Security Categorization

VistA Adaptive Maintenance (VAM) Assessing

July 24, 2018

Version 1.0

Department of Veteran Affairs

Introduction:

The Information Type / System Categorization Matrix is based on the VIP: Security Guide IT Security Engineering Information Type Identification and System Categorization Standard Operating Procedure (SOP). It effectively implements and prepares for system categorization, Step 1 in Risk Management Framework (RMF) as outlined in VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3 VA Information Security Program. The Information Type / System Categorization Matrix captures the Information Type Identifier from NIST SP 800-60 Volumes 1 and 2 as well as unique information types with description and rationale.

Background:

NIST SP 800-60 volumes 1 and 2 incorporate FIPS 199 categorization and is captured in the Provisional / Initial sub column under Security Category in the matrix below. The final sub column under Security Category in the matrix will depict the vetted categorization of each info type and the rationale of the difference from the FIPS provisional categorization.

Information Types and Provisional Impact Levels:

The following table documents the Information Types to be processed by VAM. The list of information types was developed using probable datatypes listed from the NIST SP 800-60 volume II. The VAM security working group then conducted a review of the initial list expected to be processed by VAM. This is the list of information types addressed in the table below. For each information type the following values are captured:

NIST SP 800-60 vol2 Information Type Reference # and Descriptive Title

NIST SP 800-60 vol2 Provisional Impact Values

VAM Determined Impact Values

NIST 800-60 Vol II: Special Factor Considerations and Rationale for Adjustments

NIST 800-122 Guide for Protecting Confidentiality of Personally Identifiable Information

This table is a good way to tell the story of the impact values determined for each of the information categories and to document which values differ from the NIST assigned initial impact values and the rationale behind adjustments made to the final impact levels.

Recommendation:

The OIS Cyber Security Technology and Metrics (CTM) Team's assessment of the information types relevant to this system against the NIST assigned provisional impact levels and special factors support Categorization of the System as the following:

Security Objective	VAM
Confidentiality	**Moderate**
Integrity	**High**
Availability	**High**

1. Review and Adjustment of Provisional Impact Levels:

Each of the information types listed in the table represents the types of data that could be included the VAM system. The Cyber Security Technology and Metrics (CTM) team reviewed the impact levels by using the NIST Special Publication 800-60 Volumes 1 and 2 as guidance for consideration and determination of the impact values based upon NISTs write-up and explanation of the reasoning behind the provisional impact values.

The actual end-result of categorization will be determined through a thorough analysis of the system and the data that could be consumed or originated by VAM.

2. Other Important Considerations:

It is important to note that the sensitivity level of the information types was an important factor in determining the impact levels for confidentiality, integrity, and availability. Information types that include PII and/or PHI as documented in the PTA and PIA must be protected in compliance with provisions of the Privacy Act of 1974 and with the Health Insurance Portability and Accountability Act of 1996, respectively.

Another important consideration is the large quantity of records shared and the aggregate impact that a failure to maintain confidentiality, integrity, and availability of those records could have on large numbers of the population served by the VA but also to the reputation of VA and the public trust that is required for VA to fulfill its mission in an effective manner. Section 3.2.2 of NIST SP800-122 provides guidance supporting raising the impact level for information types that represent a large number of records as a breach of 25 records are different than 25 million records. The large amounts of records if compromised represent a significant risk to the VA.

3. Security Categorization:

Please see the below table.

VAM Information Type / Categorization Matrix							
Information Type Reference # and Descriptive Title	**Security Category**						**Special Factor Considerations and Rationale for Adjustments**
	NIST 800-60 Provisional / Initial			**Final**			
	C	**I**	**A**	**C**	**I**	**A**	
C.2.8.9 Personal Identity and Authentication Information - Information Type Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information include individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc.	M	M	M	M	M	H	***Confidentiality:*** **Supplemental Guidance:** The confidentiality impact level is based on the effects of unauthorized disclosure of personal identity and authentication information on the ability of Federal agencies to determine that communications with and payments to individuals are being made with or to the correct individuals - and to protect individuals against identity theft and the Federal government against fraud. Unauthorized disclosure of raw data and other source information for identity authentication operations is likely to violate the Privacy Act of 1974 and other regulations applicable to the dissemination of personal and government information. There are many cases in which unauthorized disclosure of personal identity and authentication information will have only a limited adverse effect on government operations, assets, or individuals. However, the potential for use of such information by criminals to perpetrate identity theft and related fraud can do serious harm to individuals. Unauthorized disclosure of centrally managed personal identity and authentication information, such as passport and visa control databases can have a serious adverse effect on agency missions. **Recommended Confidentiality Impact Level:** The provisional confidentiality impact level

