Privacy Impact Assessment for the VA IT System called:

Blackboard Learn

Veterans Health Administration

Office of Connected Care Telehealth

Date PIA submitted for review:

10/25/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.lahl@va.gov	(202) 461-7330
Information System Security Officer (ISSO)	Anupam Anand	Anupam.anand@va.gov	215-823-5800ext:5159
Information System Owner	Aimee Barton	Aimee.Barton@va.gov	(202)-461-9005

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

Blackboard is a SaaS solution hosted external to the VAEC. This system provides web-based E-Learning Platform that integrates with the VA Enterprise Learning Management System (LMS), Talent Management System (TMS), and provides 24/7 access to an integrated mix of VA-developed synchronous and asynchronous learning activities in combination with dynamic opportunities for collaboration with experts and peers. These requirements may necessitate platform customization and enhancement, which shall be the responsibility of the Contractor. Should the VA Enterprise LMS change or be updated throughout the period of performance of this effort, the Contractor will support integration with the new LMS based on the integration requirements the specific of the new LMS platform.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

IT System name -Blackboard Learn. Program Office- Office of Connected Care Telehealth

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

The Blackboard Learn (Connected Care Academy (CCA)) E-Learning Platform is an electronic education platform, content, and course management system used and supported by Connected Care Telehealth to deliver courses and forums to VA and non-VA employees involved with Connected Care Telehealth modalities. It hosts forums for greater accessibility and distribution, as well as tracks attendance. The Blackboard Learn (Connected Care Academy (CCA)) E-Learning Platform contains electronic data of all users, activities, training evaluations, and other quality measures used to evaluate training effectiveness and utilization. The Blackboard Learn (CCA) E-Learning Platform can be used as a communication networking solution. The Blackboard Learn (CCA) E-Learning Platform is also a Knowledge Management System containing Connected Care Telehealth resources, guidance, and other documents for providing virtual care. It is formally linked to the VA Talent Management System (TMS) to ensure access, as TMS is the official location of training records, according to VHA Directive 0003.

C. Indicate the ownership or control of the IT system or project.

VA Controlled/ non- VA Owned and Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

Approximately 300,000 unique user accounts ("staff" is defined as:1) Telehealth Health Care Professionals who provide care using video telehealth technologies, 2) Clinical personnel supporting video visits at the point of care, 3) Any personnel virtually joining the video visit, 4) Any personnel listed on the Facility Emergency Contact List and as the point of contact in Virtual Care Manager.)

E. A general description of the information in the IT system and the purpose for collecting this information.

Name, email address, TMS Person ID, VISN, Facility and Job Title are exchanged with TMS to ensure correct integration of training results to the correct individuals.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

VA Talent Management System

The VA TMS will send a shared secret key as part of a Blackboard content launch that will allow a user to click a course link in the TMS and be taken directly to the Blackboard Learning Platform without being prompted for a blackboard user ID and Password. This functionality uses the Blackboard Auto Sign-On Building Block. All communication between VA TMS and Blackboard during content launch will use the HTTPS protocol over TLS utilizing TCP on Port 443.

The VA TMS (Success Factors HCM Suite) will send user profile data to Blackboard via a text file interface. Extracted data will be formatted into pipe-delimited text files and placed in a designated folder on an NS2-SFTP Server. All access to the SFTP server is controlled by authentication methods to validate the approved users. Data that is uploaded or downloaded from the SFTP server will use the SSH File Transfer Protocol to protect the data in transit utilizing TCP on Port 22.

Training completion records are transmitted via a Secure Web Service setup for immediate recording in the user TMS Learning History records.

**Excerpt from Blackboard Learn MOU/ISA*

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

Blackboard Learn is a subsystem of (TMS)

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

Privacy Act of 1974, 5 U. S. C. § 552a, as amended

76VA05 General Personnel Records (Title38)-VA; AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.
OPM/GOVT-1 General Personnel Records: Authority for Maintenance of the System: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The system is not being modified, therefore, no amendment or revision is required for the SORN.

According to 76VA05 above, Policies and Practices for storing, retrieving, accessing, retaining, and disposing of records in the system section on Storage states "These records may be maintained in file folders, on lists and forms, on microfilm or microfiche, and in computer processable storage media."

