U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Behavioral Health and Wellness Program (BHWP)
Bureau/Office: Bureau of Indian Education (BIE)
Date: November 15, 2022
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Bureau of Indian Education (BIE) is responsible for providing quality educational opportunities from early childhood through adulthood in accordance with federal trust responsibilities for approximately 43,000 American Indian and Alaska Native students. The BIE funds 183 elementary, secondary, and residential schools across 64 reservations and 23 states. Of these, 53 are BIE-operated and 130 are Tribally operated. Additionally, the BIE directly operates two post-secondary institutions and funds and/or operates off-reservation boarding schools and peripheral dormitories near reservations for students attending public schools. The

BIE also serves many American Indian and Alaska Native post-secondary students through higher education scholarships and support funding for Tribal colleges and universities.

The BIE is committed to creating positive, safe, and culturally relevant learning environments where students can gain the knowledge, skills, and behaviors necessary for physical, mental, and emotional wellbeing. The COVID-19 pandemic highlighted the need for comprehensive behavioral health and wellness services at a multitude of Bureau-funded schools, dormitories, colleges, and universities.

The BIE has contracted with Tribal Tech, LLC., to develop a new Behavioral Health and Wellness Program (BHWP) to address the mental health needs of students and staff at all Bureau-funded institutions including Bureau operated schools, Tribally Controlled Schools (TCS), post-secondary institutions, and Tribal colleges and universities. The BHWP's counseling program is designed to provide short-term, solution-focused brief therapy, crisis support, and care coordination via a tele-health platform and an available 24/7 crisis response hotline. To implement the BHWP in full and in accordance with required regulations including: the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the 42 CFR Part 2, Confidentiality of Substance Use Disorder Patient Records regulations, and the 25 CFR Part 43, Maintenance and Control of Student Records in Bureau Schools, the BHWP will use both an electronic health record (EHR) platform and practice management system, as well as a contracted crisis hotline service. Each are detailed below.

<u>BHWP's Electronic Health Record (EHR) Platform: AccuCare</u>
AccuCare is a web based EHR and practice management platform, developed and owned by Orion Healthcare Technology. Tribal Tech, LLC., has purchased the AccuCare platform to serve as the EHR for the BHWP. AccuCare will be utilized for documentation and providing the following behavioral health tasks: Client intakes, screenings, referral services, progress notes, treatment planning, crisis intervention, client chat, tele-health video options, electronic signature captures for consent documentation, release of information requests, uploading of external client records, data analysis, and reporting. Access to the AccuCare platform is limited to BHWP clinical staff who are licensed therapists or clinical social workers, care coordinators, and schedulers. Orion Healthcare Technology hosts the AccuCare system directly with Microsoft Azure to ensure services are provided through a secure, Health Information Trust Alliance (HITRUST) certified platform and Cyber Essentials Plus, which is the audited version of the Cyber Essentials information security standard, and which provides assurances that key information security controls are in place within an organization.

<u>BHWP's Crisis Hotline Provider: ProtoCall</u>
ProtoCall Services is a nationally recognized crisis hotline provider accredited by the American Association of Suicidology (AAS) and the Commission on the Accreditation of Rehabilitation Facilities (CARF). For BHWP, Tribal Tech, LLC., has sub-contracted with ProtoCall Services to deliver a crisis hotline which will be accessible 24 hours per day, 7 days a week, and 365 days a year, through a unique BHWP crisis call telephone number. ProtoCall Services' crisis call center, will be staffed with licensed behavioral health professionals, and will provide specific crisis support processes, including brief intakes, safety screenings, immediate crisis response, and referrals to BHWP clinicians for additional behavioral health services. ProtoCall's hotline

services are provided through a secure, HITRUST Certified, Health Insurance Portability and Accountability Act (HIPAA) of 1996 compliant platform, and the Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0 framework, which addresses the specific mandates of the Patient Protection and Affordable Care Act of 2010 and the Department of Health and Human Services for this type of service provision.