							recommended for personal identity and authentication information is ***moderate***. **Special Factors Affecting Confidentiality Impact Determination:** For agencies that manage large income information involving records of the public, the provisional confidentiality impact level can be expected to be at least ***moderate***. Where personal identity and authentication information is used in controlling access to facilities (e.g., Federal facilities, critical infrastructure facilities, key national assets) or for border control purposes, the consequences of unauthorized disclosure that permits credentials forgery can justify a ***high*** impact assignment. ***Integrity:*** **Supplemental Guidance:** The integrity impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to detect the modification or destruction of information. In the case of very large databases containing personal identity and authentication information relating to the public, there is a significant probability that erroneous actions will be taken affecting benefits entitlements of or access to facilities by large numbers of individuals. In the case of benefits, this can result in at least short-term financial hardship for citizens. It can also be expected to result in very serious disruption of the agency operations due to large time and resource requirements for taking corrective actions. **Recommended Integrity Impact Level:** The provisional integrity impact level recommended for personal identity and authentication information is ***moderate***. **Special Factors Affecting Integrity Impact Determination:** In the case of smaller organizations, and where the information affected is limited to employees,

							there will still be an impact, but the consequences may justify only a ***low*** provisional impact rating. Where a data modification permits access to facilities (or ingress into the United States) by individuals to whom access should be prohibited, the integrity impact could be ***high***. ***Availability:*** **Supplemental Guidance:** The availability impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to re-establish access to the personal identity and authentication information. Benefits determination *processes* are generally tolerant of reasonable delays. In many cases, disruption of access to personal identity and authentication information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals. **Recommended Availability Impact Level:** The provisional availability impact level recommended for personal identity and authentication information is ***high*** due to the reasoning that loss of availability could delay healthcare for individuals. VAM provides services between the users and VistA. The large amount of VistA data records and the potential loss of access to VistA if the user cannot be authenticated properly could potentially delay healthcare or at least make healthcare less efficient if VistA cannot be accessed. If VAM is down, those users cannot access VistA. **Special Factors Affecting Availability Impact Determination:** In the case of very large data bases containing personal identity and authentication information relating to the general public, there is a significant probability that processing delays will affect the benefits entitlements of or access to facilities by large numbers of individuals. The larger the number of records affected, the longer the delays that can be expected to result. This can result in financial hardship for citizens and in serious

							disruption of the agency operations due to large time and resource requirements for backlog processing. In such cases, the availability impact level would be at least ***moderate***. In the case of permanent loss of records or access to facilities by emergency personnel, the impact might even be ***high***.
D.14.1 Access to Care Information Type Access to Care focuses on the access to appropriate care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination and managing patient movement.	L	M	L	L	M	L	***Confidentiality:*** **Supplemental Guidance:** The confidentiality impact level is the effect of unauthorized disclosure of access to care information on the ability of responsible agencies to focus on the access to appropriate care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination, and managing patient movement will have only a limited adverse effect on agency operations, assets, or individuals. **Recommended Confidentiality Impact Level:** The provisional confidentiality impact level recommended for disclosure of access to care information is ***low***. **Special Factors Affecting Confidentiality Impact Determination:** Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In

							such cases, the confidentiality impact level may be ***moderate***. ***<u>Integrity:</u>*** **Supplemental Guidance:** The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Many activities associated with access to care information are not time critical and the adverse effects of unauthorized modification or destruction of health care information on agency mission functions and/or public confidence in the agency will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission. **Recommended Integrity Impact Level:** The provisional integrity impact level recommended for access to care information is ***moderate***. ***<u>Availability:</u>*** **Supplemental Guidance:** The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to care. Access to care is generally tolerant of delay. Typically, disruption of access to care information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals. **Recommended Availability Impact Level:** The provisional availability impact level recommended for access to care information is ***low***.

