US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/30/2025

OPDIV:

NIH

Name:

CC Hyland OnBase-Workflow Management

PIA Unique Identifier:

P-3196284-593797

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

Hyland OnBase is a single health information management enterprise information platform that includes the following functions:

Clinician Signoff of transcribed reports
Historical scanned/imaged document repository.
Clinician Deficiency Management
Clinician repository
Scanning of paper documents
Patient medical information releases

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

Hyland OnBase collects, maintains and/or shares the following personally identifiable information (PII):

Name, email, phone number and address of the Patient and Patient's Private Physician(s)

Medical notes, Date of Birth (DoB), Medical Records Number (MRN), Guardianship and legal documents, sex, marital status, Mother's maiden name.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of IAM Services 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 Services collects unique user credentials and stores them in an encrypted format. The IAM Service is an essential service which facilitates and governs network access to various resources.

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

Hyland OnBase is a single health information management enterprise information platform that include the following functions:
Clinician Signoff of transcribed reports (Medical personnel approve the accuracy of transcribed reports.)
Historical scanned/imaged document repository.
Clinician Deficiency Management. (Monitoring deficiencies in medical records for dictation, completion, and signature of required inpatient and outpatient medical record documentation.)
Clinician repository. (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).)
Scanning of paper documents
Release of patient medical information (specifically monitoring and processing release of information requests, tracking of patient record amendment requests and breaches.

Hyland OnBase collects, maintains and/or shares the following PII:
Name, email, phone number and address of the Patient and Patient's Private Physician(s)
Medical notes, DoB, MRN, Guardianship and legal documents, sex, marital status, Mother's maiden name.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, 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
sex, marital status
Guardianship and legal documents

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

Employees
Public Citizens
Patients
Patient's Private Physician(s)

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
Non-Governmental 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 Memorandum of Understanding (MOU) authorizes sharing dictated medical reports with 3M for operation of the backend speech recognition transcription services hosted in Austin,

Texas. An MOU exists with MRCM for filing, scanning, and transcription service performed using MRCM software by contractors located at NIH.

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.

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 maintains its own Privacy Impact Assessment (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 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.

Access to PII is assigned based upon job roles/responsibilities. A NIH IAM Services account login is required to gain access to the stored PII data. The access rights of the logged-on user's NIH IAM Services account determines file system permissions and whether PII may be accessed.

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 Services will occur at time of login to the NIH Network and 3M System. 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 and privacy awareness training. 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).

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

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 Intramural Records Retention Schedule.

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

Item 07-204 - System access records. Systems requiring special accountability for access.
These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. (DAA-GRS-2013-0006-0004)

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.