Under the Safeguards section, "Access to computerized records is limited through the use of access codes and entry logs.Additional protections is provided by electronic locking devices, alarm systems, and guard services."

"Electronic data is made available to VA field facilities via VA's Intranet. Strict control measures are enforced to ensure that disclosure is limited to the individual to whom the record is being maintained or on a "need to know" basis. Security devices (e.g., passwords, firewalls) are used to control access by VA users to Internet services, and to shield VA networks and systems from outside the firewall."

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*

There will be no changes

K. *Whether the completion of this PIA could potentially result in technology changes*

There will be no changes

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Organizational Email Address, VISN, Facility, TMS Unique Identifier

PII Mapping of Components (Servers/Database)

Blackboard Learn consists of one key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Blackboard Learn and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Single Sign On (Internal)	**Yes**	**Yes**	TMS person ID, first name, last name, email	**To authenticate user.**	**SAML-HTTP**

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Blackboard Learn collects and exchanges information with the Identity and Access Management office through Single-Sign-on (internal) for user authentication information (TMS Person ID, First Name, Last Name, and Email) through a SAML-HTTP protocol for transmission. Blackboard Learn also collects and exchanges information with the VA Talent Management System (TMS) through the Single-Sing-on (internal) process to exchange the same data elements as with Identity and Access Management through the same SAMP-HTTP protocol.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.
Purpose for Data Transfer: Facilitates the creation of user accounts, single sign on launch of content and the recording of course completions.

VA-owned data transmitted to Blackboard via the system infrastructure is hosted within AWS GovCloud US-West Region.

Blackboard has been PIV-enabled by accepting HSPD-12 PIV credentials, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns. Blackboard applications and systems are compliant with VA Identity Management Policy(VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document). Blackboard ensures all Blackboard delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion-based authentication, and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI)based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC)for internal VA customers and includes assertion-based authentication using a SAML implementation. Additional assertion implementations, besides the required SAML assertion using a multifactor authentication method with a one-time passcode, has been provided for external (VA Partners, Academic Affiliates, other Federal Agencies)and administrative users and is compliant with NIST 800-63 guidelines. The Blackboard solution conforms to the specific Identity and Access Management PIV requirements as set forth in Enabling Mission Delivery through Improved Identity, Credential, and Access Management – M19-17, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2 and supporting NIST Special Publications.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This is a subsystem of (TMS)
Blackboard Learn does record a score for post tests, and also raw data is analyzed regarding responses to questions and surveys to provide reports to leadership. These reports and analysis are retained and Blackboard Learn is recorded as the source of information both within Blackboard Learn and TMS.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Excerpt from Signed Blackboard Learn Access Control Policy and Procedures, dated October 4, 2021, Version 2.0

Blackboard has been PIV-enabled by accepting HSPD-12 PIV credentials, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns. Blackboard applications and systems are compliant with VA Identity Management Policy(VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document). Blackboard ensures all Blackboard delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion-based authentication, and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI)based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC)for internal VA customers and includes assertion-based authentication using a SAML implementation. Additional assertion implementations, besides the required SAML assertion using a multifactor authentication method with a one-time passcode, has been provided for external (VA Partners, Academic Affiliates, other Federal Agencies)and administrative users and is compliant with NIST 800-63 guidelines. The Blackboard solution conforms to the specific Identity and Access Management PIV requirements as set forth in Enabling Mission Delivery through Improved Identity, Credential, and Access Management – M19-17, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2 and supporting NIST Special Publications.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

Information is collected electronically and is not collected on a form.

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Users log into TMS and will also use their PIV card. Accuracy of this information is responsibility on Identity access management.
External Users have a way to validate prior to acceptance of validation of information.

Information in this system of records is provided by the individual employee, examining physicians, educational institutions, VA officials, and other individuals or entities. Individuals are notified when information is added to their file and are encouraged to review the documents.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

System doesn't have a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Privacy Act of 1974, 5 U. S. C. § 552a,
.

76VA05 General Personnel Records (Title38); AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.
OPM/GOVT-1 General Personnel Records: Authority for Maintenance of the System: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 1210

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:
The system collects, processes, and retains PII from employees. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted and adverse negative effect to the VA.

