Privacy Impact Assessment for the VA IT System called:

Dental Record Manager Plus (DRM+) Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

26 January 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Margaret (Peggy) Pugh	Margaret.Pugh@va.gov	202-731-6843
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202-815-9345
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

Document Storage System (DSS) Dental Record Manager Plus (DRM Plus) program is designed to provide dental health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient dental conditions, and develop and maintain the treatment plan. The DRM Plus program is an application that uses Remote Procedure Call (RPC) Broker technology that permits the facility users to store and retrieve clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. The use of the DRM Plus results in more accurate insurance billing for dental visits, consults and procedures. This application supports the filing of Dental Encounter System (DES) within the guidelines established by the Veterans Health Administration, Office of Dentistry.
DRM Plus uses RPC Broker technology, which permits the application end users to retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. The following information is retrieved from VistA: patient name, clinic name/location, visit date, and medical records information such as medication, health summaries, lab, consult, imaging. The DRM Plus dental diagnostic information, coding and crediting dental procedures, progress note (TIU (Text Integration Utilities)) are saved in VistA and dental images are saved in the VistA Imaging System. DRM Plus is publish on the Computerized Patient Record System (CPRS) Toolbar and workstation client is required.

The use of DRM Plus results in more accurate insurance billing for dental visits, consults and procedures. This application supports the filing of Dental Encounter System (DES) within the guidelines established by the Veterans Health Administration, Office of Dentistry.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*

- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

Dental Record Manager Plus (DRM Plus) application, under the Enterprise Program Management Office (EPMO), provided a customized user-friendly Windows Document System Storage (DSS) Graphical User Interface (GUI) for entering clinical encounter information and assisted with the assessment of ongoing care using current patient data for completed procedures. Dental Record Manager Plus (DRM Plus) is a GSS application that interface Veterans Health Information Systems and Technology Architecture (VistA) System using the RPC Broker technology. DRM Plus provides data input into the Veterans Health Information Systems and Technology Architecture (VistA) System Dental files, as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU) and Clinical Patient Record System (CPRS) Problem List packages. DRM Plus records diagnostic findings, including head and neck lesions, restorative and periodontal charting, and sequenced treatment planning. DRM Plus helps assure quality care, patient safety, and staff communication in an environment that is fully integrated with the VA electronic health record. This application supports the filing of Dental Encounter System (DES) within the guidelines established by the Veterans Health Administration, Office of Dentistry.

DRM Plus uses RPC Broker technology, which permits the application users to retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. Patient Information is retrieved from VistA, (such as – patient's full name (first, middle, and last name), clinic name/location, visit date, and medical records information such as medication, health summaries, lab, consult, imaging). The DRM Plus dental diagnostic information, coding and crediting dental procedures, progress note (TIU (Text Integration Utilities)) are saved in VistA and dental images are saved in the VistA Imaging System.

The use of DRM Plus results in more accurate insurance billing for dental visits, consults and procedures. This application supports the filing of Dental Encounter System (DES) within the guidelines established by the Veterans Health Administration, Office of Dentistry.

Some features of DRM Plus are summarized in the following:

- Entry of dental conditions plans and completed procedures through the use of graphic icons with extensive use of color schemes.
- Upper/Lower/Full Views with full color-coded graphics
- Sequencing of Treatment Plan procedures
- Dental History with date-change capability

- Quadrant or Tooth summaries
- Head/Neck Findings availability
- Periodontal charting
- Full Mouth Plaque Index with definitions
- ADA/Local/Quick Codes
- Creation and maintenance of tooth-specific and general patient notes

Dental Record Manager Plus (DRM Plus) application is used at all VHA sites and the software is hosted on local sites virtual server. The VA considers DRM Plus to be a COTS product because it could be sold and interfaced with other systems; but it never has been and, at least at this time, is only used by VHA sites even though we have a version that could be sold and used by non-VHA sites. The completion of the PIA will not change the DRM+ business and technology processes.

DRM+'s legal authority for operating: Title 38 United States Code (U.S.C.) §§1710(c), 1712 and Title 38 Code of Federal Regulation (CFR) 17.160 – 17.166 authorizes the provision of dental care and associated dental record-keeping. Additionally, all 50 state dental boards have specific requirements for record-keeping as a condition of licensure. The applicable System of Records Notices (SORN) are 24VA10A7, Patient Medical Record-VA, and 121VA10A7, National Patient Databases-VA, and would likely not require amendment.