C. What is the legal authority?

- Every Student Succeeds Act (Pub. L. 114-95)
- Indian Education Policies (25 CFR Part 32)
- Expenditure of Appropriations by Bureau (25 U.S.C. § 2006)
- Indian Self-Determination and Education Assistance Act (Pub. L. 93-638)
- Congressional Statement of Findings (25 USC 5301)
- Indian Child Welfare Act of 1978 (Pub. L. 95-608, 25 U.S.C. 1901)
- Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2)
- Nondiscrimination under Federal Grants and Programs (29 U.S.C. § 794)
- Enforcement of Nondiscrimination on the Basis of Handicap in Programs or Activities Conducted by the Department of the Interior (43 CFR 17.501–17.570 (Subpart E))
- Rehabilitation Act of 1973 (Pub. L. 93-112, Section 504)
- Tribally Controlled Schools Act of 1988 (25 U.S.C. 2501 et seq.)
- Indian Affairs Manual Part 30 – Education (Management), Chapter 7 – Health and Wellness Policy
- IAM Part 30 Chapter 14, Suicide Prevention, Early Intervention, and Postvention Services
- IAM Part 34 – Post Secondary Education, Chapter 7 – Suicide Prevention, Early Intervention, and Postvention Services.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
BHWP's Electronic Health Record Platform: AccuCare	AccuCare is a web based EHR platform and practice management system. Personally identifiable information (PII) will be collected to initiate and provide clinical counseling services, crisis care coordination, and communication with the client and appropriate points of contact for referrals and continued service delivery or emergency care.	Yes	**Student information** including name, date of birth, mailing address, physical address, home and/or cell phone number, school of enrollment, grade level, Tribe of enrollment, and emergency contact information. **Student's parent, guardian, or caretaker information** including name, mailing address, physical address, home and/or cell phone number. **Clients who are:** **Federal staff/employee**. Information includes name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, and emergency contact information. **School level staff/employee.** Information includes name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, and emergency contact information. **Tribal staff/employee**. Information includes name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, and emergency contact information. **Emergency contact person**. Information includes contact's name, relationship to client, emergency contact phone and/or cell phone number. In the case of a critical incident, sentinel event or death, the PII

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
			may also include: the name of client, date of birth, age; address, parent, guardian, or caretaker information if applicable, emergency contact information, manner of death or incident type, location of death or incident, time of death or incident, any known witness or collateral contact, and their contact information at the time of client death or client related incident. This information may be shared with appropriate local, Tribal, city, county, state, or federal law enforcement officials and first responders for immediate emergency response engagement, medical centers for medical care, and social service or other agencies in the event of abuse or neglect. Information will be shared with appropriate BIE and BHWP officials and administrators, as well as Tribal officials as needed for appropriate critical incident or sentinel event reporting.
BHWP's Crisis Hotline Provider: ProtoCall Services	To provide immediate behavioral health crisis support and referral to the BHWP clinical staff as needed.	Yes	**Student information** including name, date of birth, mailing address, physical address, home and/or cell phone number, school of enrollment, grade level, Tribe of enrollment, and emergency contact information. **Student's parent, guardian, or caretaker information** including name, mailing address, physical address, home and/or cell phone number. **Clients who are: Federal staff/employee**. Information includes name, date of birth, mailing address,

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
			physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, and emergency contact information. **School level staff/employee.** Information includes name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, and emergency contact information. **Tribal staff/employee**. Information includes name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, and emergency contact information. **Emergency contact person**. Information includes contact's name, relationship to client, emergency contact phone and/or cell phone number. In the case of a critical incident, sentinel event or death, the PII may also include: the name of client, date of birth, age; address, parent, guardian, or caretaker information if applicable, emergency contact information, manner of death or incident type, location of death or incident, time of death or incident, any known witness or collateral contact, and their contact information at the time of client death or client related incident. This information may be shared with appropriate local, Tribal, city, county, state, or federal law enforcement officials and first responders for

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
			immediate emergency response engagement, medical centers for medical care, and social service or other agencies in the event of abuse or neglect. Information will be shared with appropriate BIE and BHWP officials and administrators, as well as Tribal officials as needed for appropriate critical incident or sentinel event reporting.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

During the development of this PIA, the BIE identified the need to publish a new System of Records Notice (SORN) to cover BHWP records, which has been drafted by the program office with the assistance of the IA Associate Privacy Officer and is being submitted for publishing in the Federal Register. This PIA will be updated after the new SORN is published in the Federal Register.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

The BHWP is working with the Indian Affairs Office of Regulatory Affairs and Collaborative Action to obtain OMB approval for information collections used by the BHWP. This PIA will be updated after OMB approval of information collections. The following forms will be included in the OMB approval request:

- Adult Intake Questionnaire
- Youth Intake Questionnaire
- Consent to Treat
- Demographic and Referral Form
- Authorization to Release Medical Records
- SOAP (Subjective, Objective, Assessment, Plan) Note Template

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Gender
☒ Birth Date
☒ Marital Status
☒ Medical Information
☒ Disability Information
☒ Education Information
☒ Emergency Contact
☒ Race/Ethnicity
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Student Information: Name, date of birth, mailing address, physical address, phone number, cell phone number, parent, guardian, or caretaker information, emergency contact information, school of enrollment, grade level, Tribe of enrollment.

Student's parent, guardian, or caretaker information: Name, relationship to student, mailing address, physical address, home and/or cell phone number, Tribe of enrollment.

Federal staff/employee information: Name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, emergency contact information.