Mitigation:
Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

Name – For user authentication information
Organizational Email Address- For user authentication information
VISN- For user authentication information
Facility- For user authentication information
TMS Unique Identifier- For user authentication information

2.2 What types of tools are used to analyze data and what type of data may be produced?

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Blackboard Learn contains data from which an administrative user may retrieve for analysis of system usage, scoring for user knowledge and competency, reporting for OIG, Congressional requests, VHA Leadership requests, etc., and other analytical data such as trends and patterns of usage. The Office of Connected Care Telehealth Services uses this data to improve the training experience, provide up-to-date guidance resources and analysis of usage to VHA Leadership, Office of Inspector General requests, Departmental Secretary requests, and Congressional Requests.
The Data is provided in multiple formats dependent upon the request. Generally individually identifiable information is not included in the summary formats via Dashboards and briefs to these agencies.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Blackboard updates system based on what is in TMS records. Blackboard is not creating any new information.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
**Excerpt from signed Blackboard Learn System and Communications Protection Policy and Procedures, dated August 23, 2021, Version 2.0*
System and communications protection provides users with a level of assurance that Blackboard information is protected by controls to prevent unauthorized users from interfering with authorized communications and from accessing information that resides on, or is transmitted from, Blackboard systems. Blackboard policy is to:

- Monitor, control, and protect communications (information transmitted or received by information systems).
- Employ its information systems to transmit information in the most secure manner possible commensurate with the risk and magnitude of harm that could result from unauthorized transmission or receipt of information or from interference with system communications. Manners of securing the transmission of information include the use of trusted pate,

cryptographic key, data encryption, session encryption, and public key infrastructure (PKI), among other methods.

- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within its information systems.
- Employ methods to protect its information systems from denial of service (DOS) attacks.
- Provide mechanisms to protect the authenticity of communications sessions conducted on its information system.

Excerpt from the Blackboard Learn MOU/ISA ID 2274

The security of VA sensitive information (see Appendix B of the MOU/ISA for definition of sensitive information) being transmitted, processed or stored over any system and interconnection in support of this agreement must be FIPS 140-2 (or successor) compliant. The FIPS 140-2 compliance is not required if no VA sensitive data is transmitted.
The FIPS 140-2 certificate number of Blackboard's gateway cryptographic module for establishing the Virtual Private Network (VPN) tunnel is FIPS# 3617 KMS, 3739 Nitro. FIPS Compliance will be validate by Veterans Health Administration.
The connections at each end must be located within controlled access facilities using physical access control devices and/or guards. Individual users will not have access to the data except through the system security software inherent to the operating system. Access is controlled by authentication methods to validate the approved users.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

Social Security Numbers are not collected, processed, or retained in the Blackboard Learn System.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

**Excerpt from signed Blackboard Learn System and Communications Protection Policy and Procedures, dated August 23, 2021, Version 2.0*
Protect the confidentiality AND integrity of transmitted information by using SSH. Transmissions between VA and Blackboard components are verified on several levels to insure a higher level of integrity. On the very lowest level, VA hardware and networking, routers and switches have mechanisms for checking packet and transmission integrity. On another level, the vendor software application is inherently guaranteed to be delivered by design of the messaging server. When a server receives a message it persists it to the database to make sure that it will not be lost, then sends it to the destination and ensures that it is delivered via a confirmation. A different level of checking transmission integrity is handled by the logic and coding standard of the application, making sure communication and data are as expected. Also refer to VA Handbook 6517 Risk Management Framework for Cloud Computing Service.
Implement cryptographic mechanisms to prevent unauthorized disclosure of information AND detect changes to information during transmission unless otherwise protected by a hardened or alarmed carrier Protective Distribution System (PDS). VA information systems protect the integrity of transmitted information. Blackboard uses strong cryptography and encryption techniques (such as SSL, TLS, and/or IPSEC) to safeguard confidential data during transmission over public networks, in accordance with FIPS 140-2 certified encryption module(s).

