Privacy Impact Assessment for the VA IT System called:

Blackboard Learn - Enterprise

Veterans Health Administration

VHA Digital Health Office, Office of Connected Care Telehealth

eMASS ID# 1363

Date PIA submitted for review:

January 10, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Anupam Anand	Anupam.Anand@va.gov	215-823-5800 ext. 5159
Information System Owner	Aimee Barton	Aimee.Barton@va.gov	216-707-7726

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Blackboard Learn – Enterprise (Blackboard-e) is a Software as a Service (SaaS) solution that offers government and military agencies next-generation online, social and mobile tools that create a continuous learning environment, built around peer-to-peer interaction, content and discussions. For the VA it provides a web-based E-Learning Platform that integrates with the VA 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. The system infrastructure is hosted within the Amazon Web Services (AWS) GovCloud Infrastructure as a Service (IaaS) 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. What is the IT system name and the name of the program office that owns the IT system?
IT System name – Blackboard Learn - Enterprise (Blackboard-e)
Program Office – VHA Digital Health Office, Office of Connected Care Telehealth

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
The Blackboard-e also known as Connected Care Academy (CCA) is an electronic education platform (e-learning platform) that provides its users with a virtual classroom that replaces the need for traditional brick and mortar classrooms for VA and non-VA employees involved in Connected Care Telehealth services. Blackboard-e offers several core capabilities, with the cornerstones being the ability to: create courses, post and grade course assignments; prevent plagiarism; and manage and deliver course assessments. It also contains electronic data of all users, activities, training evaluations, and other quality measures used to evaluate training effectiveness and utilization.

C. Who is the owner or control of the IT system or project?
VA Controlled/non-VA Owned and Operated

2. Information Collection and Sharing

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

Expected number of users are approximately 350,000.
Users consists of : 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, and 5) Users from external agencies and organizations, such as Department of Defense, University of Florida, State Veterans Homes, American College of Physicians.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

Specific data elements collected are: Name, email address, TMS unique identifier, VISN, Facility, Job Title, Personal email address in the business Fax number field if VA employee wishes to access the system outside the VA Network, preferred pronoun and nick name

This information collected to uniquely identify the individual for authentication purposes and to update the training records in the TMS as well as additional information is collected for analysis of system usage, scoring for user knowledge and competency, reporting for Office of Inspector General (OIG), Congressional requests, VHA Leadership requests, and other analytical data such as trends and patterns of usage.

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

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

G. Is 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?

No, system only operates in one site.

3. Legal Authority and SORN

H. What is the 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 (Title 38)-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?

No. The system is not being modified; therefore, no amendment or revision is required for the SORN. The SORN covers cloud usage and storage.

4. System Changes

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

No. Completing this PIA will not result in changes to business process.

K. Will the completion of this PIA could potentially result in technology changes?

No. Completing this PIA will not result in technology 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.

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[1]
- ☐ 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)

Other PII/PHI data elements: Organizational Email Address, VISN, Facility, TMS Unique Identifier, Job title, Preferred pronoun, Nick name and Personal email address in the business Fax number field if VA employee wishes to access the system outside the VA Network

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

PII Mapping of Components (Servers/Database)

Blackboard-e consists of one database components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Blackboard-e and the reasons for the collection of the PII are in the table below.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
RDS Database	Yes	Yes	First and last name, VA or organizational Email address or Personal Email address, VISN Facility, TMS Unique Identifier, Preferred pronoun, Nick name, Business fax number and Personal email address in the business Fax number field if VA employee wishes to access the system outside the VA Network	To uniquely identify the individual for authentication purposes and to update the training records in the TMS as well as additional information is collected for analysis of system usage, scoring for user knowledge and competency, reporting for Office of Inspector General (OIG), Congressional requests, VHA Leadership requests, and other	Data at rest and in transit encrypted with FIPS 140-2 compatible encryption methods

				analytical data such as trends and patterns of usage.	

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?

Information is collected directly from the individual at the registration to Connected Care Academy. No commercial data aggregators are used.

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.

Information is collected directly from the individual. No commercial data aggregators are used.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Blackboard-e record post tests scores for individual course completion. Raw data as a whole is analyzed for system usage, scoring for user knowledge and competency, reporting for Office of Inspector General (OIG), Congressional requests, VHA Leadership requests, and other analytical data such as trends and patterns of usage.

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?
Information is collected directly from the individual at the registration to Connected Care Academy.

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

Information 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.