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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☐ Other Unique Identifying Number (list below)

Previous medication, clinic name/location, visit date, and medical records information such as medication, health summaries, lab, consult, imaging. dental images

PII Mapping of Components

Dental Records Manager Plus consists of one key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Dental Record Manager Plus and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
Veterans Health Information Systems and Technology Architecture (VistA) System	Yes	Yes	Person full name (first, middle, and last), Social Security Number, Date and place of birth, address, telephone number, etc.	Ensure correct records is retrieve from VistA	Data is encrypted

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

DRM Plus uses RPC Broker technology, which permits the application end users to retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. The following information is retrieved from VistA: patient name, clinic name/location, visit date, and medical records information such as medication, health summaries, lab, consult, imaging. The DRM Plus dental diagnostic information, coding and crediting dental procedures, progress note (TIU (Text Integration Utilities)) are saved in VistA and dental images are saved in the VistA Imaging System.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Dental Record Manager Plus (DRM) Plus is a Graphical User Interface (GUI) front-end for data input into the Veterans Health Information Systems and Technology Architecture (VistA) dental files as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU), Computerized Patient Record Search (CPRS) Problem List, and Vitals packages. This technology allows dentists and dental staff to access a patient`s entire medical record and enables them to enter diagnostic findings, treatment plan procedures and patient- and tooth-specific notes into the patient`s Electronic Health Record. Application user requires a VistA account with DRM Plus

and CPRS VistA secondary menu option/security key/VistA Person Class Code, etc. to retrieve and store new data.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

Dental Record Manager Plus (DRM) Plus is a Graphical User Interface (GUI) front-end for data input into the Veterans Health Information Systems and Technology Architecture (VistA) dental files. This software may enhance patient care by fostering the exchange of medical data.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Population Health clinical staff manages and validates the data, by querying the Veterans Health Information Systems and Technology Architecture (VistA) System database and the Dental Record Manager Plus (DRM+) application. Dental Record Manager Plus (DRM Plus) captures specific dentally related information elements not readily available in Computerized Patient Record System (CPRS). These elements include oral cavity/tooth related diagnostic findings, dental-specific care plans and a superset of completed care information. DRM Plus aids the provider in the entry of dental diagnostic information, coding and crediting dental procedures, completing TIU progress notes, and planning and tracking dental patient care. DRM Plus is a

Dental Graphical User Interface front end for data input into the VistA Dental files, as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU) and CPRS Problem List packages.

1.6 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

Title 38 United States Code (U.S.C.) §§1710(c), 1712 and Title 38 Code of Federal Regulation (CFR) 17.160 – 17.166 authorizes the provision of dental care and associated dental record-keeping. Additionally, all 50 state dental boards have specific requirements for record-keeping as a condition of licensure. The applicable System of Records Notices (SORN) are 24VA10A7, Patient Medical Record-VA, and 121VA10A7, National Patient Databases-VA, and would likely not require amendment.

1.7 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.

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 DRM+ application retrieve and collects Personally Identifiable Information (PII), Protected Health Information (PHI), and other highly delicate Sensitive Personal Information (SPI). If this information were to be breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the Veteran in crisis, identify the potential issues and concerns, and offer assistance to the Veteran so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the Veterans' information. Users are trained on how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

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: Patient full name (first, middle, last). Used as a person's identifier
Social Security Number: Assists in uniquely identifying the person's medical record.
Date of Birth: Assists to identify patient age and confirm patient identity
Personal Mailing Address: Used to contact the individual
Personal Phone Number(s): Used to contact the individual
Emergency Contact Information: Used in case of emergencies
Medical Record Number: Used to communicate and bill third party health care plans
Current Medications: Assists to determine medical history and healthcare outcome and used to administer medication
Race/Ethnicity: Assists to determine Race/Ethnicity.
Previous medications: Assists to determine medical history and healthcare outcome and used to administer medication
Dental Images: Assists to administer dental treatment.Images are stored in the VistA Imaging System.
Clinical Name/Location: Used to identify place of treatment. Included in the TIU note.
Visit Date: Used to identify the date/time of visit. Included in the TIC note.
Health Summaries: Assists to determine medical history
Labs: Assists to determine medical history
Consults: Assists to determine medical history

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

DRM+ does not analyze or produce patient data. The DRM Plus program is designed to provide dental health care facilities with an intuitive, user-friendly Windows interface for end-users to create encounter information, evaluate patient dental conditions, and develop and maintain the treatment plan. The DRM Plus program is an application that uses RPC Broker technology, which permits the facility users to store and retrieve clinical data within the VistA System

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

<u>Principle of Use Limitation:</u> 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.