							Special Factors Affecting Availability Impact Determination: Some access to care information could be deemed time-critical and is dependent on the severity of the health issue requiring immediate access to care, patient movements, etc. Delays in the communication of specific situations may cause serious impacts to the patient or care provide. This can result in assignment of a ***moderate*** impact level to such information.
D.14.4 Health Care Delivery Services Information Type Health Care Delivery Services provides and supports the delivery of health care to its beneficiaries. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation.	L	H	L	M	H	M	***Confidentiality:*** **Supplemental Guidance:** The confidentiality impact level is the effect of unauthorized disclosure of health care delivery services on the ability of responsible agencies to provide and support the delivery of health care to its beneficiaries will have only a limited adverse effect on agency operations, assets, or individuals. **Recommended Confidentiality Impact Level:** The confidentiality impact level for disclosure of health care delivery services information was determined to be ***moderate*** based the potential number of records affected and the resulting effects on the reputation of the VA if confidentiality of that data was lost. **Special Factors Affecting Confidentiality Impact Determination:** Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be ***moderate***.

							Integrity: **Supplemental Guidance:** The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Many activities associated with health care delivery services are not time critical and the adverse effects of unauthorized modification or destruction of health care information on agency mission functions and/or public confidence in the agency will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission. **Recommended Integrity Impact Level:** Because of the potential for the loss of human life, the provisional integrity impact level recommended for health care delivery services information is ***high***. ***Availability:*** **Supplemental Guidance:** The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish Health Care Administration information. Except for cases of emergency actions necessary to correct urgent threats to patient health, health care processes are usually tolerant of reasonable delays. **Recommended Availability Impact Level:** The availability impact level for health care delivery services information was determined to

							be ***moderate*** based upon the fact that the loss of VAM capability would be expected to delay access to VistA for a large number of clinical personnel. **Special Factors Affecting Availability Impact Determination:** Some health care delivery services information is time-critical and is dependent on the severity of the health threat(s) and the rapidity with which the threat is spreading/ growing. Delays in the communication of specific situations may be life threatening. This can result in assignment of a ***moderate*** or ***high*** impact level to such information.
D.16.6 Substance Control Information Type Substance control supports activities associated with the enforcement of legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities.	M	M	M	M	M	M	***Confidentiality:*** **Supplemental Guidance:** The confidentiality impact level is the effect of unauthorized disclosure of substance control information on the ability of responsible agencies to enforce legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities. Unauthorized disclosure of a significant proportion of substance control information can compromise investigations, cause apprehension operations to fail, and compromise prosecutions. **Recommended Confidentiality Impact Level:** The provisional confidentiality impact level recommended for disclosure of substance control information is ***moderate***. **Special Factors Affecting Confidentiality Impact Determination:** Unauthorized disclosure of some routine substance control information is unlikely to have more than a limited adverse effect on agency operations, agency assets, or individuals. The confidentiality impact associated with such information is ***low***. Where the unauthorized disclosure of information exposes sensitive information sources or compromises investigative or interdiction operations, the consequences of unauthorized

							disclosure of substance control information may have a serious adverse effect on agency operations, significantly degrade mission capability, and/or pose a threat to human life. Where unauthorized disclosure endangers investigations in process, investigative or intelligence information sources, or information regarding witnesses or other critical case file elements, the danger to human life and key agency missions can be significant. Where unauthorized disclosure endangers witnesses or law enforcement officers, the impact level must be rated as ***high***. Other factors affecting confidentiality impacts associated with substance control information are discussed under Section D.16.1 (Criminal Apprehension) and Section D.16.2 (Criminal Investigation and Surveillance). Some substance control information is classified (e.g., some intelligence-derived information). Classified information and other *national security information* are outside the scope of this guideline. ***Integrity:*** **Supplemental Guidance:** The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The amount of money available to perpetrators significantly increases the insider threat. The consequences of unauthorized modification or destruction of information can be serious if the information is critical to tactical operations i.e., is time-critical. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to most missions would usually be limited. **Recommended Integrity Impact Level:** Because the consequences of unauthorized modification or destruction of information can be serious if the information is critical to tactical