School level staff/employee information: Name, date of birth, mailing address, physical address, home and/or cell phone number, school affiliation, Tribe of enrollment, emergency contact information.

Tribal staff/employee information: Name, date of birth, mailing address, physical address, home and/phone number, school affiliation, Tribe of enrollment, emergency contact information.

Emergency Contact Person: Contact's name, relationship to client, emergency contact phone or cell phone number.

Disability information such as a client's Individualized Education Plan (IEP) or 504 Plan.

In the case of a critical incident, sentinel event, death, or crisis incident, PII may also include client name; age; date of birth; address; parent, guardian, or caretaker information if applicable; emergency contact information; manner of death or incident type; location of death or incident; date and time of death or incident; any known witness or collateral contact; and their contact information at time of client death or client related incident. This information may be shared with appropriate local, Tribal, city, county, state, or federal law enforcement officials and first responders for immediate emergency response engagement; medical centers for emergency medical care, and social service or other agencies in the event of abuse or neglect. Information will be shared with appropriate BIE and BHWP officials and administrators as needed, as well as Tribal officials as needed for appropriate critical incident or sentinel event reporting.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
□ Tribal agency
□ Local agency
□ DOI records
□ Third party source
□ State agency
☒ Other: Parents or legal guardians of minors. Information may be provided by authorized BIE personnel and educational staff.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
□ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems - Information may be shared between the ProtoCall Services Crisis Hotline provider system and the AccuCare electronic health record platform to initiate and provide clinical counseling services, crisis care coordination, and communication with the client and appropriate points of contact for referrals and continued service delivery or emergency care.

□ Other: *Describe*

D. What is the intended use of the PII collected?

The intended uses of the PII collected by the BHWP are to enable initiation of short-term solution focused brief therapy; crisis support; and care coordination for students and staff participating in service provision. This includes PII information necessary to obtain appropriate consent to provide treatment; completion of clinical intake, screening, assessment, treatment planning for the client; and referral for additional service provision, in accordance with all application of federal regulations governing such service provision. PII obtained also ensures appropriate care coordination and emergency contact support in the event of a critical incident, sentinel event, or death. In these instances, PII will be utilized to alert available medical centers, such as the Indian Health Service or other medical facility; EMS; and local, Tribal, city, county, state, or federal law enforcement personnel for immediate crisis response; social service or other support agencies; and Tribal officials as necessary or required. Additionally, in the event of a critical incident, sentinel event, as defined by the BIE's Critical Incident Policy, PII will be collected to complete and submit required reports such as the BIE's Suspected Child Abuse and Neglect (SCAN) and Critical Incident Report (CIR) forms.

De-identified information may be collected to provide BHWP analytics on the types of services accessed, demographic information (i.e., client age, gender, etc.), school information, number of students and staff served, top five counseling issues or trends occurring each month, and other information determined by BIE to exercise management oversight of the program, evaluate client participation, and for use in briefings, data calls, and reports. Regularly required BHWP reports will not include any PII from clients who have used services and these reports will adhere to all applicable confidentiality regulations.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Limited information may be shared with BIE employees acting in their official capacity in the performance of official functions to facilitate additional behavioral health service referrals, report critical incidents, sentinel events such as suspected abuse or neglect, and deaths. Most of the information does not contain PII. However, de-identified information is used to provide analytics on the types of services accessed, demographic information (i.e., client age, gender, etc.), school information, number of students and staff served, top five counseling issues or trends occurring each month, and other information determined by BIE to exercise management oversight of the program, evaluate client participation, and for use in briefings, data calls, and reports.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

After obtaining client consent, data may be shared with federal agencies, such as the Indian Health Service, to assist BHWP with completing referrals for clients in need of long-term counseling services or follow up medical or behavioral health care. When required by law, data may also be shared with federal law enforcement and/or federal social service agencies for immediate crisis support, critical incident response, and to report sentinel events such as suspected child abuse and/or neglect or death of a participating student or staff member.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state, or local agencies and how the data will be used.*

Data may be shared with Tribal, state, local, or private agencies and medical centers to assist the BHWP with completing referrals for clients in need of long-term counseling services, or follow-up care, crisis support, critical incident response, and to report sentinel events such as suspected child abuse and/or neglect or the death of a participating student or staff member.

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with contracted BHWP employees acting in their official capacity in the performance of official functions to provide clinical services provision; provide referral for continued long-term services; and report critical incidents, sentinel events such as suspected abuse or neglect, and death. Information may be shared with contractors providing IT support services for routine maintenance, future system enhancements and technical support.

☐ Other Third-Party Sources: *Describe the third-party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

The services provided by the BHWP are voluntary and individuals can terminate services at any time. Additionally, individuals can decline to provide information or consent to the use of their PII at any time during the counseling and/or crisis support process. However, if an individual does not wish to provide the PII necessary for completing the intake process, the BHWP will not be able to provide counseling services and/or crisis support.