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

*Excerpt from Signed Blackboard Learn Access Control Policy and Procedures, dated October 4, 2021, Version 2.0
This document establishes uniform policies, authorities, responsibilities, and compliance for access Control for Blackboard. It also provides the essential services of identification and authentication, authorization, and accountability where identification and authentication determine who can log on to an information system. Authorization determines what an authenticated user can do, and accountability identifies what a user did.
Protecting access to the Blackboard information and information systems is vital to the security of its data and mission. Access controls authorize Blackboard users to perform a defined set of actions on a specific set of resources. It is Blackboard policy to control access to information systems:

- Restricting physical access to Blackboard and Government desktop and laptop computers, servers and other communications and networking infrastructure, and portable and mobile devices to authorized users.
- Restricting Blackboard user access through separation of duties, least privilege, session lock, and session termination.
- Reviewing access controls by monitoring audit records (e.g., activity logs) to verify that only authorized and business-related activities are taking place on Blackboard information systems.
- Establishing and enforcing policies on accessing Blackboard systems locally and remotely for Blackboard users.
- Establishing and enforcing policies restricting or prohibiting all access for non-Blackboard users.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, documented in Blackboard Learn Access Control Policy and Procedures, dated October 4, 2021, Version 2.0

2.4c Does access require manager approval?

Access to Blackboard Learn for a Learner does not require manager approval but must follow VA guidelines for employees who will access through VA TMS.
Elevated privileges for access to Blackboard Learn must be approved, granted, and monitored by the VHA Office of Connected Care Telehealth Services Blackboard Learn System Administrators

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes, documented in Blackboard Learn Access Control Policy and Procedures, dated October 4, 2021, Version 2.0

2.4e Who is responsible for assuring safeguards for the PII?

Documented in Blackboard Learn Access Control Policy and Procedures, dated October 4, 2021, Version 2.0
Refer to the Procedures in 2.4a. Individuals identified in the Blackboard Learn Access Control Policy and Procedures responsible for assuring safeguards include the Information System Security Officer, Information System Owner, System Administrator, Network Engineer, and VHA Office of Connected Care Telehealth Services Blackboard Learn System Administrators

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Email, VISN, Facility, Job Title, TMS Unique Identifier

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a***

different retention period than medical records or education records held within your system, please be sure to list each of these retention periods*. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Will follow the NARA approved retention length and schedule.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, all system of records indicated are on an approved disoperation.

3.3b Please indicate each records retention schedule, series, and disposition authority.

VHA RCS 10-1 Section 1006.13. Personally identifiable information extracts. System-generated or hardcopy printouts generated for business purposes that contain Personally Identifiable Information. Temporary; destroy when 90 days old or no longer needed pursuant to a supervisory authorization, whichever is appropriate.

VHA RCS 10-1Section 1006.14. Personally identifiable information extract logs. Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days and anticipated disposition date. Temporary: destroy when business use ceases. (GRS 4.2 item 140, DAA-GRS-2013-0007-0013)

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

**** Excerpt from Blackboard Learn MOU/ISA ID 2274***

Provisions for Destruction or Return of the Data (if applicable): Blackboard and AWS leverage secure wipe/media sanitization procedures aligned with NIST 800-88 guidelines. Upon request or contract termination, data is permanently deleted from the active system as well as backups using native AWS tools. This may include erasing client database instances, S3 volumes, and content in shared storage. Data is typically deleted within 30 days of termination. All backups are live and remain within the AWS network.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

All IT system and application development and deployment is handled by VA OIT and authorized contracting staff. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified application(s). Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. Where feasible, Veterans Affairs will use techniques to minimize the risk to privacy of using PII for research, testing and training.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a potential privacy risk that records within the system will be improperly retained or disposed.