Organizational users log into the system using their PIV card. Accuracy of this information is verified Identity and Access Management.
External users inputs are not validated. However, account managers manually validate user information every 3 months.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No. System does not utilize commercial aggregator to validate the accuracy of the 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, as amended.
76VA05 General Personnel Records (Title 38); 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 Order 9397, as amended by 13478, 9830, and 12107.

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 and general public who are supporting VA telehealth programs. If this information is breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted.

Mitigation: Data collected, processed, and retained is 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 that 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.

PII/PHI Data Element	Internal Use	External Use
User First Name and Last Name	For User Authentication	For User Authentication
VA Email Address (for organizational users)	For User Authentication	Not used
Personal Email Address (for organizational users)	If VA employee wishes to access the system outside the VA Network	For User Authentication

Personal or organizational Email Address (for non-organizational users)	For User Authentication and for VA Staff to access the system external to VA Network.	For User Authentication
VISN	For report generation	Not used
Facility	For report generation	Not used
TMS Unique Identifier (Person ID)	To ensure correct integration of training results to the correct individuals.	Not used
Business Fax Number	VA Staff to access the system external to VA Network.	Not used
Preferred Pronoun	Not used	Not used
Nick name	Not used	Not used

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-e administrator may retrieve raw data for analysis of system usage, scoring for user knowledge and competency, reporting for Office of Inspector General (OIG), Congressional requests, VHA Leadership requests, and other analytical data such as trends and patterns of usage. The VA office of Connected Care Telehealth Services uses this data to improve training experience, provide up-to-date guidance resources, and analysis of usage to VHA Leadership, OIG requests, Departmental Secretary requests, and Congressional Requests. The data is provided in multiple formats dependent upon request. Generally, individually identifiable information are not included in the summary in these reports unless specifically requested.

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 individual records within the system based on what is contained or changed in TMS records. Blackboard-e is not creating any new individual records for the learners. New records are created for the users with elevated privileges.

Blackboard-e only report training completion data and no adverse action will be taken against the users. However, systems administrators are required to complete the designated trainings in order to retain admin access to the system.

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?
Data at rest and in transit encrypted with FIPS 140-2 compatible encryption methods according to VA Handbook 6500.

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-e.

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

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?

Only users with elevated privileges have access to PII after completing admin user trainings and after signing non-disclosure agreement. In order to create an admin account, admin user need to create a ticket using a Blackboard User Request portal designated only for Blackboard admin users. Once ticket is submitted, system administrators review the request, analyses and validate the need-to-know basis, allocate different privileges to the account and approve the request. Quarterly reviews on elevated privileges users are conducted to validate the need for continued access by the system administrators.

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

Yes, documented in Blackboard-e Access Control Policy and Procedures, dated November 14, 2023, Version 3.0

2.4c Does access require manager approval?

Privilege access to Blackboard-e must be approved, granted, and monitored by the VHA Office of Connected Care Telehealth Services Blackboard-e System Administrators.

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

Yes, elevated privileges are being monitored by system administrators, and tracked and recorded in Blackboard-e audit logs.

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

According to Blackboard-e Access Control Policy and Procedures, dated November 14, 2023, Version 3.0, Procedures in 2.4a. Individuals identified in the Blackboard-e 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-e 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

First and last name, VA email address, Personal email address in the business Fax number field if VA employee wishes to access the system outside the VA Network, VISN, Facility, TMS unique identifier, Job title, Preferred pronoun and Nick name.

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.*

7 years. The system follows the National Archive and Record Administration (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?

No

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

VHA RCS 10-1 Section 1140.1. Clinical Trainee Onboarding Case File (CTOCF). The Clinical Trainee Onboarding Case File (CTOCF) is a standard document set that VAMCs will utilize to onboard health professions education trainees. The case file requires VA Medical Centers to collect and retain the following documents for each clinical trainee: Application for Health Professions Trainees (VA Form 10-2850D) Declaration for Federal Employment (OF-306) Appointment letter Appointment Affidavit (SF-61) Screening Checklist (VAF 10-0453) Employment Eligibility Form (I-9), if necessary Other forms and documentation may be added to this case file in the future. Temporary. Cutoff case files at the end of the CY in which the academic year is completed. Transfer to inactive off site storage, when 7 years old. Destroy 25 years after cutoff.
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 10-2 Section 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.

This system does not have SPI

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.