BHWP services are strictly voluntary. Once an individual elects to enter into BHWP services, they have the right to refuse service provision at any point in the counseling process. For example, by refusing to provide their PII for initial entry to service; refusing to acknowledge receipt of Notice of Privacy Practices information; refusing initial consent to treat; withdrawing consent for treatment in progress; ending a Tele-behavioral health session in progress; declining referral for services; or declining to provide a release of information for referral purposes, this will be interpreted as the client declining further services. If a client refuses to consent or withdraws their consent for treatment, counseling services cannot be provided by the BHWP. However, information regarding outside behavioral health providers and/or resources will be shared with the client.

Declination, termination, or refusal of BHWP services does not exclude an individual from requesting or accessing BHWP services in the future. However, to resume BHWP services, all required PII, acknowledgement of Notices of Privacy Practices, and consent for service provision will need to be obtained prior to services commencing.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

BHWP clients are provided a Privacy Act Statement, HIPAA Notice, and FERPA Notice as appropriate.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this PIA and the new BHWP SORN that will be published in the Federal Register.

☒ Other: *Describe each applicable format.*

As part of the BHWP intake process, students and/or staff are provided the appropriate and applicable Notice of Privacy Practice statements (FERPA, HIPAA, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools, and/or 42 CFR Part 2 Notice of Privacy Practices). Adult clients must acknowledge receipt and understanding of the Notice(s) before initiating BHWP counseling services. For student clients their respective parent, guardian, or caretaker, must acknowledge receipt and understanding of the Notice(s) before initiating BHWP counseling services. The BHWP will also ensure a privacy notice banner is displayed for all licensed BHWP users accessing the AccuCare system.

For individuals accessing the BHWP's crisis hotline managed by ProtoCall Services, all crises support services are handled via telephone and will not include access to a virtual privacy notice banner. For authorized BHWP users accessing the ProtoCall Services customer portal for daily call reports, a privacy banner will be implemented prior to system launch.

□ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

BHWP client records created and located in the BHWP electronic health record, AccuCare, are retrieved manually by licensed BHWP users in the system. BIE personnel do not have access to client records. Built-in filters allow users to retrieve data by client name or client identified record number. Additionally, de-identified aggregate data, such as diagnosis codes, numbers of encounters, and types of encounters may be retrieved from within the system, along with general demographics. Summary reports can be generated automatically, or raw data can be exported into a database format for specific records or as an aggregate.

Data from the BHWP's crisis hotline provider, ProtoCall Services, including name, age, gender, school affiliation, address, and call type is retrieved manually only by authorized BHWP staff via the ProtoCall Services Customer Portal.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Generally, BHWP reports generated for BIE leadership are for statistical and programmatic uses only and will not contain any PII. However, in the case of a critical incident, sentinel event, or death, reports may be generated from either BHWP's EHR, AccuCare or BHWP Crisis Hotline Provider, ProtoCall Services, and include the following types of PII: name, date of birth, address, client information, parent, guardian or caretaker information, emergency contact information, Tribe of enrollment, school enrollment or affiliation, manner of death or incident type, location of death or incident, date and time of death or incident, any witness contact information at time of a client critical incident, sentinel event, or death. This information will be shared with the appropriate local, Tribal, city, county, state, or federal law enforcement officials and first responders for immediate emergency response engagement, medical centers for emergency medical care, and social service or other agencies in the event of abuse or neglect. Information will be shared with authorized BIE leadership and program officials, contractors, and administrators, as well as all Tribal officials as needed for appropriate critical incident or sentinel event reporting.

Reports generated for the BHWP ProtoCall Services may include individual caller name, age, gender, school affiliation, address information and call type, is retrieved manually only by persons authorized by Tribal Tech, LLC., through the ProtoCall Customer Portal. Reports containing client information are not shared with BIE. Reports prepared for BIE officials do not contain PII, they are used to provide analytics on the types of services accessed, demographic information (i.e., client age, gender, etc.), school information, number of students and staff served, top five counseling issues or trends occurring each month, and other information determined necessary by BIE to exercise management oversight of the program. ProtoCall will provide aggregate call data including the number of hotline calls received and answered, the average speed of answer, the percentage of hang ups by callers after 30 seconds, and the percentage answered within 30 seconds. Tribal Tech, LLC., will be provided with call documentation or records associated with an individual phone call from a person if follow up care is needed and if referral into BHWP services is requested. In the event of a critical incident, sentinel event or death, ProtoCall will provide all information requested for immediate response needs including contact to local, Tribal, county, city, state, or federal law enforcement and first responders. ProtoCall will provide to BHWP officials all information necessary for required critical incident or sentinel event reporting and to any additional required service programs such as social service agencies.

