PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Informatics & Information Governance (OIIG)
Health Information Governance
National Data Systems

Expert Determination: Freedom of Information Act Court Settlement

Date: ***June 6, 2016***
OIIG Identifier- ***HIG16-46***
PWS Version Number: ***2.1***

Contents

1.0 BACKGROUND

The Veterans Health Administration (VHA) is home to the United States' largest integrated health care system consisting of 150 medical centers, nearly 1,400 community-based outpatient clinics, community living centers, Vet Centers and Domiciliaries. Together these health care facilities and the more than 53,000 independent licensed health care practitioners who work within them provide comprehensive care to more than 8.3 million Veterans each year.

VHA uses a nationally recognized electronic health record and stores most of its health data in local instances, but most of this health data is available at the national level through either legacy information technology systems, and in particular in the form of SAS™ data sets, or through its new Corporate Data Warehouse (CDW).

VHA receives many Freedom of Information Act (FOIA) requests for data reports. Although most requests are for aggregate data, VHA has received request for patient level data. In 2013, VHA received two record level data requests. VHA argued it could not provide the data, but through a lawsuit (Court case No. 13-cv-12591, Baser v. Department of Veterans Affairs) and subsequent Stipulation for Compromise Settlement, VHA agreed to provide 15 data sets per fiscal year covering fiscal years 2010 – 2015. The data was de-identified according to HIPAA Expert Determination.

As part of the continuation of the Stipulation for Settlement, VHA seeks an HIPAA Expert Determination to provide guidance how to properly de-identify health data for additional fiscal years beyond fiscal year 2015, especially with the implementation of International Classification of Disease (ICD) Version 10 on October 1, 2015..

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
2. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
3. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
4. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", October, 28, 2015
5. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

3.0 SCOPE OF WORK

The Contractor shall examine the current data request and determine if the data may be statistically de-identified. Provide to NDS any statistical disclosure limitation requirements, conditions, and steps necessary to implement the recommended statistical de-identified methodology. The Contractor shall then author and provide a final HIPAA Expert Determination of De-Identification of Data Report outlining the de-identification determination of the datasets in compliance with the Expert Determination Method at 45 C.F.R. § 164.514(b)(1)(i-ii). The Contractor shall participate in discussions with NDS and the Data Requestor to explain data constraints.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The PoP shall be 6 months from date of award.

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their Task Execution Plan submission.

4.3 TRAVEL

Not applicable.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the mandatory tasks and provide the specific deliverables described below within the performance period stated in this Performance Work Statement. If for any reason, any deliverable cannot be delivered on time according to the below schedule, the Contractor shall provide a written explanation to the Program Manager, Contracting Officer Representative and Contracting Officer as soon as discovered, but not later than three days prior to deliverable due date. This written transmittal shall include a firm commitment of when the work shall be completed. This transmittal shall cite the reasons for the delay, and the impact on the overall project.

5.1 EXAMINE DATA REQUEST

5.1.1 Examine requested data by Data Requestor and determine whether the data could be considered statistically de-identified under the Expert Determination method found at Section 164.514 of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA Privacy Rule”).

5.1.2 **Deliverable**: Formal confirmation in a brief letter addressed to Director, National Data Systems, indicating requested data may be de-identified. Due 30 days after fiscal year 2016 data is available and VA receives request from Data Requestor

5.2 PROVIDE DE-IDENTIFICATION INSTRUCTIONS

Provide to National Data Systems any statistical disclosure limitation requirements, conditions, and steps necessary to implement the recommended statistical de-identified methodology.

5.2.1 **Deliverable**: Written instructions detailing the steps NDS must take to implement data de-identification. Due 30 days after Examine Data Request completed.

5.3 HIPAA EXPERT DETERMINATION DATA REPORT

5.3.1 Prepare and provide to National Data Systems a final HIPAA Expert Determination of De-Identification of Data Report outlining the de-identification determination of the datasets in compliance with the Expert Determination Method at 45 C.F.R. § 164.514(b)(1)(i-ii). The report shall include all redactions, limitations, restrictions, and recommendations.

5.3.2 Report shall address the range of fiscal years of data to which the Report applies. In particular, would the Report, if implemented by VHA correctly, be valid for fiscal year 2017, 2018, and beyond**.**

5.3.3 Report shall address when a new patient-unique identifier is created taking into consideration previously released fiscal years. For example, if fiscal year 2016 begins with resetting/creating new patient identifiers because it is the first fiscal year with ICD-10 diagnosis and procedure coding, the report shall recommend how many fiscal years the same patient identifier may be used. VHA began using ICD-10 diagnosis and procedure codes on October 1, 2015, and no longer assigns the ICD-9 version of diagnosis and procedure codes.

5.3.4 **Deliverable**: Participate in up to six (6) two (2) hour meetings with National Data Systems and data requestor to discuss general recommendations and seek clarifications on content contained in HIPAA Expert Determination of De-Identification.

5.3.5 **Deliverable**: Report required by this task. This report is due no later than 120 days from time of initial assignment unless another timeline has been agreed to by all impacted parties.

6.0 GENERAL REQUIREMENTS

6.1 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract.

6.2 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word, MS Excel, MS PowerPoint, MS Project, MS Visio and Adobe Postscript Data Format (PDF).

6.3 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance

A. Quality of Product	1. Demonstrates understanding of VHA health data complexity. 2. Considers impact of previously released VHA health data to data requestor. 3. Recommends solution for de-identification that may be extended beyond FY16. 4. Accounts for injury and diseases unique to Veterans 5. Provides solution that would be acknowledged and accepted by US. Department of Health and Human Services, Office of Civil Rights, as authoritative.	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.4 FACILITY/RESOURCE PROVISIONS

Not applicable.

6.5 GOVERNMENT FURNISHED PROPERTY

Not applicable

6.6 SHIPMENT OF HARDWARE OR EQUIPMENT

Not applicable.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor’s information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA’s sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality

assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B3. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third

party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B4. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b. The Contractor/Subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B5. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. Within 10 workingday's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

SCHEDULE FOR DELIVERABLES

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

Task	Deliverable ID	Deliverable Description
5.1	5.1.2	**Examine Data Request** Due Thirty (30) days after fiscal year 2016 data is available and VA receives request from Data Requestor. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.2	5.2.2	**Provide De-Identification Instructions** Due Thirty (30) days after Examine Data Request completed. Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.3	5.3.4	**HIPAA Expert Determination Data Report** Draft plan is due Forty (40) days after completing Provide De-Identification Instructions; Final plan is due Ten (10) days after receipt of Government comments. Participate in meetings as necessary both with Data Requestor and Government. Electronic submission to: VA PM, COR, CO Inspection: (select one) origin/destination Acceptance: (select one) origin/destination
5.3	5.3.5	**Participate in 6 meetings both with Data Requestor and Government.** Electronic submission to: VA PM, COR, CO Inspection: (select one) origin/destination Acceptance: (select one) origin/destination