Mitigation: Blackboard Learn (Connected Care Academy (CCA)) E-Learning Platform strictly adheres to the Records Management Schedule to ensure that no records are maintained longer than necessary. To mitigate this risk, Blackboard Learn (Connected Care Academy (CCA)) E-Learning Platform will coordinate with the VA records officer to ensure that the proposed schedule is accurate.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Identity and Access Management	For authentication purpose	User authentication information (TMS person ID, first name, last name, ema	SAML -HTTP
VA Talent Management System (TMS)	For authentication and employee training records and retention.	User authentication information (TMS person ID, first name, last name, ema	SAML -HTTP

Blackboard Learn collects and exchanges information with the Identity and Access Management office through Single-Sign-on (internal) for user authentication information (TMS Person ID, First Name, Last Name, and Email) through a SAML-HTTP protocol for transmission. Blackboard Learn also collects and exchanges information with the VA Talent Management System (TMS) through the Single-Sing-on (internal) process to exchange the same data elements as with Identity and Access Management through the same SAMP-HTTP protocol.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The internal sharing of data is necessary for individuals to receive VHA benefits, however, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

.This Privacy Impact Assessment (PIA) serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the

website of the agency, publication in the Federal Register, or other means." A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed. The SORN also contains notice of the collection of this information.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice

76VA05 General Personnel Records (Title38)-VA;
OPM/GOVT-1 General Personnel Records: Authority for Maintenance of the System:

.

.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Notice is provided in this PIA and the SORN
The following notice is presented to the users through the login process:

> This U.S government system is intended to be used by [authorized VA network users] for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.
>
> Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

Privacy Policy language is being reviewed to further define policy specific to the information within Blackboard and how the information may be used.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

The personnel records in these files are the official repository of the records, reports of personnel actions and the documents and papers associated with these actions. The personnel action reports and other documents give legal force and effect to personnel transactions and establish employee rights and benefits under pertinent laws and regulations governing Federal employment. They provide the basic source of factual data about a person's Federal employment while in the service and after his or her separation. Records in this system have various uses, including screening qualifications of employees; determining status, eligibility, and rights and benefits under pertinent laws and regulations governing Federal employment; computing length of service; and other information needed to provide personnel services

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Information is used in accordance with employment needs however, since it is maintained in a privacy act system of records, individuals have the right to consent to additional uses in accordance with the Privacy Act.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

> **Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals wishing to access their records should contact the appropriate office as follows: a. Federal employees should contact the responsible official (as designated by their agency) regarding records in this system. b. Former Federal employees should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118, regarding the records in this system. Individuals must furnish the following information so their records can be located and identified: full name(s), date of birth, Social Security number, last employing agency (including duty station, when applicable), and approximate dates of employment. All requests must be signed

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

N/A

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Current and former VA employees wishing to request amendment of their records should contact the Director, Department of Veterans Affairs Shared Service Center (00), 3401 SW 21st Street, Topeka, Kansas 66604. Individuals must furnish the following information for their records to be located and identified: Full name(s), date of birth, Social Security number, and signature. To facilitate identification of records, former employees must also provide the name of their last Department of Veterans Affairs facility and approximate dates of employment

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The procedures are specified in the System of Records Notice.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The individual has the ability to see their personal information directly in the system after secure login protocols are used by selecting the drop-down arrow beside their name and selecting the option for personal information. There are limitations for changes that are permitted by individual users. The Connected Care Academy Help Desk is the mechanism through which an individual may request corrections or amendments to their individual records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals***

involved might change their behavior. *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The individual has the ability to see their personal information directly in the system after secure login protocols are used by selecting the drop-down arrow beside their name and selecting the option for personal information. There are limitations for changes that are permitted by individual users. The Connected Care Academy Help Desk is the mechanism through which an individual may request corrections or amendments to their individual records.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

See Blackboard Learn MOU/ISA ID 2274, section 3.2.11 Security Parameters
User access system via TMS

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

The minimum requirements for employees to work in support of this interconnection, to include background investigations and security clearances, will be determined by the contract(s) or requirements governing the support services provided by the vendor. Blackboard will be responsible

for ensuring that their employees meet the standards set forth in all applicable contracts or requirements and for continuously monitoring and tracking the status of all Blackboard employees relevant to this interconnection.
Veterans Health Administration employees, TMS Learning users, VA and non-VA contracted employees involved with Connected Care Telehealth modalities.
The VHA Office of Connected Care Telehealth Services is responsible for establishing the criteria for what PII can be shared and follows all VA directives, policies, and procedures and all applicable laws for determining sharing of PII.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Users are classified in several categories and permissions are set for the level of access based on the category:

