US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/19/2024

OPDIV:

IHS

Name:

Electronic Dental Record

PIA Unique Identifier:

P-2496837-698776

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)?

Yes

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.

None

Describe the purpose of the system.

Dentrix Enterprise is an Electronic Dental Record (EDR) Commercial off the shelf (COTS) dental clinic application that has continuous upgrading and program development to meet the patient treatment documentation and patient management needs of the IHS Federal, Tribal and Urban (I/T/U) clinics. The EDR program includes a patient electronic health [dental] record system and incorporates a digital image management system, scheduling module, a billing module and Accounts Receivable management tool. The patient record can be accessed at any of the clinics that are within the local service unit Information Technology (IT) infrastructure network system which allows multiple providers to access the patient’s full record (within that local service unit network system). Additionally, the EDR program and data are connected to a local data back-up system to ensure patient treatment information will not be lost.

Functions performed by this system include:

1) Administrative; to include digital scheduling of patients, billing, and the ability to track patient treatment needs for recall appointments.

2) Clinical; Paperless charting, Treatment planning, and clinical note recording.

3) Financial Tools; Accounting of treatment and insurance billing, Revenue generation and analysis tools.

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

The system will collect and store patients':
A. Health and dental records containing: Examination, diagnostic and treatment data; proof of IHS eligibility; social data such as name, sex, address; date of birth; medical record number; Social Security Number (SSN); employment status; driver's license number; mother's maiden name; contact information such as email and phone number; tribe; case records for special programs.

B. Registers of individuals requiring follow-up dental treatment.

C. Logs of individuals provided health care by staffs of specific hospital components such as: x-ray and laboratory.

D. Operation and/or disease indices for particular hospitals which list each relevant patient by the operation or disease.

E. Third-party reimbursement records containing name, address, date of birth, date of admission and Medicare or Medicaid claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to process and validate third-party reimbursement claims.

Personnel must have appropriate access rights to access into the EDR system and additional role-base rights granted locally to access individual patient records. Information Technology (I.T.) support staff may also need to access the EDR system and view patient information to provide initial setup of the system and follow-up maintenance and trouble-shooting to ensure proper function of the system. At times, the system may fail and need to be debugged or upgraded to function properly. This may necessitate giving temporary access to outside personnel who work for the software manufacturer. Temporary access (credentials) would be used for these outside personnel with oversight from the local I.T. department

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

The EDR is installed as an individual EDR system (instance) at each participating [service unit] location. The installation at each location consists of either a virtual or physical server connected to a local network infrastructure system and workstations at each site which may also connect to an IHS-wide network system for data aggregation. (Individual patient record and non-data treatment information is not shared on the IHS-wide network.) The EDR data is stored on a Structured Query Language (SQL) Database Management System (DBMS) that resides on the server and the EDR application either resides on a workstation or on a Terminal/Application server. EDR users connect using the EDR thin client or, in the case where the EDR application is installed and runs on a local workstation, fat client. Users access the application directly on their workstations and the workstation communicates with the EDR Database server over a network connection, either Local

Area Network (LAN) or Wide Area Network (WAN).

In summation, each of the I/T/U service units have a closed local area network and link to the database and server for the EDR. The servers are kept in a physically secured server room of the service unit or in another location managed by the IHS Area office. In scenarios where the service unit has multiple satellite clinics, the satellite clinics may be either set up as stand-alone clinics or may have continuous direct connection to the main EDR server.

The EDR processes patient demographic and dental record data. (The system shall collect and store permanent information to include patient identifiers such as name, sex, Date of birth, Medical record number, and medical and dental health information. PII from the system to include the above as well as detailed treatment may be shared with dental insurance companies in the process of billing. This information needs to be stored in the system to identify the patient.

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

Yes

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

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Employment Status
x User names, passwords
x sex

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

Employees
Public Citizens
Patients
PII from providers is collected by the system and used for billing and recording of who the treating provider was. Other users, such as billing clerks, medical records, Dental Medical Support Assistants, and dental department staff will have to submit credentials when accessing the system.

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The purpose of EDR is to automate dental records, access the patient chart (includes medical/dental history & treatments), online scheduling, and insurance billing. To create user accounts.

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

Secondary uses are to carry out quality assessment, medical audits, utilization review or to provide accreditation or certification of health care facilities or programs; to conduct analytical and evaluation studies sponsored by IHS; to provide statistics and use statistical data for research purposes.

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

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 552a, Privacy Act of 1974; 4 U.S.C. 2901, Federal Records Act; 42 U.S.C. 248, Section 321 of the Public Health Service Act, as amended; 42 U.S.C. 254a, Section 327A of the Public Health Service Act, as amended; 25 U.S.C. 13, Snyder Act; 25 U.S.C. 1601 et seq., Indian Health Care Improvement Act; and 2 U.S.C. 2001-2004, Transfer Act of 1954.

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.

09-17-0001 IHS Medical Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
- In-Person
- Hardcopy
- Email
- Online
- Other

Government Sources
- Within the OPDIV
- Other HHS OPDIV
- State/Local/Tribal
- Other Federal Entities

Non-Governmental Sources
- Public

Identify the OMB information collection approval number and expiration date

OMB Approval is not required. This Electronic Dental System falls under the Clinical Exam Exception at 5 CFR 1230.3(h)(5).

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.

Not applicable

Describe the procedures for accounting for disclosures.