DRM+ is used by the VHA sites Dental Service staff.
Local VHA site Dental Service Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS request for new user's Veterans Health Information Systems and Technology Architecture (VistA) ePAS request can include VistA menu options/security keys, Clinical Patient Record System (CPRS) access, etc. There are application-specific VistA menu option/security keys, and VistA role-specific configuration.
Local VHA site OI&T is responsible to complete the ePAS request. The following is the DRM Plus user's requirements:
VistA DRM+ Secondary Menu option
VistA DRM+ Security Key
VistA Person Class Code
VistA User Class Code
VistA Electronic Signature Code
VistA Default Division
VistA New Person File required DRM+ fields completed (e.g. initials field)
VistA Dental Provider File (8-Digit Dental Provider ID)
VistA DENTV DRM ADMINISTRATOR. Field populated (DRM+ Administrator only)
Local VHA site OI&T is responsible to complete the ePAS request.
Local VHA site Dental Administrator must confirm/configure:
Confirm that at least one or two users are set up as Dental Administrator within DRM Plus
Perform restricted functions unable to be performed by regular DRM Plus users
Permissions set up prior to any other users being set up within the application

All VHA staff is responsible for assuring safeguards for the PII. Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly. VHA facilities ISSO is responsibility to monitor VistA access and verify the TMS training has been completed and current.

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
Social Security Number
Date of Birth
Personal Mailing Address
Personal Phone Number(s)

Emergency Contact Information
Medical Record Number
Current Medications
Race/Ethnicity
Previous medications
Dental Images (stored in the VistA Imaging System)
Clinical Name/Location:
Visit Date:
Health Summaries:
Labs:
Consults:

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

The DRM+ data is stored in the Veterans Health Information Systems and Technology Architecture (VistA) System which is to be maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)." https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. Retire annually to the records storage facility. If not recalled by the accessioning facility for reactivation, destroy by WITNESS DISPOSAL 72 years after retirement (75 after the last episode of care).

Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual. VA Electronic Health Records (ERM) system permanently retains data as part of ongoing healthcare.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

Official record held in the office of record. Maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted, VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)." https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. Retire annually to the records storage facility. If not recalled by the accessioning facility for reactivation, destroy by WITNESS DISPOSAL 72 years after retirement (75 after the last episode of care).

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

The DRM+ records are to be maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)." https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. Retire annually to the records storage facility. If not recalled by the accessioning facility for reactivation, destroy by WITNESS DISPOSAL 72 years after retirement (75 after the last episode of care).

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

DRM+ Patches (VistA KIDS build and GUI executable) are not released National installation prior to testing.
With an approved MOU (Memorandum of Understanding) from the IOC site(s), the vendor, Document Storage System (DSS, Test Patches are installed and tested in the VistA and DRM+ Pre-Production Test System. ICO site(s) tester(s) complete the Test Site(s) User's Acceptance VistA Pre-Production System document prior to VistA and DRM+ Production System installation. Test patients are created in the VistA Pre-Production System to be used when testing new DRM+ Patches. VistA Pre-Production System Test patients' data are scrambled and DRM+ Test shortcut located on the application server DocTest folder is mapped to the VistA Pre-Production System hostname and port number.

New DRM+ Patches are released for National installation after the ICO Test Site(s) User's Acceptance VistA Production System document(s) are received.

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.

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: No data to store within the DRM+ System. The greater the risk is that the information could be compromised or breached in the Veterans Health Information Systems and Technology Architecture (VistA) System.

