDF copy of their medical record online. The Portal is available to all former detainees who have been discharged from an IHSC-staffed facility, whether they have been released from ICE custody or ordered removed from the United States. While the Portal is a publicly-available website, access credentials are required in order to view any records within the Portal. Neither IHSC personnel nor the vendor can access patient medical records in the Portal. The Portal also employs strong security safeguards to help protect detainee

[1] DHS/ICE/PIA–037 Electronic Health Records System, *available at* www.dhs.gov/privacy.
[2] The components of eHR are as follows:

- eClinicalWorks (eCW): Is the core component of the electronic health record and is used to document healthcare that is provided to detainees at IHSC-staffed facilities.
- Open Dental: Captures dental examination and treatment information. The component includes a graphical tooth chart and drawing capabilities.
- Dental X-Ray: Captures information related to dental X-Rays.
- Correctional Pharmacy Software (CIPS): Allows pharmacists to monitor and track the inventory and dispensing of medications.
- Diagnostic services: Interfaces with external healthcare providers who provide diagnostic services such as laboratory and diagnostic imaging studies.
- Referral Component: Allows for the authorization of payment for specialty, emergency, in-patient, and other healthcare services provided to detainees by external healthcare providers and facilities.
- MedPAR 2.0: A web-based application that allows non IHSC personnel to request authorization for external healthcare services. Information is transmitted from MedPAR into the referral component.

information, as detailed below in the "Auditing and Accountability" section. Before the Portal was developed, former ICE detainees could only access their medical records in one of two ways:

- A written request to the detention facility; or
- A request to the ICE Freedom of Information Act (FOIA) Office.

While these options will still be available once the Portal is fully deployed, the Portal will ease the burden on former detainees by allowing them to access a copy of their medical records online.

Uploading Records to the Portal

Designated IHSC staff must "web enable" a detainee's medical record in order to populate the Portal. Web enabling is the process of making the record internet-compatible so that former detainees can retrieve the file when they log into the Portal. All records are required to be enabled, and this process occurs when ICE first books the detainee into a detention facility.

When IHSC staff receive a notification from ICE's Office of Enforcement and Removal Operations (ERO) that a detainee is pending discharge from an ICE facility, they click a button in the detainee's eHR record to publish a PDF copy of the detainee's medical record to the Portal. The medical record will be available via the Portal within 3 to 7 days after a detainee's discharge.

Accessing the Portal

Upon discharge from an IHSC-staffed facility, ICE personnel provide former detainees with a credentials letter (available in both English and Spanish) that includes the Portal's web address and the former detainee's username and temporary password. The first time that former detainees access the Portal, they must enter both the username and temporary password on the credentials letter, and confirm their identity by providing their date of birth. They can then create a permanent password for each subsequent log-in attempt. Former detainees must also set up a security question before accessing the Portal. Finally, former detainees must consent to the following:

- Rules of Behavior for using the Portal; and
- The IHSC Privacy and Security Policy that details how ICE will use the detainee's personally identifiable information (PII).

A copy of the former detainee's consent is saved in his or her eHR record.

Former detainees accessing the Portal will see the PDF files containing their medical records. They can then view, print, and save their medical records on their personal devices (e.g., laptop, tablet), as well as share their medical records with third parties (e.g., medical providers,

family, legal representatives), as necessary. Limiting a former detainee's ability to share his or her medical information could have a negative impact on the detainee's health or well-being.

The medical records are available on the Portal within 3-7 days after discharge, and up to one year after discharge. For example, if a detainee was discharged from ICE custody on June 1, 2017, his or her medical record would be made available from June 4th to 8th, and would be accessible in the Portal until June 1, 2018. Once published to the Portal, the contents of the record are converted to a PDF file and stored in a File Transfer Protocol (FTP) site located on an ICE network server. Records are retrieved from the FTP server and transmitted to the Portal as former detainees access their medical records. After one year, the records are deleted from the Portal. The records are available in the eHR system pursuant to the applicable records retention schedule and remain accessible via written or FOIA request. More information about records retention in the eHR system is discussed below.