- Guests are have permission restrictions set to read-only specific information and do not have the ability to access any personal identifiable information.
- Learners have the ability to access content, but only see their own identification information
- Instructors create course content and resource materials and have ability to read and enroll users based on their information within the system (username, first name, last name, and email address.)
- Evaluators who have the ability to generate reposts and evaluate the statistical data from the reports.
- Administrative personnel who have the ability to read, write, and modify the information.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contractors do have access to the system and PII. The Blackboard contract staff provide troubleshooting and assistance with any issues that cannot be resolved at the VA System Administrator level. Other contractors work with the creation and maintenance of the training materials and resources within the system allowing them to have access to PII. Contractors are required to provide validation of required Privacy and Security Risk Assessment training with Rules of Behavior and HIPPA privacy training. Their access is monitored and controlled based on their role with the office.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

VA Privacy Controls and HIPPA Training are required. These are required annually per VA policy This is covered by the signed Blackboard Learn Awareness and Training Policy and Procedures, dated October 4, 2021, Version 2.0 filed with the Authority to Operate.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:
This information is found on the FedRAMP site for Blackboard Learn

1. *The Security Plan Status:* Approved by FedRAMP as a moderate complexity system.
1. *The System Security Plan Status Date:* Version 2.3 dated July 8, 2022
2. *The Authorization Status:* Approved Authorization to Operate (Both E-Authorization (150943) and F-Authorization(150707))
3. *The Authorization Date:* 27 January 2022
4. *The Authorization Termination Date:* 11 January 2025
5. *The Risk Review Completion Date:* July 16, 2020
6. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Excerpt from the FedRAMP Blackboard Learn Saas A10 FIPS 199.docx located on MAX.gov under the system documentation. The Blackboard Learn system has been determined to have a security categorization of Low (L).

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include:

Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MbaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

This is a System as a Service (SaaS). Amazon AWS GovCloud U.S.West Region

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

MOU/ISA ID number 2274
Contract number is NNG15SD19B
Order number is 36C10A20F0278

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

Blackboard Learn does not hold significant details about accounts of cloud consumers.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

A Contract is in place with the vendors and VA. Please direct all contract related questions to Rhonda Johnston (Rhonda.Johnston@va.gov) and or Harold Bonds (Harold.Bonds@va.gov)

Excerpt from the Memorandum of Understanding and Interconnection Security Agreement Between Veterans Health Administration and Blackboard, Section 3.2.9 through 3.2.11
Policies that govern the protection of the information/data for Veterans Health Administration include but are not limited to VA Directive and Handbook 6500 (or successors). Policies that govern the protection of the information/data for Blackboard Learn SaaS include but are not limited to the System and Information Integrity Policy, Version 2.0. All documents are available upon request.

Both parties are responsible for auditing application processes and user activities involving the interconnection with enough granularity to allow successful investigation of any breaches and security incidents. Activities that will be recorded include event type, date and time of event, user identification, workstation information, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for a minimum of one (1) year. Audit logs which describe a security breach must be maintained for six (6) years. Those responsible for maintaining audit logs must ensure that audit logs are successfully stored for the required duration.

The following detailed security measures and controls implemented by each organization to protect the confidentiality, integrity, and availability of the connected systems and the information that will pass between them are outlined below:

Veterans Health Administration implements the following security measures and controls:

- Identification and Authentication – User access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. VA utilized "two-factor authentication" for general users. A separate token and non-mail enabled account is required for users who require elevated privileges on IT systems.
- Logical Access Controls – VA accounts are separated into domains and the system administrators only manage those accounts within their domain. Accounts are audited every ninety (90) days. VA policy requires account termination within twenty-four (24) hours of an employee/contractor departure. Accounts are terminated immediately in the event of a hostile termination.
- Physical and Environmental Security – Physical and environmental controls are maintained at VA facilities. *{Authorization is tightly controlled for any physical or environmental facilities.}*
- Firewall, IDS, ad Encryption – Intrusion detection systems (IDS) are in place at gateways and throughout the VA network. The VA's Cybersecurity Operations Center monitors the VA network 24X7. Suspicious activity is reviewed and determined recommendations are formulated and assigned to the system administrators. FIPS 140-2 validated encryption is required for transmission of sensitive information.