Mitigation: If the DRM+ information on the Veterans Health Information Systems and Technology Architecture (VistA) System is part of ongoing research or health care support, the information should be maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)." https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. Retire annually to the records storage facility. If not recalled by the accessioning facility for reactivation, destroy by WITNESS DISPOSAL 72 years after retirement (75 after the last episode of care).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Information System & Technology Architecture (VistA)	Retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System. summaries, lab, consult, imaging. The DRM Plus is designed to provide dental diagnostic information, evaluate	Demographics, Outpatients visits, Problem list codes, Diagnosis codes, Procedure codes, Laboratories, Pharmacy, X-Ray images	DRM Plus uses RPC Broker technology, which permits the application end users to retrieve and store clinical data within the Veterans Health Information Systems and Technology Architecture (VistA) System.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
	patient dental conditions, coding and crediting dental procedures, progress note (TIU (Text Integration Utilities)) are saved in VistA and dental images are saved in the VistA Imaging System. The use of the DRM Plus results in more accurate insurance billing for dental visits, consults and procedures. This application supports the filing of Dental Encounter System (DES) within the guidelines established by the Veterans Health Administration, Office of Dentistry.)		

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

Follow the format below:
Privacy Risk: The privacy risk associated with maintaining PII/PHI is that sharing data within the Department of Veteran's Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the population Healthcare and non-Healthcare providers. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

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: The privacy risk associated with maintaining PII/PHI is that sharing data outside of the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. All personnel accessing veteran information must have a successfully adjudicated.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

All data in DRM+ is secondary data, extracted from VistA data. The VistA data is generated as part of routine medical care. Veterans are provided with Privacy Act statements as part of routine medical care. All enrolled Veterans and Veterans who are treated at VA Medical Centers but not required to enroll are provided the VHA Notice of Privacy Practices (NoPP) every three years, or sooner if a change necessitates an updated notice. The NoPP is also prominently posted in every VAMC (posters) and on the VA public-facing website.

Additional notice is provided by the System of Record Notice (SORN), in **24VA10A7, Patient Medical Record-VA**, **- https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf,** and in **121VA10A7, National Patient Database-VA,** 121VA10A7.pdf (sharepoint.com). A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

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

DRM+ extracts data that exists that was generated in the course of routine medical care. Patients can in general decline to provide information in routine medical care. Individuals should view the PIA for their local facility VistA to see whether they can consent to their information being used or decline it

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

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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.

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: If notice isn't provided then individuals will unknowingly be giving up their information that will be used for other purposes.

Mitigation: To prevent any inaccurate data, only authorized VA clinical personnel have access to the information. Notice is provided by SORN 24VA10A7 and 121VA10A7 and all individuals should check their local VA facilities VistA PIA for more information regarding notice and consent (if applicable).

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?

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.

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).

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 question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

VHA Directive 1605.01 Privacy and Release of Information, Paragraph 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Under the jurisdiction of VHA, VHA Directive 1605.01 Privacy and Release of Information, Paragraph 8 states the rights of the Veterans to amend their records. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. A request for amendment of

information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains. The individual requesting the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations. Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

If the individual discovers that incorrect information was entered into their CPRS medical record, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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.

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 the individual accidentally provides incorrect information in their correspondence.

Mitigation: Veterans provide information at the local VAMC. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Local VHA site Dental Service Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS request for new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application users have completed the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training. Dental staff roles are determined by the VistA Person Class codes. Dental Providers must have a valid Dental Person Class in VistA File 200 (New Person) File. Residents must have one of the following person classes:

V030300 - Dental Residence
V115500 - Dental Specialized Physicians
V115600 - Interns and Residents

Local VHA site OI&T is responsible to complete the ePAS request.
OI& Technical staff: ePAS approval for System Administrator (grant server access), Application Administrator (manage application), VistA Management (manage VistA System DRM+-related tasks)permission. Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training.
Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers

Note: Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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 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.

No. Contractors and vendors does not have access to COTS Interface Division servers/applications.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual HIPAA, Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes. DRM+ is in the process of submitting for an ATO in eMASS once all artifacts are uploaded, it is being prepared for its own ATO for the month of May 2021.

Section 9. 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**

ID	Privacy Controls
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.

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2021.04.20 10:49:08 -04'00'

Privacy Officer, Margaret Pugh

Amine Messaoudi 1136390

Digitally signed by Amine Messaoudi 1136390
Date: 2021.04.20 11:12:50 -04'00'

Information Security Systems Officer, Amine Messaoudi

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.04.20 10:21:43 -05'00'

Information System Owner, Christopher Brown

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).

VHA Handbook 1605.04, VHA Notice of Privacy Practices:

Notice of Privacy Practices IB 10-163 (sharepoint.com)

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090