Available for Public Use

Universal Service Administrative Co.

PRIVACY IMPACT ASSESSMENT FOR THE CONNECTED CARE PILOT PROGRAM

January 6, 2021

Prepared by:

Laurence H Schecker, Associate General Counsel and Privacy Officer, USAC

Max Mansur, ISSO, USAC

Record of Approval

Document Approval		
USAC Privacy POC		
Printed Name: Laurence H Schecker		**Associate General Counsel and Privacy Officer**
Signature: Laurence H Schecker Digitally signed by Laurence H Schecker Date: 2021.01.08 10:24:16 -05'00'	**Date**	
Accepted by:		
Printed Name: Margaret Drake		**FCC Senior Agency Official for Privacy**
Signature: Margaret E Drake Digitally signed by Margaret E Drake Date: 2021.01.08 10:31:45 -05'00'	**Date**	

Version History

Date	Description	Author
12/7/2020	Draft of Privacy Impact Analysis (PIA)	L. Schecker and M. Mansur, USAC
12/9/2020	Revisions of Draft	B. Moradi, FCC OGC
1/6/2021	Final PIA	L. Schecker and M. Mansur, USAC

Table of Contents

Connected Care Pilot Program

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 FCC has directed the Universal Service Administrative Company (USAC) to comply with the requirements of the E-Government Act related to privacy. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

The FCC completed the **Initial Privacy Assessment (IPA)** for the CCP.[3] 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 of the E-Government Act, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination that a PIA is necessary.

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.

[3] Initial Privacy Assessment (IPA) for the Connected Care Pilot Program (FCC SAOP Oct. 2, 2020)

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO 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, if so, a brief description of the PII, the applicable Privacy Act System of Records Notice (SORN), 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 The Connected Care Pilot Program (CCP)
DOES THE SYSTEM CONTAIN PII? Yes[4]
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) CCP is an application on the USAC Appian Cloud that uses business information retrieved from the Rural Health Care (RHC) System (MyPortal) including business contact information for individuals. Users are instructed not to enter personally identifiable information. The responses in this PIA focus on PII in the form of business contact information for individuals, although it is possible for individuals, contrary to instructions, to provide personal rather than business information.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? N/A – This system does not retrieve information based on individual PII.
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. §§ 151-154, 201-205, 214, 254, 303(r), and 403.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. CCP data will be uploaded to the FCC's Electronic Comment Filing System (ECFS).

[4] *See Id.* (CCP IPA).

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

☐ New Boundary

☒ Existing Boundary

CCP is a new application on the existing EPC boundary that is in the process of being redefined to include CCP and other USAC applications that run on USAC's Appian Cloud. It will be renamed the USAC AppCloud system.

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[5] please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

☐ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]

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

Appian Cloud

☐ The FCC 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) [list applicable system(s)]

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

☒ Yes, all the IT systems are FedRAMP certified.

Appian Cloud

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

1.3. Collection of Data

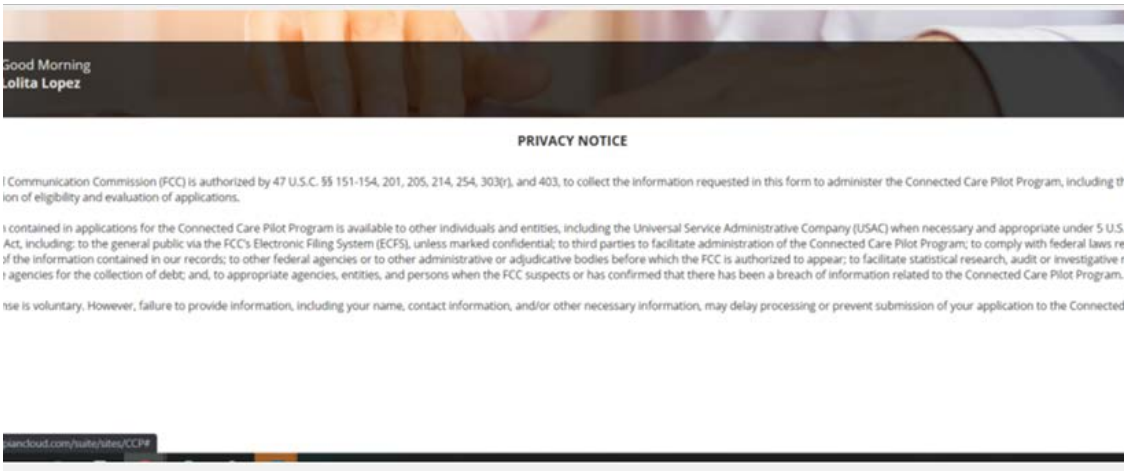
A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

[5] *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.

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

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 Statement[6] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

No PII is collected directly from individuals via CCP. The Health Care Provider (HCP) data is collected from USAC's RHC System (MyPortal). The Privacy Notice for the CCP is shown here



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

We only retrieve user information from the RHC System, which limits the collection of business PII to only that which is needed to perform the program mission.

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

The RHC system is responsible for any business-related PII that happens to be collected. Users of the RHC system are refreshed hourly in a table that is integrated with CCP such that a new user or deactivation of user in RHC is provisioned or deactivated in CCP.

[6] A Privacy Act Statement 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. CCP utilizes a Privacy Notice.

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.

Users are created in CCP by ingesting data from the RHC System. Applications and attachments filed in CCP will be posted to the FCC's Electronic Comment Filing System (ECFS), unless the user has marked the attachment confidential, in which case only the application will be posted to ECFS.

Are internal connections reflected in the System Security Plan (SSP)?

Yes.

Are Information Sharing Agreements (ISAs) created for external connections?

No, an ISA is not required for the only external connection because that connection is over Internet to FCC's Electronic Comment Filing System Public Application Programming Interface (API). This is a one-sided information flow to ECFS.

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")?

As described in 1.4.A., information will be shared to the FCC's ECFS via API. No information will be shared with third-parties directly from the system.

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

The records in CCP are retained pursuant to NARA Records Schedule Number DAA-0173-2017-0001-0004, adopted in USAC's record retention schedule (line 3) (10 years after the end of the calendar year from date filed or prepared, or when no longer needed for business or audit purposes, whichever comes later).

1.5. Data Security and Privacy

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

Confidentiality	**__High**	**___Moderate**	**_x__Low**
Integrity	**__High**	**___Moderate**	**_x__Low**
Availability	**__High**	**___Moderate**	**_x__Low**

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

The CCP application will reside in the Appian Cloud instance that also has the E-rate Productivity Center (EPC). The System Security Plan (SSP) for EPC is being rewritten as an AppCloud SSP that includes CCP and EPC. As such, the controls for CCP are aligned with the controls for EPC.

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.

No privacy controls are inherited from Appian Cloud. There is an ISA with Appian Cloud in place.

1.6. Access to the Information

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

USAC users (including USAC contractors), FCC users

B. Does this system leverage USAC multifactor authentication?

Yes, CCP will be using Okta MFA.

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

N/A – CCP is not a system of records as that term is defined by the Privacy Act, 5 U.S.C. 552a(a)(5).