Portal User Groups

There are four groups of users who can access the Portal:

- Former detainees can view, print, and save a PDF copy of their electronic medical record. This access is read-only. Former detainees do not have access to the live eHR system.
- Designated IHSC staff and contract staff can web enable and publish records into the Portal from eHR.
- Designated IHSC staff with administrator permissions can view statistical reports about Portal usage.
- System administrators help set up the Portal and configure the settings and customization of notices, such as the site privacy policy. Administrators also monitor and report on Portal usage. These reports include statistics on log-in information (e.g., number of former detainees who have logged in, number of unsuccessful log-in attempts), trends in use, and the number of web-enabled detainee records.

Reason for the PIA Update

With the publication of this PIA Update, ICE will now offer former detainees access to a copy of their medical records via an online Patient Medical Record Portal (the "Portal"). The Portal, part of the eClinicalWorks (eCW) component of the eHR, provides former detainees discharged from ICE detention (including those who have been removed from the United States) online access to a read-only PDF copy of their ICE medical record. In addition to records access via the Portal, former detainees may also request their medical records by either writing to the detention facility or making a request under the Freedom of Information Act (FOIA). The Portal may ease the burden on former detainees seeking a copy of their medical records. This Update

also describes the records retention schedule for eHR records, which was approved by the National Archives and Records Administration (NARA) after the 2013 PIA was published.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

5 U.S.C. § 301; 44 U.S.C. § 3101; 8 U.S.C. §§ 1103, 1222, and 1231; and 42 U.S.C. § 249 authorize the collection of information in the IHSC Patient Portal.

Records in eHR are covered by the Alien Health Records System of Records Notice (SORN).[3]

A system security plan for the eHR system has been completed, and the Authority to Operate (ATO) was authorized in September 2016.

Records in the IHSC Portal are covered by the "Electronic Health Records (eHR) System" retention schedule. The applicable records control number is DAA-0567-2015-0002.[4]

Characterization of the Information

With this update, ICE will be collecting and storing the former detainee's log-in credentials (i.e., username, password, and security question and answer). The Portal also automatically records both successful and unsuccessful attempts to log in, and notes when a former detainee's account has been locked due to three unsuccessful log-in attempts.

The information provided through the Portal is the same information that is already collected and stored in the eHR. With this update, ICE is providing former detainees another option to access a copy of their medical record. The Portal does not use any information from commercial sources or publicly available data.

This update does not change the procedures that ICE has in place to ensure that the information in eHR is accurate. Specifics regarding how ICE maintains data accuracy in this system can be found in the eHR PIA.

ICE has not identified any additional risks related to characterization of the information.

Uses of the Information

Designated IHSC personnel select an option within the eHR to generate a PDF copy of a former detainee's medical record in the Portal. The Portal provides another option for former detainees to access a copy of their medical records. The Portal allows former detainees to view,

[3] DHS/ICE-013 Alien Health Records System, 83 FR 12015 (March 19, 2018).
[4] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2015-0002_sf115.pdf.

print, and save a PDF copy of their medical records for their own personal use. As explained previously, the Portal has four user groups (former detainees, designated IHSC staff and contract staff who can web enable and publish records to the Portal, IHSC staff with administrator privileges, and system administrators). Former detainees are given read-only access to their medical records. They are not able to alter or amend the records in any way.

Privacy Risk: There is a risk that because the Portal gateway is public, it could be accessed by unauthorized individuals.

Mitigation: User roles and access controls are incorporated so that only individuals with a need to know can access specific portions of the Portal. At discharge from ICE detention, former detainees are given a credentials letter with a username and temporary password for accessing the Portal. Former detainees are required to enter these log-in credentials, create a permanent password establish a security question and answer, and confirm their date of birth to access their medical records in the Portal. Former detainees will be locked out of the Portal following three unsuccessful log-in attempts. They are advised both on the credentials letter and on the welcome screen of the Portal that they will need to request their medical records in writing if they are locked out of the Portal.[5] Furthermore, system administrators can unsubscribe users as necessary and appropriate, including when the system is being used in an unauthorized manner. Employees or contractors found to be inappropriately accessing or using the eHR face disciplinary measures up to and including termination.

