Universal Service Administrative Co.

PRIVACY IMPACT ASSESSMENT FOR THE RURAL HEALTH CARE (RHC) SYSTEM BOUNDARY

February 22, 2022

Record of Approval

Document Approval		
USAC PRIVACY POC		
Laurence H. Schecker		**Senior Advisor, Associate General Counsel and Privacy Officer**
Signature Laurence Schecker	**Date** Feb 22, 2022	
Accepted by:		
Linda S. Oliver		**FCC Acting Senior Agency Official for Privacy**
Signature Linda L. Oliver Digitally signed by Linda L. Oliver Date: 2022.02.24 09:28:32 -05'00'	**Date**	

Version History

Date	Description	Author
TBD	Privacy Impact Assessment	L. Schecker, R. Kolachina, M. Mansur

Table of Contents

Rural Health Care System

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks."[2]

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by OMB and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

The Universal Service Administrative Company's (USAC's) Privacy Officer will conduct an **Initial Privacy Assessment (IPA)** with the Information System Security Officers (ISSOs), the system's manager(s), in collaboration with others who routinely work with the system and the information it collects, uses, stores, and shares. The USAC Privacy Officer, in consultation with the FCC Senior Agency Official for Privacy (SAOP), uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the USAC Privacy Officer and the FCC SAOP make a determination that a PIA is needed.

If you have any questions, please contact the USAC Privacy Officer at privacy@USAC.org or the FCC Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. User System Boundary Overview

For each IT system that resides within the RHC System Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII, the System of Records Notice (if applicable), the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

Please copy the table as necessary to complete the information for each system within the boundary.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Rural Health Care System
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The RHC System functionality requires USAC to use and store only business information, including business contact information for individuals. It is possible for individuals, contrary to instructions, to provide personal rather than business information. If that were to occur, the categories of business and personal information could include contact information, employer identification numbers (which could be social security numbers (SSN) only if individual provided it instead of business employer identification number (EIN)), and bank account information for payment processing, as well as other PII elements entered into free text fields.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? Because the RHC System collects and maintains business contact information only, it is covered by FCC-2, Business Contacts and Certifications.
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. §§ 254(h)(1)(A) and 254(h)(2)(A); 47 C.F.R. §§ 54.600 – 54.633.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

A. Is this a new ATO Boundary or an existing ATO Boundary?

☒ New Boundary

☐ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service USAC receives/will receive from the cloud computing provider:

N/A

☐ USAC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [AWS S3]

☐ USAC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS)

☐ USAC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS)

C. **If the IT systems in the ATO Boundary are in the cloud, are the they FedRAMP certified?**

N/A

☐ Yes, all the IT systems are FedRAMP certified

☒ No, none, or only some, of the IT systems are FedRAMP certified

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

The business PII (or individual PII included contrary to instructions) is collected to identify and validate the entity seeking to receive financial assistance.

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third-parties? If collected from individuals themselves, link to the Privacy Act Notice[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

Business PII will be collected from individuals. USAC's privacy notice is posted on its website -- https://www.usac.org/about/privacy-policies/

C. What steps is USAC taking to limit the collection of PII to only that which is necessary?

USAC collects only information mandated by the FCC under the RHC rules, orders, and other guidance. For the RHC system, this is business PII (unless individual PII is entered contrary to instructions).

D. What steps will USAC take to make sure this PII is accurate, complete, and up-to-date?

Health Care Providers (HCPs) either through HCP users or designated consultants or consortia apply for funding and must provide business-related PII in order for applications to be reviewed and funds to be committed for compliant applications. The HCP is responsible for providing accurate, complete, and up-to-date information in order to receive a funding commitment from USAC. Service providers must provide accurate invoices in order to be paid on a commitment. The review process for applications provides verification that business-related PII provided by HCPs or others is accurate, complete, and up-to-date.

1.4. Use of the Data

A. **Please explain the data flow, including whether the PII will be ingested from, or shared with, another system.**

The RHC System collects business PII including business contact information for individuals; it is not intended to collect individual PII, but may collect individual PII entered contrary to instructions . Data input into the RHC System by HCPs and Service Providers is shared with the USAC Enterprise Data Services (EDS), which stores RHC data in the Enterprise Data Warehouse (EDW). RHC also shares disbursement information

[4] A Privacy Act Notice must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

with USAC's Financial Operations System (FOS) and receives service provider information from E-File.

B. Will the information be shared with third-parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

Yes. The RHC database is accessed through a VPN by the FCC in order to populate FCC's Enterprise Data Management (EDM) data warehouse. An external user of the system, including an HCP applicant, consortium, consultant, or service provider, is able to access its RHC System information (as authorized by the HCP) within the RHC Program. There is otherwise no sharing with third parties (e.g., through an "API").

C. How long will the PII be retained and how will it be disposed of?

The Rural Health Care Program records are retained in accordance with the National Archives and Records Administration (NARA) Records Schedule Number DAA-0173-2017-0001-0004. Disposal of obsolete or out-of-date paper documents and files is by shredding only. Electronic data, files, and records are destroyed by electronic erasure in compliance with NIST guidelines.

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X__Moderate**	**___Low**
Integrity	**__High**	**_X__Moderate**	**___Low**
Availability	**__High**	**_X__Moderate**	**___Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

Transmission of RHC data between RHC and other USACsystems such as FOS and Enterprise Data Services (EDS), and between RHC and the FCC EDM, is protected through firewalls and secured sockets layer (SSL) encryption, and indirect transfers of data are protected by encryption or comparable security safeguards. RHC operates on a FISMA Authorized infrastructure provided by USAC's General Systems and Services (GSS) system that provides network management, data protection, access control, and system auditing controls in concert with RHC system level controls. The RHC system also inherits USAC Enterprise Common Controls (ECC) that are provided for all USAC systems and include privacy and IT Security policies and controls.

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU) , or similar document is in place, please summarize the privacy applicable portions of the document.

RHC does not inherit controls from any external provider.

An umbrella ISA is maintained between USAC and the FCC for population of the FCC EDM with USAC data. An addendum is maintained specifically for RHC that allows FCC to retrieve data directly from RHC databases.

1.6. Access to the Information

A. Which types of users will have access to the PII in this information system?

Reports regarding RHC activities may potentially include information about specific business entities and contact information, and those reports are available only to limited USAC and FCC staff on a least privilege and need-to-know basis. Reports generated from RHC are provided to USAC managers for verification and approval of the RHC users. Reports may also be generated and provided pursuant to inquiries received under applicable law.

B. Does this system leverage Enterprise Common Controls (ECC)?

RHC leverages Enterprise Common Controls. RHC uses multi-factor authentication through OKTA.

C. Does the system leverage the FCC's Accounting for Disclosure control?

No.