							operations (i.e., is time-critical), the provisional integrity impact level recommended for substance control information is ***moderate***. **Special Factors Affecting Integrity Impact Determination:** Unauthorized modification or destruction of information (particularly time-critical information) affecting internal communications can jeopardize investigations, prosecutions, the lives of witnesses, and the safety of enforcement officers. In some cases, unauthorized modification or destruction of information can result in loss of human life. In such cased, the integrity impact level is ***high***. Other factors affecting integrity impacts associated with substance control information are discussed under Section D.16.1 (Criminal Apprehension) and Section D.16.2 (Criminal Investigation and Surveillance). ***Availability:*** **Supplemental Guidance:** The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to substance control information. Most substance control processes are usually tolerant of reasonable delays. **Recommended Availability Impact Level:** The provisional availability impact level recommended for most substance control information is ***moderate***. **Special Factors Affecting Availability Impact Determination:** The consequences of unavailability of information can be serious if the information is critical to tactical operations i.e., is time-critical. Failure of some processes during tactical operations can result in both threats to human life and severe harm to public confidence in the agency. The impact level assigned to information and information systems associated with these tactical processes is ***high***.

Security Category High-Water Mark by Impact Level	M	H	M	M	H	H	**Assigned Security Category Derived from Final Impact Values = H**

4. Discussion of Information Types and Use Specific to VAMs:

The information types listed in this security categorization document are derived from the VistA Region 3 PTA signed May 9, 2017. These are intended to be representative of the types of data elements accessed by VistA users through the VAM application. The detailed information elements include the following from the VistA PTA referenced above:

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- 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
- Gender
- Guardian name and contact information
- Next of kin name and contact information
- Military and service history
- Employment information
- Veteran dependent information
- Education information
- Research medical statistics
- Service connected rating and disabilities

- Criminal background information
- Date of death

C.2.8.9 Personal Identity and Authentication Information -Information Type

Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information includes individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc…

This data type was included because VAM will route users to VistA modules, such as, Pharmacy, Allergy and Vitals. VAM users will access healthcare records that include the types of PII information types described above. Specifically, VAM users will have access to veteran's social security numbers, names, dates of birth, etc… as these data elements are needed to ensure that the veteran being treated is matched to the correct medical record.

Special Factor Considerations and Rationale for Adjustments

For this information type NIST assigns a provisional impact level of "moderate" to the potential harm to the VA's credibility, reputation, and ability to serve its mission that could result from the loss of data confidentiality, integrity and availability respectively.
The special factors that NIST lists as examples of factors that could warrant an adjustment or tailoring of the provisional impact levels include the following:

Confidentiality - Where personal identity and authentication information is used in controlling access to facilities (e.g., Federal facilities, critical infrastructure facilities, key national assets) or for border control purposes, the consequences of unauthorized disclosure that permits credentials forgery can justify a ***high*** impact assignment. This was considered not applicable to VAM as the data elements are not used in controlling access to the types of facilities listed.

Integrity - In the case of smaller organizations, and where the information affected is limited to employees, there will still be an impact, but the consequences may justify only a ***low*** provisional impact rating. Where a data modification permits access to facilities (or ingress into the United States) by individuals to whom access should be prohibited, the integrity impact could be ***high***. This was considered not applicable to VAM as data modification would not permit access to facilities (or ingress into the United States) by individuals to whom access should be prohibited.

Availability - In the case of very large data bases containing personal identity and authentication information relating to the general public, there is a significant probability that processing delays will affect the benefits entitlements of or access to facilities by large numbers of individuals. The

larger the number of records affected, the longer the delays that can be expected to result. This can result in financial hardship for citizens and in serious disruption of the agency operations due to large time and resource requirements for backlog processing. In such cases, the availability impact level would be at least moderate. In the case of permanent loss of records or access to facilities by emergency personnel, the impact might even be high. Consideration of this explanation led the VAM team to a discussion of the potential harm that loss of availability of the Personal Identity and Authentication Information accessed via VAM would cause to the VA. It was determined that this impact level warranted an adjustment from moderate to **High** as the permanent loss of this information type would necessarily impede the ability of VA personnel to reliably match medical records to individual veterans thus disrupting medical care to those individuals which would negatively impact the VA mission of providing healthcare services to veterans and could potentially result in harm to veterans not receiving the correct healthcare on a timely basis.

D.14.1 Access to Care Information Type

Access to Care focuses on the access to appropriate care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination and managing patient movement.