Both the AccuCare EHR and ProtoCall Services systems have features that allow reports to be generated from data in the system or user actions within their respective systems. Audit logs for AccuCare can be manually accessed by BHWP system administrators through a request to Orion Healthcare. Audit logs can capture licensed user access and actions performed in the system including licensed username and account creation, licensed user record modification, client record creation, client record modification, disabling or termination of licensed user account access; user logon date and time; number of failed login attempts; and files accessed. Clinical record activities can be tracked based on record type including intake, assessment, screening, treatment plan, progress note, and referral. Additional utilization reports for clinical service type, demographic information, and prevention data can be exported through a Data Query module accessed by licensed administrative users.

ProtoCall Services also utilizes audit logs detailing an individual user's authorized access and actions performed within the ProtoCall Service system. Audit logs can capture user access and actions performed in the system including username and account creation, user record modification, call record creation, call record modification, disabling or termination of user account access, user logon date and time, number of failed login attempts, and files accessed are available to authorized BHWP staff upon request.

□ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Client demographic and clinically required data is collected by the BHWP Care Coordinator and BHWP licensed providers from the school point of contact at time of client referral, from the client individually, and from the client's parent, guardian, or caretaker when necessary. Information is entered at the time of receipt into the AccuCare electronic health record and cross-checked verbally with the school point of contact, the client individually and with the parent, guardian, or caretaker to ensure proper receipt of client name, and correct spelling of name, address, demographic information, phone number, school affiliation or school of enrollment to ensure accurate data information at client record creation and data entry.

BHWP Care Coordinators and licensed providers rely on the school point of contact, the individual client, and the parent, guardian, or caretaker where applicable for the accuracy and timeliness of data and information gathered. At each clinical encounter, the licensed provider will take steps to re-verify the client's name, demographic information and ask about any changes to demographic information since the last clinical encounter to ensure continued accuracy.

ProtoCall Services hotline responders verify the spelling of the first and last name of the caller, any demographic information provided by the caller, as well as the caller’s phone number by verbally reading back the information gathered and verifying the accuracy of data entry into its software. ProtoCall Service hotline responders are reliant on the caller for accurate data and information at time of call receipt and response. Calls received generate a singular unique call record that is not duplicated or expanded.

Clients can seek records about themselves that are maintained in this system of records and if the individual believes the records are not accurate can request corrections or the removal of material from the record by writing to the System Manager identified in the BHWP SORN or by contacting the IA Associate Privacy Officer. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K and, as applicable, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools.

B. How will data be checked for completeness?

As noted above in Section 3, Part A, client demographic and clinically required data is collected by the BHWP Care Coordinator and BHWP licensed providers from the school point of contact at time of client referral, from the client individually, and from the client’s parent, guardian, or caretaker when necessary and checked for completeness and accuracy. Information is entered at the time of receipt into the AccuCare electronic health record and cross-checked verbally with the school point of contact, the individual client, and with the parent, guardian, or caretaker to ensure completeness and proper receipt of client name, correct spelling of name, address and demographic information, phone number, and school affiliation or school of enrollment at time of record creation and data entry.

BHWP Care Coordinators and licensed providers rely on the school point of contact, the individual client, and the parent, guardian, or caretaker where applicable for the completeness, accuracy, and timeliness of information gathered. At each clinical encounter, the licensed provider will take steps to re-verify the client's name, demographic information and inquire of any changes to demographic information since the last clinical encounter to ensure continued completeness of the data record.

As noted above in Section 3, Part A, ProtoCall Services hotline responders verify the complete spelling of the first and last name of the caller, any demographic information provided by the caller, as well as the caller’s complete phone number by verbally reading back the information gathered and verifying that accuracy and completeness of data entry into its software. ProtoCall Service hotline responders are reliant on the caller for providing complete and accurate data and information. Calls received generate a singular unique call record that is not duplicated or expanded.

Clients can seek records about themselves that are maintained in this system of records and if the individual believes the records are not complete can request corrections or the removal of material from the record by writing to the System Manager identified in the BHWP SORN or by contacting the IA Associate Privacy Officer. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K and, as applicable, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

As noted above in Section 3, Parts A and B, client demographic and clinically required data is collected by the BHWP Care Coordinator and BHWP licensed providers from the school point of contact at the time of client referral, from the individual client, and from the client's parent, guardian, or caretaker when necessary and checked for accuracy and completeness and verified as the most current information. BHWP Policy and Procedures outline procedures to ensure information is entered at the time of receipt by the Care Coordinator or licensed provider into the AccuCare electronic health record and cross-checked verbally as current with the school point of contact, the individual client, and with the parent, guardian or caretaker to ensure complete and proper receipt of client name, spelling of name, complete address and demographic information, correct spelling of address, complete phone number, and school affiliation or school of enrollment at time of record creation and data entry.