Former detainees must agree to the system's Rules of Behavior, as well as IHSC's Privacy and Security Policy before accessing the Portal. The IHSC Privacy and Security Policy outlines the authority for maintenance of the system, the purpose of collection, how ICE may disclose the detainee's PII, and whether providing information to ICE is mandatory or voluntary. Finally, the copy of the medical record available through the Portal is a read-only PDF that cannot be altered. This helps ensure the data quality and integrity of the information contained within the system.

Notice

Former detainees are handed a credentials letter at the time of their release from ICE detention. The letter contains background information about the Portal, the former detainee's log-in credentials for the Portal, and the internet address to the Portal. Both the Portal and the credentials letter are available in English and in Spanish.[6] When former detainees log in for the first time, they are instructed to create a permanent password for each subsequent log-in attempt.

[5] IHSC administrators will periodically unlock accounts (no sooner than 4 hours after the account has been locked) so that former detainees can access their medical records. However, former detainees still must correctly input their log-in credentials to view their records.
[6] The Patient Medical Record Portal will ultimately be available in other frequently encountered languages.

ICE also provides notice within the Portal itself. When former detainees log in, they must agree to the IHSC Privacy and Security Policy that details how ICE uses the detainee's PII as well as the security safeguards that are in place. The Privacy and Security Policy contains a detailed Privacy Notice that lists the authority for maintenance of the system, the purpose of collection, how ICE may disclose the detainee's PII, and whether providing information to ICE is mandatory or voluntary. The Privacy and Security Policy is also available in both English and Spanish, and will be publicly available on ICE's website. Finally, ICE provides the public (including former detainees) with notice of the Portal by the publication of this PIA update, and the Alien Health Records SORN.[7]

ICE has not identified any additional risks related to notice.

Data Retention by the project

Medical information accessible via the Portal is retained for one year after the former detainee has been released from ICE custody. After one year, ICE deletes former detainees' medical records in the Portal. Former detainees who wish to obtain a copy of their medical records after one year must either write to the detention facility or make a written request to the ICE FOIA Office. Adult medical records are maintained in eHR for 10 years and then destroyed. Medical records pertaining to minors (those under 18 years old) are maintained in eHR until the minor reaches his or her 27th birthday. The records are then destroyed.

Privacy Risk: There is a risk that information in the Portal is retained for longer than necessary to accomplish the purpose for which it was originally collected.

Mitigation: The retention period approved by NARA is narrowly tailored to fulfill the purposes of the Portal. Making the records available in the Portal for one year gives former detainees sufficient time to access an electronic copy of their medical records. If former detainees need a copy of their medical record after one year and did not save the PDF version on their personal devices, then they can still get a copy by either writing to the detention facility or filing a FOIA request. Further, because the amount of storage space on the Portal is limited, IHSC will delete records from the Portal after one year.

Information Sharing

With this update, ICE will make information in the eHR system available to former detainees who have been released in the past year. While ICE has always made this information available to former detainees upon written request, ICE is now providing former detainees with access to their medical records online. ICE will not use the Portal to share this information with anyone besides former detainees.

Privacy Risk: There is a risk that data will be accessed by unauthorized individuals.

[7] DHS/ICE-013 Alien Health Records System, 83 FR 12015 (March 19, 2018).

Mitigation: ICE limits dissemination of Portal log-in credentials to former detainees who have been discharged from ICE detention facilities. Former detainees must log in using the appropriate username and password and confirm their identity by entering their date of birth in order to access the Portal. This significantly reduces the risk that an unauthorized third party can access the contents of the Portal. Further, ICE user access is limited to IHSC personnel who have a legitimate need to know.

