US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/11/2025

OPDIV:

NIH

Name:

3M Automated Medical Record Processing

PIA Unique Identifier:

P-2051788-466477

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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?

Existing

Does the system have Security Authorization (SA)?

No

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

The 3M Health Information Systems (3MHIS) is a comprehensive suite of health information management applications utilized to monitor Clinical Research Information System (CRIS) medical record deficiencies, scan and view hard copy medical record documentation, abstract clinical diagnoses and procedures, monitor disclosures, and facilitate the transcription, signature, and storage of all dictated medical reports.

Patient and clinician demographic information is collected, along with clinical documentation identifiers and location information. The staff information is voluntarily provided at the time of dictation or authorship. The information is collected in the course of providing medical and clinical

research services to registered Clinical Center (CC) patients.

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

3MHIS is comprehensive suite of health information management applications that maintains patient demographic information (age, sex marital status), along with clinical documentation (medical notes, physician orders, signatures), patient identifiers (name, medical record number (MRN), phone number, email address, mailing address, date of birth (DOB), mother's maiden name) and location information (inpatient or outpatient location) and legal documents (guardianship and legal custody documents). 3MHIS also maintains staff information, specifically, name, professional designation, Institute, Center, Office (ICO) affiliation. Staff information is provided at the time of dictation or authorship. Patient information is collected during medical and clinical research services.

The 3MHIS suite includes:
ChartID (Identification) is 3M's master patient index and stores patient identifier, demographics, physician orders and medical notes.

ChartFact monitors medical record deficiencies for dictation, completion, and signature of required inpatient and outpatient medical record documentation.

ChartLocator tracks the physical location of the hard copy medical record.

ChartReserve stores appointment requests for clinics, units, and procedure areas that require a hard copy medical record.

ProviderID is the repository for current and inactive credentialed medical staff and maintains ancillary staff and medical student demographics for those individuals that require access to the dictation system and Electronic Signature Authentication (ESA).

ChartScript is the repository for transcribed dictations.
Transcription Client is used to transcribe and/or edit back-end speech recognized dictated medical reports.

ESA/ChartScriptMD stores electronic signatures. It serves as the signing application for dictated medical reports; allows dictating and countersigning clinicians access to edit and sign dictations. Authorized users can also type their own reports.

ChartScan used by staff to scan hard copy medical record documentation; allows for full scanning and quality checking.

ChartView/ViewLinc - ChartView is for viewing scanned/archived medical documentation by patient. ViewLinc is accessed within CRIS and displays only the document/patient information that user is currently viewing in CRIS.

ClinTrac/3M Coding & Reimbursement - ClinTrac stores clinical diagnoses and procedures for inpatient visits, initial outpatient encounters, resource intensive day hospital and procedure area visits, and procedures performed in Interventional Radiology. Other data such as protocol, anesthesia, and readmission status associated with that visit are also abstracted. 3M Coding & Reimbursement is utilized to perform International Classification of Diseases (ICD-10) and Current Procedural Terminology (CPT) coding and passes all codes to the ClinTrac application.

ChartLinc/ViewLinc - ChartLinc processes all inbound Admission Discharge and Transfer (ADT) messages and outbound messages. ViewLinc displays all scanned documents that are sent to

CRIS.

ChartRelease/DisclosureTrac is used to monitor and process release of information requests for all patients, tracking of patient record amendment requests and breaches.

Administrator (Admin) Consoles is used for monitoring user access, document indexing, and in-progress transcription.

Users log in to this system using the NIH Identity, Credential, and Access Management (ICAM) Services which maintains its own unique privacy impact assessment (PIA), including all legal authorities documented. The ICAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format.

CRIS maintains its own unique privacy impact assessment, 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.

3MHIS is a comprehensive suite of health information management applications utilized to monitor medical record deficiencies, scan and view hard copy medical record documentation, abstract clinical diagnoses and procedures, monitor disclosures, and facilitate the transcription, signature, and storage of all dictated medical reports.
Patient and clinician demographic information is collected, along with clinical documentation identifiers and location information. The staff information is voluntarily provided at the time of dictation or authorship. The patient information is collected in the course of providing medical and clinical research services to registered CC.

3MHIS maintains patient and clinician demographic information, along with clinical documentation identifiers and location information. Staff information is provided at the time of dictation or authorship. Patient information is collected during medical and clinical research services. 3MHIS includes the following:
ChartID
ChartFact
ChartLocator
ChartReserve
ProviderID
ChartScript
Transcription Client
ESA/ChartScriptMD
ChartScan
ChartView/ViewLinc
ClinTrac/3M Coding & Reimbursement
ChartLinc/ViewLinc
ChartRelease/DisclosureTrac
Admin Consoles

NIH ICAM and CRIS maintain their own unique PIAs, 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
Demographics, sex
guardianship and legal custody documents

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

Employees
Public Citizens
Patients
Patient's Private Physician

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Information is collected to identify and route clinical documentation electronically for user review and confirmation.

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 Clinical Center 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, HHS/NIH/CC

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Hardcopy
Email
Online
Government Sources
Within OpDiv
Other HHS OpDiv
State/Local/Tribal
Foreign
Other Federal Entities
Other
Non-Governmental Sources
Public
Private Sector
Commercial Data Broker
Other

Identify the OMB information collection approval number and expiration date

N/A. 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 Memorandum of Understanding (MOU) authorizes sharing dictated medical reports with 3M for operation of the backend speech recognition transcription services hosted in Austin, Texas.

A MOU exists with MRCM for filing, scanning, coding and transcription service performed using MRCM software by contractors located at NIH. First Class Solutions is a subcontractor of MRCM and will be reflected in the updated MOU.

Describe the procedures for accounting for disclosures.

If a request for an accounting is received, there are audit logs to allow the system owner to provide information about dictation reports disclosed to 3M and MRCM for authorized business functions. In addition, the system owner would review the disclosures tracked in the ChartRelease/DisclosureTrac.

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

The 3M system performs medical record processing, providing essential clinical documentation to CRIS. CRIS is an approved Privacy Act System and maintains its own PIA, including all legal authorities documented. Individuals are notified that their personal information will be collected at the time of admission to the CC and collected in CRIS. 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.

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 Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

Access to PII is assigned to personnel based upon current job responsibilities.

A NIH IAM Systems account login is required to gain access to the stored PII data.

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 and privacy awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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

Health Information Management Department (HIMD) staff and direct contractors receive 3MHIS application 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 03-005: Patient Medical Records
These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study.

Disposition: TEMPORARY. 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 information technology (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.