VHA Digital Health Office, Office of Connected Care does test new or modified IT systems for VHA operations prior to deployment, and PII may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, PII is used 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 may be used for that training purpose. However, VHA Digital Health Office, Office of Connected Care minimize the use of PII 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 testing and training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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:

Principle of Minimization: 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-e (Connected Care Academy (CCA)) E-Learning Platform strictly adheres to the Records Management Schedule to ensure no records are maintained longer than necessary. To mitigate this risk, Blackboard-e (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?

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 (IAM)	For Authentication purpose	First Name, Last Name, Email	SAML-HTTP
VA Talent Management System (TMS)	For authentication and employee training records and retention	TMS Person ID, First Name, Last Name, Email	SAML-HTTP

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: 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 to unintended parties or recipients.

Mitigation: Internal PII transfer between TMS and IAM teams 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).

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.

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***
University of Florida	To provide on-line telehealth program completion information to the College of Nursing, UoF	Full name, Personal or organizational Email address, Course/Program name and user completion date	Memorandum of Understanding	Encrypted email

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: There is a risk of PII being send to the wrong individual, thereby, exposing PII to unauthorized personal.

Mitigation: VA has appointed a POC to send the information to a designated individual in University of Florida in an encrypted email to minimize personal involvement.

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 2022, Pub.L. 107-347 §208(b) 91)(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 is disclosed.

The SORN (OPM-GOVT 1 and 76VA05 General Personnel Records (Title 38)-VA) 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.

Notice is provided.

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, this is consider adequate

Further reviews of the Privacy Policy language have defined specific policy to the information within Blackboard and how the information may be used and is included in the notice provide through the login process.

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.

Individuals have the opportunity and right to decline to provide information. This will not result in penalty or denial of service for the learners. However, failure to provide information will prevent privilege access to the system.

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 described 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)?
This system does not exempt from access provisions of the Privacy Act.

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?
This is Privacy Act system.

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 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 Record 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 individuals have 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 Support 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 Support 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?
Users have access to the system by signing into Blackboard.com

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?

Other government agencies do not have access to this system.

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 have permissions restricted to read-only for specific information, files, or folders, granted only through administrative settings. They do not have the ability to access any personal identifiable information.
- Learners have the ability to access content, but only see their own personal identifiable information.
- Instructors create course content and resource materials and have the ability to read and enroll users based on their information within the system (Learner's username, first name, last name, and email address).
- Evaluators who have the ability to generate reports and evaluate the statistical data from the reports.
- Elevated privilege users have the ability to read, write, and manage/modify the information within the system. There are differing levels of elevated privileges are assigned to specific roles.
- System Administrator have the ability to read, write, and manage/modify the information within the system as well as to approve elevated privilege users.

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.

Some contractors do have access to the system and PII, based on their support functions and roles. 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 and are allowed access to PII based on their role and support function. Contractors are required to provide validation of required Privacy and Security Risk Assessment training with Rules of Behavior and HIPPA Privacy Training on an annual basis to maintain their continued access.

This access is monitored and controlled based on their role with the OCC Telehealth office. All contractors are required to sign a non-disclosure agreement prior to getting access to the system.

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 for all uses. These are required annually per VA Policy. This is covered by the signed Blackboard-e Awareness and Training Policy and Procedures, dated November 14, 2023, Version 3.0 filed in eMASS with the Authorization to Operate.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06 Jan 2021
3. *The Authorization Status:* Approved Authorization to Operate
4. *The Authorization Date:* 27 January 2022
5. *The Authorization Termination Date:* 26 January 2025
6. *The Risk Review Completion Date:* 11 Jan 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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.***
N/A

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.

This is a Software 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.*

Yes.
MOU/ISA ID number 2274
Contract number is: Contract NNG15SD19B
Order Number is: Order 36C10A23F0112
Contract Language is included in the ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE APPLICABLE PARAGRAPHS TAILORED FROM: THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

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.

No. Backboard-e does not collect ancillary data.

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.

Yes. A contract is in place with the vendors and VA describing ultimate accountability for the data.

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-e 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
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 provided in this Privacy Impact Assessment is true and accurate.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.10.21 16:48:56 -04'00'

Privacy Officer, Nancy Katz-Johnson

ANUPAM ANAND

Digitally signed by ANUPAM ANAND
Date: 2024.10.24 11:01:46 -04'00'

Information Systems Security Officer, Anupam Anand

AIMEE BARTON

Digitally signed by AIMEE BARTON
Date: 2024.10.24 16:27:14 -04'00'

Information Systems 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; screen shot of a website collection privacy notice).

00-18287.pdf (govinfo.gov)

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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