BHWP Care Coordinators and licensed providers rely on the school point of contact, the individual client, and the parent, guardian, or caretaker where applicable for the accuracy, timeliness, completeness of information gathered, and verification that the information provided is the most current. BHWP Policy and Procedures outline procedures that require the licensed provider at each clinical encounter, to take steps to re-verify with the client's name, demographic information and inquired of any changes to demographic information since the last clinical encounter to ensure continued completeness of the data record, and verify the information is current.

As noted above in Section 3, Parts A and B, ProtoCall Services hotline responders verify the complete spelling of the first and last name of the caller, any demographic information provided by the caller, as well as the caller's phone number by verbally reading back the information gathered and verifying that accuracy and completeness of data entry into its software, and verification from the caller that the information is current. ProtoCall Service hotline responders are reliant on the caller for providing current, complete, and accurate data and information. Calls received generate a singular unique call record that, per ProtoCall Service policy and procedure, is not duplicated or expanded. An individual may call the crisis line more than once, however each call is treated as a singular unique call record.

Clients can seek records about themselves that are maintained in this system of records and if the individual believes the records are not current can request corrections or the removal of material from the record by writing to the System Manager identified in the BHWP SORN or by contacting the IA Associate Privacy Officer. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K and, as applicable, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

A records retention schedule for the BHWP is being developed and will be submitted to the National Archives and Records Administration (NARA) for scheduling and approval. Pending approval by NARA, records will be treated as permanent records.

Records associated with a 42 CFR Part 2 program that is discontinued or is taken over or acquired by another program will be processed per 42 CFR § 2.16 Security for records and § 2.19 Disposition of records by discontinued programs.

Information Technology records are maintained under the Departmental Records Schedule (DRS) 1.4A Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the office's activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three years after cut-off.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

A records retention schedule for the BHWP is being developed and will be submitted to NARA for scheduling and approval. Pending approval by NARA, records will be treated as permanent records. Once the BIE receives an approved disposition authority from NARA, disposition of data will follow NARA guidelines and the approved Records Schedule for transfer, pre-accession, and accession activities to NARA. These activities will comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIE's records retention schedule. When records are eligible for disposition, system administrators dispose of records by shredding or pulping paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

Upon termination of service contract with the Contracting Agency, the Contractor will transfer all electronic health record information to the BIE for appropriate record keeping and storage in alignment with all federal requirements.

Records associated with a 42 CFR Part 2 program that is discontinued or is taken over or acquired by another program will be processed per 42 CFR § 2.16 Security for records and § 2.19 Disposition of records by discontinued programs.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure, and destruction) affect individual privacy.

There is a high risk to the privacy of individuals due to the sensitive PII contained in the BHWP. BHWP is rated as a FISMA high system and requires management, operational, and technical controls established by NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information. Orion hosts their system directly with Microsoft Azure provided through a secure, HITRUST Certified platform and the Cyber Essentials Plus (audited version of the Cyber Essentials information security standard) which provides assurance that key information security controls are in place within an organization. ProtoCall Services detailed call documentation is provided through a secure, HITRUST Certified, HIPAA Compliant platform, and the MARS-E 2.0 framework, which addresses the mandates of the Patient Protection and Affordable Care Act of 2010 and the Department of Health and Human Services.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to information is strictly limited to authorized personnel who need access to perform official functions. System and information access is based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. System administrators use user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Employees annually complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure they understand their responsibility to protect privacy. Employees and contractors must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hard copy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that BHWP may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained to provide a service or perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official duties. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and “need-to-know” factors, based on the “least privilege” principle. Access restrictions to data and various parts of the system’s functionality is role-based and requires BHWP Manager approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. BHWP meets information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. Information is gathered directly from the individual client and if appropriate, the client’s parent/guardian or caretaker; or the school point of contact making referral. It is possible that inaccurate information may be obtained from any of these points of contact. However, BHWP team members interacting with an individual client, and if applicable, their parent, guardian, or caretaker, will work to verify all demographic information on file is correct, complete, and current at each encounter.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The BHWP is responsible for the creation, management, retention, and disposition of the clinical records in the AccuCare electronic health record as the information owner in accordance with required regulations and approved NARA records retention schedule. The BIE ensures only records needed to support its program, Tribes, and Tribal members is maintained. Information collected is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
A records retention schedule for the BHWP records is being developed and will be submitted to NARA for scheduling and approval. Pending approval by NARA, BHWP records will be treated as permanent records. BHWP system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password

files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off.

Records associated with a 42 CFR Part 2 program that is discontinued, assumed, or acquired by another program will be processed per 42 CFR § 2.16 Security for records and § 2.19 Disposition of records by discontinued programs.

