US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/14/2024

OPDIV:

NIH

Name:

CC 3M 360 Encompass

PIA Unique Identifier:

P-6093912-905025

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The NIH Clinical Center's (CC) use of 3M 360 Encompass is to abstract clinical diagnoses and procedures, provide medical record coding and essential clinical documentation to the NIH Clinical Research Information System (CRIS).

3M 360 Encompass stores clinical diagnoses and procedures for NIH CC inpatient visits, initial outpatient encounters, resource intensive day hospital and procedure area visits, and procedures performed in Interventional Radiology. Protocol, anesthesia, and readmission status associated with that visit are also abstracted.

The 3M 360 Encompass system, which includes Coding and (&) Reimbursement System (CRS) application, is utilized to abstract clinical diagnoses and procedures and assign medical codes.

(3M was originally the Minnesota Mining and Manufacturing Company.)

Describe the type of information the system will collect, maintain (store), or share.

3M 360 Encompass stores the following patient information, retrieved from the Clinical Research Information System:
Name, Mother Maiden Name, E-Mail Address, Phone Numbers, Medical Notes, Date of Birth, Mailing Address, Medical Records Number, Legal Documents and CRIS Order identification (ID). In addition, medical notes (clinical diagnoses and procedures for inpatient visits, initial outpatient encounters, resource intensive day hospital and procedure area visits, and procedures performed in Interventional Radiology, protocol, anesthesia, and readmission status associated with that visit) are also abstracted.

Clinician information collected includes name, designation (Doctor of Medicine (MD), Doctor of Osteopathic Medicine (DO), Doctor of Optometry (OD), etc.), work phone and work address.

3M CRS is utilized to perform International Classification of Diseases (ICD-10) and Current Procedural Terminology (CPT) coding and passes all codes to the ClinTrac application (a module included in the 3M software).

Medical record documentation is shared with First Class Solutions, Incorporated (Inc.) a subcontractor of Medical Record Corporation of Maryland (MRCM) to support ICD-10 coding services. They are direct contractors to the CC.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services. The purpose of the IAM is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM collects unique user credentials and stores them in an encrypted format. The IAM is an essential service which facilitates and governs network access to various resources.

NIH IAM Services, ClinTrac and CRIS maintain their own unique privacy impact assessment (PIA), with all legal authorities documented.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NIH CC's use of 3M 360 Encompass is to abstract clinical diagnoses and procedures, provide medical record coding and essential clinical documentation to the NIH CRIS.

3M 360 Encompass stores the following patient information, retrieved from the CRIS: Name, Mother Maiden Name, E-Mail Address, Phone Numbers, Medical Notes, Date of Birth, Mailing Address, Medical Records Number, Legal Documents and CRIS Order ID. In addition, medical notes (clinical diagnoses and procedures for inpatient visits, initial outpatient encounters, resource intensive day hospital and procedure area visits, and procedures performed in Interventional Radiology, protocol, anesthesia, and readmission status associated with that visit) are also abstracted.

Clinician information collected includes name, designation (MD, DO, OD, etc.), work phone and work address.

3M CRS is utilized to perform ICD-10 and CPT coding and passes all codes to the ClinTrac application (a module included in the 3M software).

Medical record documentation is shared with First Class Solutions, Inc., a subcontractor of MRCM to support ICD-10 coding services. They are direct contractors to the CC.

Those requiring access to this system log in using the NIH IAM Services. The purpose of the IAM is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software.

NIH IAM Services, ClinTrac and CRIS maintain their own unique PIA, with all legal authorities documented.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth
Name
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Legal Documents
CRIS Order ID
Physician designation

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Patient identification and medical documenting.

Describe the secondary uses for which the PII will be used.

The system can be used to compile a list of cases performed by NIH surgeons in the CC Operating Room.

Identify legal authorities governing information use and disclosure specific to the system and program.

The legal authority to operate and maintain this Privacy Act records system is 42 U.S.C. §§ 241, 248, 282 and 284

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0099, Clinical Research: Patient Medical Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the DOC

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

A MOU exists with MRCM for filing, scanning, coding and transcription service performed using MRCM software by direct contractors located at NIH. First Class Solutions is a subcontractor of MRCM and will be reflected in an updated MOU. First Class Solutions employees are direct contractors (badged) to NIH.

Describe the procedures for accounting for disclosures.

Audit logs are used to track and disclose what information is shared and tracked outside of NIH.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Every patient must voluntarily execute a protocol consent and authorization prior to entry onto an intramural research protocol and treatment at the CC. In addition, each patient is provided a formal notification of Information Practices at the Clinical Center and must certify that they have been so advised.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

General admission and protocol consent forms are signed by each patient. Additionally, an information practices notification form is reviewed and acknowledged in writing by each patient at the time of initial admission to the CC.

Enrollment in a clinical research trial is voluntary and the collection of personally identifiable information (PII) and medical notes is necessary to conduct research and provide clinical care. Therefore, a patient may not opt out of the collection or use of their PII while participating in research at the CC.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

All patients are notified of information practices upon admission. Each patient would be advised at the time of the next admission about major system changes and the CC Information Practices Notice would be revised and provided to each patient again.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The CC Department of Clinical Research Informatics (DCRI) Privacy Office will review the complaint and coordinate with the NIH Office of the Senior Official for Privacy (OSOP) to respond to the concern. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC DCRI Privacy Office.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access to PII is assigned to personnel based upon current job responsibilities. A NIH IAM account login is required to gain access to the stored data.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Dual factor authentication with NIH Personal Identity Verification (PIV) card and NIH IAM Account will occur at time of login to the NIH Network. System owners are responsible for creating the proper security groups within their systems with the applicable permissions for group members to enforce least privilege.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Health Information Management Department (HIMD) staff and direct contractors receive 3M 360 Encompass system training on the job by HIMD section leads.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item 03-001: Clinical Care Services Records
These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule.
Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff. DAA-0443-2019-0001-0001

Item 03-005: Patient Medical Records.
These records document admissions and medical treatment for a patient accepted in a research project.
Disposition: Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference. DAA-0443-2012-0007-0010

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.