This data type was included because VAM will route users to VistA modules, such as, Pharmacy, Allergy and Vitals. VAM users will access healthcare records that directly determine the access to appropriate care information type described above. Specifically, VAM users will have access to veteran's healthcare vitals, such as blood pressure, heart rate, temperature, allergies, etc… These data elements directly affect the type of care, location, and availability of care that will result from a veteran's need to see an allergist, a cardiologist, or other healthcare professionals which will then drive the type, location, and timeliness of care which are all elements of the access to care information type defined above. The confidentiality, integrity and availability of the data elements described will be a key factor in determining the type of care and therefore the access to care available to the veteran.

Additionally, VAM will provide access to data used to enroll providers which would include certificate information and potentially criminal background information.

Special Factor Considerations and Rationale for Adjustments

For this information type NIST assigns a provisional impact level of:
Low for Confidentiality,
Moderate for Integrity, and
Low for Availability.

These impact levels are in relation to the potential harm to the VA's credibility, reputation, and ability to serve its mission that could result from the loss of data confidentiality, integrity and availability of this information type. The special factors that NIST lists as examples of factors that could warrant an adjustment or tailoring of the provisional impact levels include the following:

Confidentiality - Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be moderate. These special factors were considered not applicable to VAM as the data elements applicable to the Access to Care information type are already considered under other information types, such as, the Personal Identity and Authentication and Healthcare Delivery Services information types. No modification was made to the NIST provisional impact level of Low for confidentiality.

Integrity - The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Many activities associated with access to care information are not time critical and the adverse effects of unauthorized modification or destruction of health care information on agency mission functions and/or public confidence in the agency will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission. The provisional integrity impact level recommended for access to care information is moderate. These additional considerations were determined to be not applicable to VAM as modification of the data elements discussed by NIST are already covered under Healthcare Delivery Services information type and the data accessed by VAM users does not directly affect external communications that might contain healthcare data. No modification was made to the NIST provisional impact level of Moderate for integrity.

Availability - Some access to care information could be deemed time-critical and is dependent on the severity of the health issue requiring immediate access to care, patient movements, etc… Delays in the communication of specific situations may cause serious impacts to the patient or care provided. This can result in assignment of a moderate impact level to such information. The provisional availability impact level recommended for access to care information is low. These

additional considerations were determined to be not applicable to VAM as delays in the availability of the data elements discussed by NIST are already covered under Healthcare Delivery Services information type. No modification was made to the NIST provisional impact level of Low for integrity.

D.14.4 Health Care Delivery Services Information Type

Health Care Delivery Services provides and supports the delivery of health care to its beneficiaries. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation.

This data type was included because VAM will route users to VistA modules, such as, Pharmacy, Allergy and Vitals. VAM users will access healthcare records that include the types of healthcare delivery information types described above. Specifically, VAM users will have access to veteran's healthcare data, such as, vitals (i.e., blood pressure, heart rate, temperature, etc.), pharmacy data on medicines prescribed for the veteran, and allergies, etc… as these data elements are part of the patient records required for delivery of healthcare to veterans.

Special Factor Considerations and Rationale for Adjustments

For this information type NIST assigns a provisional impact level of:
Low for Confidentiality,
High for Integrity, and
Low for Availability.

These impact levels are in relation to the potential harm to the VA's credibility, reputation, and ability to serve its mission that could result from the loss of data confidentiality, integrity and availability of this information type. The special factors that NIST lists as examples of factors that could warrant an adjustment or tailoring of the provisional impact levels include the following:

Confidentiality - Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be moderate. Consideration of these factors led the VAM team to a discussion of the potential harm that loss of confidentially of the Health Care Delivery Services information accessed via VAM would cause to the VA. It was determined that

this impact level warranted an adjustment from low to **Moderate** as the unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations.

Integrity - The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Many activities associated with health care delivery services are not time critical and the adverse effects of unauthorized modification or destruction of health care information on agency mission functions and/or public confidence in the agency will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect operations and public confidence in the agency and the agency mission. Because of the potential for the loss of human life, the provisional integrity impact level recommended for health care delivery services information is high. No modification was made to the NIST provisional impact level of High for integrity.