There is a risk that individuals may not have adequate notice on how their PII will be collected and used. This risk is mitigated as individuals are notified of the privacy practices through this PIA, privacy notice, and Privacy Act Statements, as well as the new BHWP SORN that will be published in the Federal Register. During the development of this PIA, the BIE identified the need to publish a new SORN to cover BHWP records, which is currently being drafted by the program office with the assistance of the IA Associate Privacy Officer. This PIA will be updated after the new SORN is published in the Federal Register. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used. This risk is also mitigated in that service provision cannot move forward without client, or where appropriate, their parent, guardian, or authorized caretaker's receipt of the appropriate Notice of Privacy Practice forms, and their written or electronically signed acknowledgement of receipt of the Notice of Privacy Practice, FERPA, HIPAA, 25 CFR Part 43 Maintenance and Control of Student Records in Bureau Schools, and/or 42 CFR Part 2 Notice of Privacy Practices forms.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The AccuCare EHR is hosted on Microsoft's HITRUST-certified Azure platform, which is a DOI-approved and FedRAMP-certified cloud service provider. The cloud service provider implements protections, controls and access restrictions as required to maintain the necessary FedRAMP certification. Access to the AccuCare application is restricted to licensed users only. Data is backed up nightly with redundancy and offsite storage. ProtoCall Services has deployed its primary call center application in Microsoft's HITRUST certified Azure platform. Microsoft Azure also hosts the Customer Portal.

In addition to the risk mitigation actions described above, the "least privilege" security principle, such that only the least amount of access is given to a user to complete their required activity, is enforced. All access is controlled by authentication methods to validate the authorized user. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information modules before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The use of the system and data collected is relevant and necessary to the purpose for which BHWP was established and supports the Indian Affairs mission outlined in 25 CFR Part 32, Indian Education Policies; Indian Self-Determination and Education Assistance Act (Pub. L. 93-638, 25 U.S.C. 450 and 450a); Indian Child Welfare Act of 1978 (Pub. L. 95-608, 25 U.S.C. 1901); Title 25 Part 43 Maintenance and Control of Student Records in Bureau Schools; and 42 CFR Part 2, Confidentiality of Substance Use Disorder Patient Records.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No. This system does not derive new data or create previously unavailable data about an individual to be placed in the individual's record through data aggregation.

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes.

☒ No. This system does not derive new data or create previously unavailable data that would make a determination about an individual through data aggregation.

E. How will the new data be verified for relevance and accuracy?

Not Applicable. BHWP is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to the AccuCare electronic health record is limited to BHWP clinical treatment staff and identified care coordinators who have been created in the system as licensed users. Licensed users are assigned access to data on a 'least privilege' principle and 'need to know' to perform official functions; this includes clinical treatment staff access to individually assigned clients only and their respective client records. The Lead Clinician will have access to all client records and data information to ensure clinical quality and appropriate clinical documentation completion per BHWP Policy and Procedure, and applicable federal regulation. BHWP System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. Audit logs for AccuCare can be manually accessed by administrative users via request to Orion Healthcare. Audit logs capture licensed user access and actions performed in the system including licensed username and account creation; licensed user record modification; client record creation; client record modification; disabling or termination of licensed user account access; user logon date and time; number of failed login attempts; and files accessed to ensure information accessed remains within a "need to know" basis to perform only official functions. Access is not provided to any BHWP, BIE, or Tribal governmental office or official who are not considered, or added, as licensed users on the AccuCare platform.

ProtoCall Services uses Active Directory Federation Services (ADFS) to administer access controls and permissions to various systems based upon an employee's position. ProtoCall uses Security Information and Event Management (SIEM) to continually monitor user activity and ProtoCall Services security team is alerted should a user access an unauthorized area. In the event security is alerted that an unauthorized user tried to access the system, an investigation will ensue and ProtoCall will change the user's access in the Active Directory.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

□ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards, or Caller ID)?

□ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The purpose of BHWP and its use of the AccuCare electronic health record and the ProtoCall Services' primary call center application is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within system. More detailed information on AccuCare system audit logs and ProtoCall Services' primary call center application's user audit logs can be found in Section 2, Part I.

□ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The BHWP system is not intended to monitor individuals; however, the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system to prevent unauthorized monitoring.

M. What controls will be used to prevent unauthorized monitoring?

The BHWP can audit usage activity in the AccuCare electronic health record system for all licensed users. Firewalls and network security configurations are also built into the architecture of the system to prevent unauthorized monitoring and access. BHWP System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. BHWP assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

As noted above in Part 4, Section H; ProtoCall Services uses ADFS to administer access controls and permissions to various systems based upon an employee's position. ProtoCall uses SIEM to continually monitor user activity and ProtoCall Services' security team is alerted should a user access an unauthorized area. In the event security is alerted that an unauthorized user tried to access the system, an investigation will ensue, and ProtoCall Services will change the user's access in the Active Directory.