The IHS, with respect to each system of records under its direct control (i.e., Privacy Act System of Record 09-17- 0001, Medical, Health, and Billing Records) must keep a record of the date, nature, and purpose of each disclosure of a record to any person or Agency under subsection (b) of the Privacy Act (5 U.S.C. § 552a) and the name and address of the person or Agency to whom the disclosure is made. This record must be kept for 5 years or the life of

the record; whichever is longer, after the disclosure for which the accounting has been made. An individual (beneficiary) is entitled, upon request, to get access to this disclosure record of his or her own personal records with the exception for disclosures made under subsection (b)(7) of the Privacy Act (as a result of civil or criminal law enforcement activity). The IHS must inform any person or other Agency about any correction or notation of dispute made by the IHS in accordance with subsection (d)(4) of the Privacy Act (Access of Records) of any record that has been disclosed to the person or Agency if an accounting of the disclosure was made. This is a mandatory reporting requirement and may be recorded utilizing the IHS-505, "Disclosure Accounting Record" form.

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

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of PHI and of the individual's rights and IHS' legal duties with respect to PHI. A copy of the Notice is provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office provides a copy of the current Notice to the patient. The staff member has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record.

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.

The registration staff informs the patient of the requirements of the Privacy Act and HIPAA, and the date is entered into the Patient Registration System(PRS). The registration staff member will provide a copy of the current Notice to the patient and will briefly summarize the purpose of the Notice. The patient does not have to read the Notice, instead an alternate means may be used to communicate the content, e.g., a video shown in the waiting room or a staff member or accompanying family member may read the Notice to the patient. The staff member must ask the patient if he or she has any questions. The Notice describes the patient’s right to revoke authorization to use or disclose information, as well as restrict disclosures for certain uses.

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

It is IHS policy to provide adequate notice of its uses and disclosures of PHI/PII and of the individual's rights and IHS' legal duties with respect to PHI/PII. The IHS prominently and clearly displays the Notice (2-7.18) in every facility (http://www.hipaa.ihs.gov/). A copy of the Notice is also provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office or other appropriate department provides a copy of the current Notice to the patient. The patient acknowledges receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. An IHS staff member signs and dates the Acknowledgement form and files the signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" into the patient's medical record. No less than every three years, IHS provides notification of the availability of the Notice and how to obtain the Notice. If the Notice is revised by a material change, the revised Notice must be posted in clear and prominent locations in every facility and on its web site, on or after the effective date of the revision. The revised Notice will be posted on the IHS website within the 60 days of a material revision. The revised Notice is also given to all patients who come into a facility after the effective date of the revision and is available upon request on or after the effective date of the revision. Additionally, IHS provides the revised notice to all eligible patients registered in the patient registration system within 60 days of the revision of the Notice. Any individual, whether or not a patient, has the right to request and receive a copy of the Notice at any time, except an inmate. Inmates have no rights to the Notice (45 CFR § 164.520 (a)(3)). Any major

changes in the system that affect how PII is disclosed or used will require signed approval from each individual before disclosure occurs. This would be obtained digitally when the patient comes in to be seen by the provider.

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.

According to IHS policy all complaints regarding HIPAA Privacy and Privacy Act violations shall be addressed to the Chief Executive Officer or designee. Complaints must be documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Individuals may also file complaints directly to the Secretary, Department of Health and Human Services (HHS).

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

As each patient checks in to the dental clinic the dental receptionist accesses the patient record and verifies the accuracy and updates it as needed. The system tracks all changes to data, and who made the changes and can be recovered and viewed. The system can be defined to limit who has permission to access, and change data.

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.

The system employs Role-Based Access Control (RBAC) which ensures users have the minimum level of access required to complete day-to-day job duties. The system captures audit trails to maintain accountability on the system (s), meaning it tracks which users make changes and what changes they make to the 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.

The system employs Role-Based Access Control (RBAC) which ensures users have the minimum level of access required to complete day-to-day job duties.

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.

HHS Security Training and Awareness
IHS Information Systems Security Awareness annual training

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

HIPAA Privacy
HIPAA Security
Privacy Act Basics

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 Retention Schedule Number DAA-0513-2014-0003, sequence 0003, titled "Health Records File. Electronic Health Record." cites the Retention Period as follows: "Destroy/delete 75 years after last episode of patient care or date of death."

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

EDR systems are subject to all IHS security policies and procedure regarding administration and operation of sensitive systems. These policies address comprehensive administrative, technical, and physical controls. EDR servers are securely maintained physically, technical controls have been designed into the system to restrict access to only those with a need to know, and encryption is employed when EDR data leaves the local network. The EDR system has an existing Authority to Operate (ATO) certification and is under continuous three-year ATO cycle recertification and accreditation. The last ATO three-year recertification was granted on October 1, 2020. The three-year cycle ATO review and security assessment is being performed and any outstanding issues will be addressed in a Plan of Action and Milestones (POAM) to the satisfaction of the Designated Approving Authority (DAA)

In a typical clinic configuration, the EDR server(s) are located in a locked, access-controlled, computer room together with the RPMS and the telecommunications equipment servers. The client software runs on workstations in the service areas called “operatory(ies)”, in the provider offices, and in the Administrative/reception areas of the dental clinics. The EDR server and the clients use the existing LAN and/or WAN (for remote dental clinics with no local EDR database or application server) to inter-operate. Ensemble, the interface engine software for the Resource Patient Management System(RPMS)–EDR interface, will use Secure Socket Layer (SSL) encryption. Federal Information Processing Standard(FIPS) 140-2 CISCO(brand) routers and clients will be used to establish secure connections over a WAN depending on the type of configuration needed at each site. IHS OIT plans to push Group Policy Objects to EDR servers connected to the IHS D1 Domain. This Group Policy named “Network Policy Server(NPA) Member Srv Security Policy” will set local EDR server security settings in a manner compliant with IHS security policy. Typically this policy includes custom settings for User Rights/ Security and Network options such as (Audit generation, Log file, Registry permissions settings).