Availability - Some health care delivery services information is time-critical and is dependent on the severity of the health threat(s) and the rapidity with which the threat is spreading/ growing. Delays in the communication of specific situations may be life threatening. This can result in assignment of a moderate or high impact level to such information. Consideration of these special factors explanation led the VAM team to a discussion of the potential harm that loss of availability of the Healthcare Delivery Services information accessed via VAM would cause to the VA and to the veterans it serves. It was determined that this impact level warranted an adjustment from low to **Moderate** as the loss of availability of this information could result in delays in the communication of specific situations which may be life threatening.

D. 16.6 Substance Control Information Type

Substance control supports activities associated with the enforcement of legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities.

This data type was included because VAM will route users to VistA modules, such as, Pharmacy. VAM users will access healthcare records that include the substance control information type described above. Specifically, VAM users will have access to veteran's healthcare data, such as, pharmacy data on medicines prescribed for the veteran as these data elements are part of the patient records required for delivery of healthcare to veterans. The data related to medications and patient medical record history could be used in enforcing substance control laws and regulations.

Special Factor Considerations and Rationale for Adjustments

For this information type NIST assigns a provisional impact level of:
Moderate for Confidentiality,
Moderate for Integrity, and
Moderate for Availability.

These impact levels are in relation to the potential harm to the VA's credibility, reputation, and ability to serve its mission that could result from the loss of data confidentiality, integrity and availability of this information type. The special factors that NIST lists as examples of factors that could warrant an adjustment or tailoring of the provisional impact levels include the following:

Confidentiality - Unauthorized disclosure of some routine substance control information is unlikely to have more than a limited adverse effect on agency operations, agency assets, or individuals. The confidentiality impact associated with such information is ***low***.

Where the unauthorized disclosure of information exposes sensitive information sources or compromises investigative or interdiction operations, the consequences of unauthorized disclosure of substance control information may have a serious adverse effect on agency operations, significantly degrade mission capability, and/or pose a threat to human life. Where unauthorized disclosure endangers investigations in process, investigative or intelligence information sources, or information regarding witnesses or other critical case file elements, the danger to human life and key agency missions can be significant. Where unauthorized disclosure endangers witnesses or law enforcement officers, the impact level must be rated as ***high***. It was determined that this impact level did not warrant an adjustment from **Moderate**. No modification was made to the NIST provisional impact level of Moderate for Confidentiality.

Integrity - The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of information (particularly time-critical information) affecting internal communications can jeopardize investigations, prosecutions, the lives of witnesses, and the safety of enforcement officers. In some cases, unauthorized modification or destruction of information can result in loss of human life. In such cased, the integrity impact level is ***high***. It was determined that this impact level did not warrant an adjustment from **Moderate**. No modification was made to the NIST provisional impact level of Moderate for Integrity.

Availability - The consequences of unavailability of information can be serious if the information is critical to tactical operations i.e., is time-critical. Failure of some processes during tactical operations can result in both threats to human life and severe harm to public confidence in the agency. The impact level assigned to information and information systems associated with these tactical processes is ***high***. It was determined that this impact level did not warrant an adjustment from **Moderate**. No modification was made to the NIST provisional impact level of Moderate for Availability.

5. Conclusion:

The CTM Team's assessment of the information types relevant to this system against the NIST assigned provisional impact levels and special factors support that the Security Category High-Water Mark by Impact Level is determined to be **High**.

The information types that categorizes VAM as high are:

1) C.2.8.9 Personal Identity and Authentication Information with Availability as a high impact level due to the loss of Availability as the permanent loss of this information type would necessarily impede the ability of VA personnel to reliably match medical records to individual veterans thus disrupting medical care to those individuals which would negatively impact the VA mission of providing healthcare services to veterans and could potentially result in harm to veterans not receiving the correct healthcare on a timely basis.
2) D.14.4 Health Care Delivery Services Information Type the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life.

Signatures:

Information System Security Officer Signature Bobbi Dee Begay 168891 Digitally signed by Bobbi Dee Begay 168891 Date: 2018.08.21 14:35:29 -06'00'

Privacy Officer Signature RITA K GREWAL 114938 Digitally signed by RITA K GREWAL 114938 Date: 2018.08.21 16:09:14 -04'00'

Project Manager Signature Robert R. Rickard 294038 Digitally signed by Robert R. Rickard 294038 Date: 2018.08.27 15:00:10 -07'00'

System Owner Signature Robert R. Rickard 294038 Digitally signed by Robert R. Rickard 294038 Date: 2018.08.27 15:01:40 -07'00'