In addition, all users will be required to consent annually to DOI Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training.

The BHWP audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards (AccuCare) (ProtoCall Services)
☐ Key Guards
☒ Locked File Cabinets (AccuCare) (ProtoCall Services)
☒ Secured Facility (AccuCare) (ProtoCall Services)
☒ Closed Circuit Television (AccuCare) (ProtoCall Services)
☐ Cipher Locks
☒ Identification Badges (AccuCare) (ProtoCall Services)
☐ Safes
☐ Combination Locks
☒ Locked Offices (AccuCare) (ProtoCall Services)
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password (AccuCare) (ProtoCall Services)
☒ Firewall (AccuCare) (ProtoCall Services)
☒ Encryption (AccuCare) (ProtoCall Services)
☒ User Identification (AccuCare) (ProtoCall Services)
☐ Biometrics
☒ Intrusion Detection System (IDS) (AccuCare) (ProtoCall Services)
☒ Virtual Private Network (VPN) (AccuCare) (ProtoCall Services)
☒ Public Key Infrastructure (PKI) Certificates (AccuCare) (ProtoCall Services)
☐ Personal Identity Verification (PIV) Card
☒ Other. ProtoCall Services is HiTRUST Certified. ProtoCall Services is also compliant with the MARS-E 2.0 framework which includes validation that certain NIST 800-53 security controls are in place and in accordance with the Center for Medicaid Services (CMS) guidance. ProtoCall's detailed call documentation is provided through a secure, HITRUST Certified, HIPAA Compliant platform, and the MARS-E 2.0 framework, which addresses the mandates of the Patient Protection and Affordable Care Act of 2010 and the Department of Health and Human Services. Orion Healthcare Technology hosts the AccuCare electronic health record system directly with Microsoft Azure provided through a secure, HITRUST

Certified platform and the Cyber Essentials Plus (audited version of the Cyber Essentials information security standard) which provides assurance that key information security controls are in place within an organization.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits (AccuCare) (ProtoCall Services)
☒ Backups Secured Off-site (AccuCare) (ProtoCall Services)
☒ Rules of Behavior (AccuCare) (ProtoCall Services)
☒ Role-Based Training (AccuCare) (ProtoCall Services)
☒ Regular Monitoring of Users' Security Practices (AccuCare) (ProtoCall Services)
☒ Methods to Ensure Only Authorized Personnel Have Access to PII (AccuCare) (ProtoCall Services)
☒ Encryption of Backups Containing Sensitive Data (AccuCare) (ProtoCall Services)
☒ Mandatory Security, Privacy and Records Management Training (AccuCare) (ProtoCall Services)
☒ Other.

- ProtoCall Services Privacy Officer and Security Officer are responsible for ensuring all ProtoCall Services staff, processes and systems are HIPAA compliant. The following are steps taken to ensure compliance:
- All ProtoCall Services employees are required to sign a confidentiality agreement upon hire that includes HIPAA compliance information.
- All ProtoCall Services employees are required to successfully complete a HIPAA-training within 30 days of hire and annually thereafter, employees receive additional annual internal training and quarterly refresher emails.
- ProtoCall Services' Security and Privacy Officer contact information is on the front page of our Employee Portal.
- All ProtoCall Services' employees have a mechanism to immediately and readily report suspected privacy or security concerns. Suspected concerns may be immediately escalated to our Administrative on-call 24/7/365 for consultation, otherwise they are reviewed within 48 business hours by the Privacy Officer.
- All ProtoCall Services' facilities require access by an issued keycard which has the employee's photo adhered to it, and employees are required to always wear their keycard.
- All visitors are required to sign a confidentiality agreement and are issued a keycard to wear at all times. Visitors needing to access systems that contain PHI are not left alone during that process.
- Paper containing PHI is kept to a minimum, however, if paper PHI needs to be stored it is within a locked office within lockable file drawers accessible only by authorized staff.
- All ProtoCall Services' facilities are outfitted with shredders and/or a locked repository for items to be shredded by our shredding vendor.
- All ProtoCall Services' call takers must use the hosted Data Center environment to access our call-handling software. Remote workers must use two-factor authentication to access the data center.

- All remote ProtoCall Services' employees are required to sign a Remote Worker Agreement to which they must adhere to specific, Home Office requirements.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The BIE Deputy Associate Chief Information Officer serves as is the Information System Owner. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in BHWP. The ISO and the Privacy Act system managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the IA Associate Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The BHWP ISO and ISSO are responsible for the daily oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The BHWP ISO, ISSO, and bureau and office system administrators are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within one hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the IA Associate Privacy Officer and DOI Privacy Officials. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.