There is also a benefit in providing former detainees online access to their medical records so they may share that information, as necessary, with third parties, such as other medical providers, family, friends, or legal representatives. With the deployment of the Portal, former detainees will be able to access medical information more quickly and efficiently.

Redress

The right to request access to and amendment of records under the Privacy Act of 1974 (5 U.S.C. § 552a) is limited to United States citizens and lawful permanent residents. Executive Order No. 13,768 *Enhancing Public Safety in the Interior of the United States* (January 25, 2017) states: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[8] This Executive Order precludes DHS from extending such rights by policy. Additionally, the Judicial Redress Act of 2015 (5 U.S.C. §552a note), which amended the Privacy Act, provides citizens of certain countries with access, amendment, and other redress rights under the Privacy Act in certain limited situations.[9]

As a result of Executive Order 13,768, DHS's "Mixed Systems Policy"[10] was rescinded by the DHS Privacy Office in its Privacy Policy Guidance Memorandum (April 25, 2017).[11] However, DHS will consider individual requests to determine whether or not an individual may

[8] The full text of Executive Order 13,768 can be found here: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.
[9] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website https://www.justice.gov/opcl/judicial-redress-act-2015.
[10] The DHS' "Mixed Systems Policy" extended most Privacy Act protections to visitors and aliens whose information was collected, used, maintained, or disseminated in connection with a mixed system of records (i.e., contains PII on U.S. citizens and lawful permanent residents, as well as non-U.S. citizens and non-legal permanent residents). Memorandum Number 2007-1, DHS Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.
[11] DHS Memorandum 2017-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 25, 2017) (DHS Privacy Policy), available at https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01. As the DHS Privacy Policy notes, Executive Order 13768, does not affect statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. §1367. These laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and aliens, regardless of a person's immigration status.

access or amend records contained in this system. Individuals seeking access to and notification of any records contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE Freedom of Information Act (FOIA) Officer. Individuals who wish to contest the accuracy of records in the system may submit these requests to the ICE Privacy Division.

In addition, the DHS Privacy Policy Guidance Memorandum makes clear that DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain accurate records serves to undermine efficient decision making by DHS personnel, and can create the risk of errors made by DHS and its personnel. Also, PIAs are published, in part, to ensure that projects, programs, and systems maintain accurate data. Finally, the Portal enhances redress for former detainees, as it is now easier for former detainees to access their medical records and review them for any inaccuracies.

Auditing and Accountability

Data integrity is safeguarded by providing former detainees read-only copies of their medical records through the Portal. The information contained in the Portal or elsewhere in eHR cannot be changed by former detainees because they do not have access to the live eHR system. Furthermore, former detainees who access the Portal must consent to the Rules of Behavior and the IHSC Privacy and Security Policy, which is also available on ICE's public website.

The IHSC Privacy and Security Policy also details what information ICE will collect and store, the security safeguards in place for the Portal, and how ICE can share information in the eHR both internally within DHS and with external third parties. Any ICE employees or contractors found to have used the Portal in an unauthorized manner may be disciplined in accordance with ICE policy. In addition, the Portal employs strong security safeguards to protect former detainees' PII, including: requiring credentials to view medical records, encrypting data transmission between the Web Server and the client browser, and incorporating strong password requirements. Because the Portal requires a user account to view patient medical records, neither IHSC personnel nor the vendor can view patient PII in the Portal.

Employees and contractors (including facility staff) with access to the Portal receive appropriate training prior to using the system. First, all ICE employees and contractors are required to participate in annual privacy and security training. Second, IHSC staff also receive Portal-specific training prior to using the Portal.

The eHR system user roles determine what information the user sees and what the user can do in the system. As discussed previously, there are four categories of users.

- Former detainees will have the ability to access a copy of their medical records through the Portal.

- Designated IHSC staff and contract staff can web enable and publish records into the Portal from eHR.
- Designated IHSC staff with administrator permissions can view statistical reports about Portal usage.
- System administrators configure the Portal, determine which individuals can access the system, and report statistics on Portal usage.

Responsible Official

Lauren Berkebile
Acting Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security