US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

March 08, 2022

OPDIV:

IHS

Name:

AARingMd

TPWA Unique Identifier:

T-5687858-107677

Is this a new TPWA?

Yes

Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

Yes

Indicate the SORN number.

SORN Number: 09-17-0001

If SORN is not yet published, identify plans to put one in place.

null

Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

No

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

Expiration Date: 1/1/01, 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: null

Does the third-party Website or application contain Federal Records?

Yes

Describe the specific purpose for the OPDIV use of the third-party Website or application:

AA RingMD will be the clinical video telehealth platform that will be used to support telehealth at the Indian Health Service with healthcare providers, patients and others joining the encounter (audio and/or video). AA RingMD will capture the demographic data to register users both patients and healthcare providers. The visit date is captured in the Indian Health Service Resource and Patient Management System (RPMS) which is the Electronic Health Record (EHR).

Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?

Yes

Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:

The public can use an in-person visit or another Telehealth platform.

Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?

Yes

How does the public navigate to the third party Website or application from the OPIDIV?

They will recieve an email containing the URL/ link to their visit

Please describe how the public navigate to the thirdparty website or application:

The public will click the link which takes them to their secure visit.

If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to anongovernmental Website?

No

Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?

Yes

Provide a hyperlink to the OPDIV Privacy Policy:

ihs.gov/privacypolicy

Is an OPDIV Privacy Notice posted on the third-part website or application?

No

Is PII collected by the OPDIV from the third-party Website or application?

Yes

Will the third-party Website or application make PII available to the OPDIV?

Yes

Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:

The healthcare provider will document the telehealth encounter in the Resource and Patient Management system (RPMS) as the system of record. The intended use of the PII is to support patient care. PII elements captured are: "Name," "Email Address," "Phone Numbers," "Medical Records Number" and "IHS staff login credentials." Audio or video will not be collected.

Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:

The user receives an email containing their email address. No further PII is provided except the date and time of the visit.

If PII is shared, how are the risks of sharing PII mitigated?

IHS is not linking PII to the email address.

Will the PII from the third-party website or application be maintained by the OPDIV?

Yes

Describe how PII that is used or maintained will be secured:

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

What other privacy risks exist and how will they be mitigated?

The telehealth platform is being configured to allow a guest to join the visit (e.g interpreter, consultant, guardian). The privacy risk is mitigated by giving the patient the ability to agree or object to others joining the telehealth encounter.