Blackboard implements the follow security measures and controls:

- Identification and Authentication – Three user authentication methods are utilized in the Blackboard Learn platform today. 1) Local username/password-based authentication with all authentication actions contained entirely within the Blackboard Learn application. 2) HTTPS MAC-based single sign-on form the VA's TMS to Blackboard Learn SaaS. This authentication mechanism leverages a trust between TMS and Blackboard Learn and only authenticates standard, low privilege end-user/learners. Users must first authenticate with TMS to access this Blackboard Learn authentication mechanism. 3) Security Assertion Markup Language (SAML)-based authentication via VA's SSOi infrastructure and Blackboard's SAML authentication provider. This authentication process is only available to users authenticated via VA.
- Logical Access Controls – Blackboard has developed a formal user request form, as stipulated in the Access Control Policies and Procedures. This form outlines the process for granting logical access to Blackboard Learn SaaS components. Each completed request form must be based on a business need and is limited to ony the access requirements for that individual to perform his/her identified role within the Blackboard Learn SaaS. Once a user's access is approved, the Blackboard Learn SaaS Development and Operations (DevOps) team places the user in a Captain role per the respective environments they require access to and provides the user with OKTA credentials. OKTA ensures all privileged users are authenticating via multi-factor authentication (MFA). AWS Identity Access Management (IAM) accounts are integrated with OKTA.
- Physical and Environmental Security – Blackboard fully inherits the control from AWS as the system has no physical components managed by Blackboard. All environmental and physical access controls are managed and inherited from AWS GovCloud.
- Firewall, IDS, and Encryption – Blackboard Learn SaaS monitors the information system by employing a number of automated mechanisms, such as Amazon CloudWatch, CloudTrail, CloudWatch Logs, Virtual Private Cloud (VPC) Flow Logs, Logstash, and Crowdstrike. These logs are forwarded to AWS S3 and then any security-relevant logs are ingested by Splunk for further analysis and review. Blackboard security operations center (SOC) to continuously monitor these logs for malicious activity.
    - Blackboard has implemented internal management interfaces of the boundary at the following levels:
        - AWS Elastic Load Balancer: AWS Load Balancers provide dedicated HTTPS management interfaces for Blackboard Learn SaaS
        - AWS EC2 and VPC Security Groups
    - Blackboard Learn SaaS VPCs are configured into four separate logical divisions
    - Management
        - Security
        - Customer
        - Virtual Security Operations Center (VSOC)
        - Security groups within VPC separate via IP address, IP address subsets, and Ports
    - AWS Security Groups have been configured to employ various rules. Each of these activities are logged within S3 and forwarded over to Splunk for review/analysis.

- AWS Ubuntu Virtual Machine (VM) Management: SSH access is configured on the jumphost as an external management port. SSH is used on the jumphost to connect to Ubuntu server VMs. Blackbaord Staff using SSH must be on the corporate network to connect to the Blackboard Learn SaaS environment.
- Amazon Management Console: The management console uses a separate management-band interface over HTTPS using TLS
- Blackboard Learn SaaS uses public and private subsets to separate from publicly accessible systems
- All inbound incoming traffic is protected using Security Groups and Network Access Control Lists (NACLs) in AWS. Blackboard operates on a deny-all, permit-by-exception policy. Blackboard only allows communication via Blackboard-approved ports and protocols.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

Blackboard Learn does not use Robotics Process Automation (RPA)

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access

ID	Privacy Controls
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2023.01.12 15:48:07 -05'00'

Privacy Officer, Dennis Lahl

Anupam Anand 404738 Digitally signed by Anupam Anand 404738
Date: 2023.01.13 11:02:20 -05'00'

Information System Security Officer, Anupam Anand

AIMEE BARTON Digitally signed by AIMEE BARTON
Date: 2023.01.17 16:34:42 -05'00'

Information System Owner, Aimee Barton

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

76VA05 General Personnel Records (Title38)-VA; AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a), 7304, 7406(c)(1), and 7802.

OPM/GOVT-1 General Personnel Records: Authority for Maintenance of the System: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 1210

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices