Initial Operating Capability Site Memorandum of Understanding



<Month><Year>

Version *<#.#>*

Department of Veterans Affairs

This template contains a paragraph style called Instructional Text. Text using this paragraph style is designed to assist the reader in completing the document. Text in paragraphs added after this help text is automatically set to the appropriate body text level. For best results and to maintain formatting consistency, use the provided paragraph styles. Delete all instructional text before publishing or distributing the document.

This template conforms to the latest Section 508 guidelines. The user of the template is responsible to maintain Section 508 conformance for any artifact created from this template.

Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Place latest revisions at top of table.

The Revision History pertains only to changes in the content of the document or any updates made after distribution. It does not apply to the formatting of the template.

Remove blank rows.

Table of Contents

[Initial Operating Capability Site Memorandum of Understanding 1](#_Toc435621732)

[Initial Operating Capability Site Profile Template 4](#_Toc435621733)

[Point of Contact Information 4](#_Toc435621734)

[Other IOC Agreements: 5](#_Toc435621735)

[Initial Operating Capability Evaluation Success Criteria Example (VistA) 5](#_Toc435621736)

[Patch or Software Name 5](#_Toc435621737)

[Table of IOC Evaluation Success Criteria 5](#_Toc435621738)

[Category/Criteria/Metric 5](#_Toc435621739)

[Performance 5](#_Toc435621740)

[Scope 6](#_Toc435621741)

[Data Quality 6](#_Toc435621742)

[Stakeholder Acceptance 6](#_Toc435621743)

[Initial Operating Capability Evaluation Success Criteria Example (HealtheVet) 7](#_Toc435621744)

[Patch or Software Name 7](#_Toc435621745)

[Table of IOC Evaluation Success Criteria 7](#_Toc435621746)

[Category/Criteria/Metric 7](#_Toc435621747)

[Performance 7](#_Toc435621748)

[Scope 8](#_Toc435621749)

[Data Quality 8](#_Toc435621750)

[Configuration 8](#_Toc435621751)

[Compliance 8](#_Toc435621752)

[Stakeholder Acceptance 9](#_Toc435621753)

[Released and Unreleased Dependencies Template 10](#_Toc435621754)

[Released Dependencies: 10](#_Toc435621755)

[Unreleased Dependencies: 10](#_Toc435621756)

[Data Transfer Agreement Guidelines 11](#_Toc435621757)

[Data Transfer Agreement Template 12](#_Toc435621758)

[Agreement for Data Exchange Between Product Development in the Office of Information and Technology and *<Insert Outside Agency Name>* 12](#_Toc435621759)

[Purpose: 12](#_Toc435621760)

[Terms of the Agreement: 12](#_Toc435621761)

[Data Transfer Agreement Example 16](#_Toc435621762)

[Example Agreement for Exchange Between Product Development in the Office of Information and Technology (OIT) and Wellknot Medical Systems 16](#_Toc435621763)

[Purpose: 16](#_Toc435621764)

[Terms of the Agreement: 16](#_Toc435621765)

[Software/Patch Information for Change Control Board (CCB) Template 20](#_Toc435621766)

[Section I –Software/Patch Information 20](#_Toc435621767)

[Section II – Impacts 20](#_Toc435621768)

[Section III – Cross Dependencies 21](#_Toc435621769)

[Section IV– Supporting Documents 21](#_Toc435621770)

# Initial Operating Capability Site Memorandum of Understanding

**Department of Veterans Affairs Memorandum**

Date: <Insert date>

From: Director, Software Development Services

Subj: Initial Operating Capability Evaluation of <Insert patch or software>

To: Director <Site name and location> or (Bay Pines VAMC) (Station ID#00) <City, State>

We are pleased to have your facility join us as an Initial Operating Capability (IOC) Evaluation site for the <system/application name> software project. <insert what functionality/or benefit is provided by the software being tested>.

As an IOC Evaluation site installing and implementing evaluation software, your facility will assume a key role in the release process, which is an essential step in the development of software that will be utilized nationally throughout the Department of Veterans Affairs. Your site will also serve to test the installation of the software in a production environment to ensure its compatibility with other Legacy VistA and/or HealtheVet VistA packages.

The <project name> Development Team agrees to the following responsibilities:

1. If sensitive data is being transferred, a Data Transfer Agreement (DTA) is required. Product Development (PD) will agree to and sign a DTA with the IOC site staff before any exchange of sensitive data is performed.
2. The Development Manager will verify with the [VHA Privacy Office](mailto:IACH9@med.va.gov) that the national Business Associate Agreement (BAA) provides sufficient coverage for the activities performed in the MOU.
3. We will work with your Office of Information and Technology (OIT) and <respective service> staff as the primary support for the <system/application name> software during the test period. Support will be provided via telephone, including dial-in service to your computer system if necessary. We may opt to use available tools (e.g., Kernel) to monitor testing at your site. You can be assured that appropriate respect for the sensitivity and value of your site's database will be given and that absolute discretion will be observed. Staff will sign all necessary security agreements with your site. Conference calls will be scheduled on a regular basis to promote an ongoing dialog throughout the testing phase.
4. Evaluation of this software may include other software which contains critical dependencies. These dependencies are split into two lists and are described below.
5. Released Dependencies. This includes software that has passed all testing for implementation nation-wide. It may include required tools from the PD HealtheVet VistA Toolset, monitoring software, services, integrated software, or something else. These are not part of testing, as they are already approved for national use.
6. Unreleased Dependencies. This includes software that has not undergone testing and is not yet approved for nation-wide implementation. These dependencies may include required tools from the [OIT HealtheVet VistA Toolset](http://vista.med.va.gov/vistaarch/healthevet/Documents/Tools-List-Extended.doc) monitoring software, services, integrated software, or other dependencies. The list of unreleased dependencies is part of this field test.
7. Provide the list of [Released and Unreleased Dependencies](#_Released_And_Unreleased).
8. In the event of the participants needing elevated privileges, all participants in the project will follow the VA and OIT change management process and approvals. It is noted regional process might differ across the regions.

As a test site, we are asking VHA accept the following responsibilities:

1. Agree to and sign a DTA with Development staff before any exchange of sensitive data is performed.
2. .
3. Evaluate all system/application functionality.
4. Assist the Development Team in validating the functionality of the software and the accuracy of all reports produced by the package.
5. Review and comment on the <documentation manuals> documentation produced for this package.
6. Report all problems to the Development Team promptly, with as much detail as possible, to ensure that the situation may be promptly addressed and corrected.
7. Participate in periodic conference calls.
8. <Include any additional responsibilities.>

As a test site, we are asking Field Operations to accept the following responsibilities:

1. Install all software related to this <new functionality/functionality enhancement>as promptly as possible, including all of the dependency software. PD understands and endorses the installation of new software into a test environment on your VistA system as a preliminary condition to the installation of that software into your production, or live, accounts. However, to ensure prompt resolution of problems and to ensure a complete test, the software must be placed into a production environment within <*#*> working days of receipt
2. Report all problems to the Development Team promptly, with as much detail as possible, to ensure that the situation may be promptly addressed and corrected.
3. Participate in periodic conference calls.

In addition, we ask that you meet the following conditions:

1. Allow access to your system by the Development Team to support the research and resolution of problems. The details of this access will be worked out with your OIT staff. The contacts for this software are:
2. <Insert Development Manager's name, title, and phone number>
3. <Insert the assigned Development Team member names, titles, and phone numbers>
4. These individuals can be reached through FORUM or Microsoft Outlook. They can also be reached via telephone at the numbers listed above. If there is a problem, it is vital that one of the developers be contacted as soon as possible with as much detail as possible to identify the problem and correct it.
5. Load patches on existing hardware. No additional hardware is required. Use the software exactly as provided. To support you in the evaluation, the development team makes all necessary modifications to the software. Any emergency fixes made by the site must be reported to this office immediately. During evaluation, **local enhancements must not be implemented** in order to preserve the reliability and integrity of the test.
6. Provide complete security of this software, including all of the conditions stipulated in the signed DTA related to this Memorandum of Understanding (MOU), until it has been released nationally. Therefore, no copies of the routines, files, or data dictionaries may be released without the written consent of PD. Final disposition/disposal of the software will be followed as stipulated by the signed DTA related to this MOU. We are confident that you will treat the software in such a manner and will inform us immediately of any possible breaches in this security.
7. <Include any additional responsibilities>

Recent experiences on a variety of software packages system-wide have served to emphasize the degree of importance of conducting thorough and timely evaluation of software before release. You are requested to discuss this evaluation with the Service Chiefs of the individuals in the positions identified on the enclosed Test Site Profile so that all affected parties may reach an understanding of the impact the test may have on your medical center and the resources that may be necessary to accomplish tasks. Respond directly on the e-mail (not in the document) with any additional information or corrections that need to be made to the IOC Site Profile.

We look forward to working with your staff in the successful implementation of this product. This agreement will cover the life of the test cycle. Questions regarding the requirements outlined in this memorandum should be directed to <Development Manager’s name> at <Development Manager’s phone number>.

Approval to be obtained by QA Program Coordination Group.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Director Software Development Services

Attachments: IOC Site Profile

IOC Evaluation Success Criteria

cc: VISN <##> Chief Information Officer (CIO),

Product Support Team Manager, Product Support Team <Insert Name>

# Initial Operating Capability Site Profile Template

<Software Name>

Have a member of the Office of Information and Technology (OIT) staff review the information in this Initial Operating Capability (IOC) Site profile. Respond directly on the e-mail (not in the document) with any additional information or corrections that need to be made to the test site profile.

|  |  |
| --- | --- |
| **Site Name:** | <Insert Initial Operating Capability Site name, City, State> |
| **Telnet Address:** | <Insert Telnet Address> |
| **Operating System:** | <Insert Operating System> |

## Point of Contact Information

Point of Contact Information may have been obtained via a site questionnaire. If so, confirm that the information below is correct. Otherwise, provide the points of contact for each of the service areas impacted by the functionality outlined in this Memorandum of Understanding (MOU).

| Service/Application | Name | Phone Number |
| --- | --- | --- |
| <Insert each point of contact’s information> |  |  |
|  |  |  |
|  |  |  |

## Other IOC Agreements:

# Initial Operating Capability Evaluation Success Criteria Example (VistA)

## Patch or Software Name

This Memorandum of Understanding (MOU) contains measurable criteria used to declare that the 10-10EZ Online Processing Phase 2.5 Project is successful. This project will be successful when a 10-10EZ application is submitted via the web, routed through forum to the veteran-selected facility and processed into VistA.

Specifically in VistA:

1. New data elements collected are made available for review, edit, acceptance and filing into the local VistA patient database via the Enrollment Application System (EAS).
2. New data elements are printed on the EAS system-generated 10-10EZ form, which is sent to the veteran for signature.
3. Obsolete data elements are excluded from review, edit, acceptance, and filing into the local VistA patient database.
4. Obsolete data elements do not print on the EAS system-generated 10-10EZ form.

## Table of IOC Evaluation Success Criteria

### Category/Criteria/Metric

#### Performance

Real time data transfer – Performance of Web

* Allows entrance and submission of a 10-10EZ application.
* Bundles data into two e-mail messages; one is a simple listing of data, easily readable and intended for staff members; the other is a formatted data dump which is processed into the holding file by the 10-10EZ software.
* Provides the correct address and fax number for parent VA facilities.

Real time data transfer – Performance at Forum

* Routes all web applications to the target facility
* Monitors receipt to the field facility
* Logs Remedy request on behalf of field facility for transmission problems

Real time data transfer – Performance at VistA

* Mail message is received by the VA10-10EZ Mail Group and is viewable/printable.
* Enrollment/Registration staff is able to perform the various functions of the EAS application, and to process the application into VistA if appropriate to assist with the completion of the registration process and print the 10-10EZ form.
* Fileman validity checks are performed during the filing process. A mail message is sent as appropriate and available for follow-up by Enrollment/Registration staff.

#### Scope

Data storage – VistA

* E-mail transmissions received from the web server via GATEWAY.FORUM will be stored in the 1010EZ HOLDING file (#712) indefinitely. Once processed, via the EAS, the data values are also filed within the VistA patient file(s), Means test file, and the Insurance file.

Data storage – Forum

* Retains Mail Basket with vaporization date of 180 days;
* Receives acknowledges messages from the VistA facilities, places in ACK Mail Basket with vaporization within 14 days;
* Receives daily Submissions List messages from web server, places in LIST Mail Basket with vaporization set to 14 days.

#### Data Quality

Mapped data

* All data fields map to a VistA storage location appropriately.

#### Stakeholder Acceptance

By the VistA system

* Sign off in Forum from each test site Point of Contact indicating concurrence that the Project was successful.

# Initial Operating Capability Evaluation Success Criteria Example (HealtheVet)

## Patch or Software Name

This Memorandum of Understanding contains measurable criteria used to declare that the HDR Prototype is successful. The table contains the criterion measure, the metric and the evaluator who will determine that the measure has been satisfied. The next paragraph is a “plain-English” summary of the measures presented in the table.

A successful prototype will show real-time transmission and storage of clinical data into the oracle HDR database in the Corporate Data Center Operations (CDCO). The data will be sent from your VistA database and will be selected data elements from twelve distinct clinical domains. A bulk load of two years’ worth of clinical data from those twelve domains is stored in the database for all active patients in the system. A determination of the most efficient method of the bulk loading process is a part of the success of the project. Real-time data stored as a result of event triggers from VistA based transactions must have a high level of data quality, meaning that data is stored with the correct patient, with the correct date and time identifier, and in the correct clinical location. Any patient safety issues identified in the testing phase that are associated with the data storage shall be resolved before the prototype is declared a success. Bulk loading and real-time data processing and storage must exist in the prototype stage without major gaps in stored data or availability, and without major data quality problems. At the end of the 30-day period, success concurrence will be sought from VHA OI leadership and from the management team at your site.

## Table of IOC Evaluation Success Criteria

### Category/Criteria/Metric

#### Performance

Bulk Load

* 2 years’ worth of bulk patient clinical data is stored in the HDR from each site, the process of bulk loading will take less than one week to complete

Real Time Data Transfer – Performance at VistA System

* CPRS cover sheet load time is lengthened by less than 2 seconds when all maintenance triggers related to the prototype are installed and functioning
* CPU processor time is less than 10% affected when all maintenance triggers are installed and functioning
* Real time data transfer occurs for at least 30 calendar days without an unscheduled break in service of more than one day

Real Time Data Transfer – Performance at Interface Engines

* Every HL7 message generated by the HDR software is processed by the local interface engine

Real time data transfer – impact on WAN

* Every HL7 message generated by the local interface engine is communicated over the WAN to the enterprise IE in ACC.

Real time data transfer – Performance at CDCO

* Processing of all messages and storage of all data at CDCO HDR is completed within one hour of processing through enterprise interface engine

#### Scope

Data storage – what data is stored

* Pharmacy, Allergies and Vitals data are fully mapped and stored in the HDR via the data plug-ins
* Demographics, Laboratory are fully mapped and stored in the HDR via the 3M ASN.1 standard
* TIU, Radiology, encounters, health factors and problem list are stored as “loosely coded” text (meaning a lower degree of normalization)
* Orders are stored as text (all order states)
* All domains use the data plug-ins as a storage mechanism

Windows

* One of the three sites is a Windows site

VMS Cache Site

* Two of the three sites are VMS Cache sites

#### Data Quality

Mapped Data

* A statistically significant sample of all data in each mapped domain is certified via IV&V process

Data stored as text

* A statistically significant sample of all data is each non-computational domain is certified via IV&V process

#### Configuration

HDD/MMI

* Demographics for patients with national ICNs stored in HDR

#### Compliance

VHA HL7 v2.4

* All messages are certified and accepted by VHA

#### Stakeholder Acceptance

By the VistA System

Signed statement from all prototype site leadership team (Director, COS, Associate Director) indicating concurrence that the prototype project was successful

# Released and Unreleased Dependencies Template

<Insert patch or software>

Initial Operating Capability (IOC) Evaluation of this software may include other software which contains critical dependencies. These dependencies are split into two lists and are described below.

* Released Dependencies. This includes software that has passed all testing for implementation nation-wide. It may include required tools from the OIT HealtheVet VistA Toolset, monitoring software, services, integrated software, or something else. These are not part of testing, as they are already approved for national use.
* Unreleased Dependencies. This includes software that has not undergone testing and is not yet approved for nation-wide implementation. These dependencies may include required tools from the OIT HealtheVet VistA Toolset monitoring software, services, integrated software, or other dependencies. The list of unreleased dependencies is part of this field test.

Replace the example dependencies below with your release and unreleased dependencies. If there are no dependencies, indicate a negative response for either or both.

## Released Dependencies:

* VistALink
* SDS

## Unreleased Dependencies:

* KAAJEE (see attached criteria for testing)

# Data Transfer Agreement Guidelines

Data Transfer Agreements (DTAs) are to be in place whenever there is sensitive data involved in a transfer with an agency or department external to the Office of Information and Technology (OIT) (see [Displaying Sensitive Data Guide](http://vaww.oed.wss.va.gov/process/Library/displaying_sensitive_data_guide.docx) for the definition of sensitive data).

Approach the need for a DTA as a risk assessment. It is a matter of assessing the risk comfort level for the data’s use and mitigating it via the DTA.

Based on the information in a Memorandum of Understanding (MOU), ask these questions:

* Who will have access and control of the data?
* How much accountability needs to be in place before the data is transferred?
* What is the risk of misuse?

The DTA is designed to formalize the rules as to how the data is controlled based on the answers to those questions. The DTA then covers the accountability and control issues in terms of:

* How the Data is to be used
* To whom the data is disclosed (who is authorized to use it)
* How the data is to be transmitted or transferred
* Where the data is to be stored and controlled
* How long the data will be made available
* How the data is it is to be disposed or returned at the termination of the MOU with an agency, company, department, or entity outside of OIT.

All data that is transferred outside of OIT must comply with the directives listed in the DTA.

* An example of a completed DTA can be found here.
* Agreement to the conditions of the DTA by all parties must be accomplished through faxed hardcopy signature of the DTA document and become part of the permanent project’s records in the project’s documentation folder (e.g., TSPR, ClearQuest, etc.).

What constitutes a ‘**transfer’**? A transfer occurs when someone or some area outside of a project or department has been given some level of control (meaning the ability to read, capture, change, modify, or delete) over that project’s or department’s data. The DTA spells out the conditions for the transfer of control and how the data is to be used.

As a best practice – Information Security Officers and Privacy Officers should regularly review these agreements.

# Data Transfer Agreement Template

## Agreement for Data Exchange Between Product Development in the Office of Information and Technology and <Insert Outside Agency Name>

### Purpose:

This Agreement establishes the terms and conditions under which the <insert name> will provide, and <insert name> will use the data to <be very specific in why data is being shared, and state the method of transfer and how that will be accomplished>.

Any other uses will be subject to prior approval by the <transferring agency Directors>.

### Terms of the Agreement:

1. This Agreement is by and between the <insert name> and <insert name> (Owner), a component of the U.S. Department of Veterans Affairs (VA).
2. This data transfer agreement covers the transfer and use of data by the <insert name> and <insert name>, for the project specified in this agreement. This Agreement supersedes any and all previous data.
3. The terms of this Agreement can be changed only by a written modification of the agreement by the agency signatories (or their designated representatives) to this Agreement or by the parties adopting a new agreement in place of this Agreement.
4. The <transferring agency> retains all ownership rights to the data file(s) and VA retains all ownership rights to the VA data file(s) provided to you under this Agreement.
5. The <insert user name> will be designed as custodians of the VA data for the <user name> and will be responsible for complying with all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use and disclosure of the Owner’s data provided under this agreement. The User agrees to notify the Owner within fifteen (15) days of any change of custodianship.

Technical Representative for <Transferring Agency>

<Insert Name and Phone Number>

Custodian for <User Agency>

<Insert Name and Phone Number>

1. The following named individuals are designated as their agencies’ Points of Contact for performance of the terms of the Agreement.

Point-of-contact on behalf of <Transferring Agency>

<Insert Name and Phone Number>

Point-of-contact on behalf of <User Agency>

<Insert Name and Phone Number>

1. Except as Product Development (PD) shall authorize in writing, the User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the Office of Information and Technology (OIT) data covered by this Agreement to any person outside the <User Agency>. The User agrees that, access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to Owner’s data to perform this Agreement.
2. The parties mutually agree that any derivative data or file(s) that is created from the original data may be retained by the User until the project specified in this Data Transfer Agreement (DTA) has been completed. The use of the data will be for the time period covered by the <Insert MOU or Proposal Name> <Insert Time Frame>. At the end of this period <insert terms of agreement for return or data, destruction of data or renewing agreement> you are authorized to keep the data on your system in a secure encrypted partition in accordance with Federal Information Processing Standards (FIPS) 140-2 validation.
3. The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the Owner will notify the User to destroy or return such data at Users expense using the same procedures stated in the above paragraph of this section.
4. The User will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the Owner’s data and to prevent unauthorized use or access to it. VA sensitive information must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be validated by National Institute of Standards and Technology (NIST) to meet the currently applicable version of FIPS 140 (See <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm> for a complete list of validated cryptographic modules). Only approved encryption solutions using validated modules may be used when protecting data during transmission. Additional security controls are required to guard VA sensitive information stored on computers used outside VA facilities. All VA data must be stored in an encrypted partition on the hard drive and must be encrypted with FIPS 140 validated software. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. Further, the User agrees that the data must not be physically moved or transmitted in any way from the site indicated in item number 5 without first being encrypted and obtaining prior written approval from the data owner.

* If the data user becomes aware of the theft, loss or compromise of any device used to transport, access or store VA information, or of the theft, loss or compromise of any VA data, the user must immediately report the incident to his or her supervisor. That supervisor must within one hour inform the <Fill in VA Information Security Officer and the Director names and phone numbers>. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements for responding to security incidents.

1. The authorized representatives of OIT and the Inspector General will be granted access to premises where the data are kept by the User for the purpose of confirming that the User is in compliance with the security requirements.
2. No findings, listing, or information derived from the data, with or without identifiers, may be released if such findings, listing, or information contain any combination of data elements that might allow the deduction of a veteran without first obtaining written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement. Examples of such data elements include but are not limited to social security number, geographic indicator, age, sex, diagnosis, procedure, admission/discharge date(s), or date of death. The Owner shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from its files provided under this Agreement identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual. The Owners’ review of the findings is for the sole purpose of assuring that data confidentiality is maintained and that individuals cannot be identified from the findings. The Owner agrees to make this determination about approval and to notify the User within two weeks after receipt of findings. The Owner may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual.
3. The User may not reuse the Owner’s original or work file(s) for any other purpose.
4. In the event that the Owner determines or has a reasonable cause to believe that the User disclosed or may have used or disclosed any part of the data other than as authorized by this Agreement or other written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement, the Owner in its sole discretion may require the User to: (a) promptly investigate and report to the Owner the User’s determinations regarding any alleged or actual unauthorized use or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by the Owner, submit a formal response to an allegation of unauthorized disclosure; and (d) if requested, return the Owner’s data files to the Owner. If the Owner reasonably determines or believes that unauthorized disclosures of Owner’s data in the possession of User have taken place, the Owner may refuse to release further data to the User for a period of time to be determined by the Owner, or may terminate this Agreement.
5. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. §1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by §1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. §552a(i)(1)) may apply if it is determined that the User, or any individual employed or affiliated therewith, knowingly and willfully discloses Owner’s data. Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. §641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted.
6. All questions of interpretation or compliance with the terms of this Agreement should be referred to the OIT official names in item 18 (or their successors).
7. Authority for VHA to share this data for the purpose indicated is under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, is 45 CFR 164.512(k)(6)(ii), under the Privacy Act is routine use 30 in VA system of records, 121VA19, entitled National Patient Databases-VA and under 38 USC 5701(b)(3) and (e).
8. On behalf of both parties the undersigned individuals hereby attest that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Director, Software Development Services Date**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Facility CIO/IRM Chief Date**

<Organization Receiving Data Transfer>

# Data Transfer Agreement Example

## Example Agreement for Exchange Between Product Development in the Office of Information and Technology (OIT) and Wellknot Medical Systems

### Purpose:

This Agreement establishes the terms and conditions under which the AXP program will provide, and Wellknot Medical System will use the data to test alignment of Wellknot civilian based medical information with Veterans Administration veteran medical records. Test data limited to 200 veterans whose last name begins with the letter ‘G’. The data is needed to ensure the systems are compatible as part of a pilot program to expand the scope of veteran medical knowledge base. Data is to be transferred via tape cartridge - data to be Gutmann method 125 encrypted with a 24 bit key. Transfer to be provided by secured courier of VA’s choice.

Any other uses will be subject to prior approval by Michael Hecker, Program Executive Officer PEO (VHIT).

### Terms of the Agreement:

1. This Agreement is by and between the Wellknot Medical Systems and PD (Owner), a component of the U.S. Department of Veterans Affairs.
2. This data transfer agreement covers the transfer and use of data by the Wellknot Medical Systems and PD for the project specified in this agreement. This Agreement supersedes any and all previous data.
3. The terms of this Agreement can be changed only by a written modification of the agreement by the agency signatories (or their designated representatives) to this Agreement or by the parties adopting a new agreement in place of this Agreement.
4. The AXP program retains all ownership rights to the data file(s) and OIT retains all ownership rights to the OIT data file(s) provided to you under this Agreement.
5. The Operations Director - Wellknot Medical Systems will be designated as custodian of the VA data for the Pilot Project Test and will be responsible for complying with all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use and disclosure of the Owner’s data provided under this agreement. The User agrees to notify the Owner within fifteen (15) days of any change of custodianship.

Technical Representative for - AXP application - Jon Doe –

Senior Development Manager 727 - 555 -2356

Custodian for - Wellknot Medical Systems

Ed Coleman, Operations Director 505 - 555 -5678

1. The following named individuals are designated as their agencies’ Points of Contact for performance of the terms of the Agreement.

Point-of-contact on behalf of PD - Jon Doe –

Senior Development Manager 727 - 555 -2356

Point-of-contact on behalf of Wellknot Medical Systems - Data Service Center

Harry Welch - 505 555 – 8855.

1. Except as OIT shall authorize in writing, the User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the OIT data covered by this Agreement to any person outside the <Wellknot Medical Systems>. The User agrees that, access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to Owner’s data to perform this Agreement.
2. The parties mutually agree that any derivative data or file(s) that is created from the original data may be retained by the User until the project specified in this DTA has been completed. The use of the data will be for the time period covered by the MOU and this DTA for the AXP data pilot for a period not to exceed 90 days. At the end of this period, you will erase all OIT related data, purge all Wellknot databases of OIT data and return the original encrypted tape you are NOT authorized to retain any data.
3. The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the Owner will notify the User to destroy or return such data at Users expense using the same procedures stated in the above paragraph of this section.
4. The User will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the Owner’s data and to prevent unauthorized use or access to it. VA sensitive information must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be validated by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140 (See <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm> for a complete list of validated cryptographic modules). Only approved encryption solutions using validated modules may be used when protecting data during transmission. Additional security controls are required to guard VA sensitive information stored on computers used outside VA facilities. All VA data must be stored in an encrypted partition on the hard drive and must be encrypted with FIPS 140 validated software. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. Further, the User agrees that the data must not be physically moved or transmitted in any way from the site indicated in item number 5 without first being encrypted and obtaining prior written approval from the data owner.

* If the data user becomes aware of the theft, loss or compromise of any device used to transport, access or store VA information, or of the theft, loss or compromise of any VA data, the user must immediately report the incident to his or her supervisor. That supervisor must within one hour inform xxxx - VA Security Officer at (xxx) xxx-xxxx and the Assistant Deputy Chief Information Officer (CIO) – PD Program Management at (xxx) xxx- xxxx. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements for responding to security incidents.

1. The authorized representatives of OIT and the Inspector General will be granted access to premises where the data are kept by the User for the purpose of confirming that the User is in compliance with the security requirements.
2. No findings, listing, or information derived from the data, with or without identifiers, may be released if such findings, listing, or information contain any combination of data elements that might allow the deduction of a veteran without first obtaining written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement. Examples of such data elements include but are not limited to social security number, geographic indicator, age, sex, diagnosis, procedure, admission/discharge date(s), or date of death. The Owner shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from its files provided under this Agreement identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual. The Owners’ review of the findings is for the sole purpose of assuring that data confidentiality is maintained and that individuals cannot be identified from the findings. The Owner agrees to make this determination about approval and to notify the User within two weeks after receipt of findings. The Owner may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual.
3. The User may not reuse the Owner’s original or work file(s) for any other purpose.
4. In the event that the Owner determines or has a reasonable cause to believe that the User disclosed or may have used or disclosed any part of the data other than as authorized by this Agreement or other written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement, the Owner in its sole discretion may require the User to: (a) promptly investigate and report to the Owner the User’s determinations regarding any alleged or actual unauthorized use or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by the Owner, submit a formal response to an allegation of unauthorized disclosure; and (d) if requested, return the Owner’s data files to the Owner. If the Owner reasonably determines or believes that unauthorized disclosures of Owner’s data in the possession of User have taken place, the Owner may refuse to release further data to the User for a period of time to be determined by the Owner, or may terminate this Agreement.
5. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. §1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by §1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. §552a(i)(1)) may apply if it is determined that the User, or any individual employed or affiliated therewith, knowingly and willfully discloses Owner’s data. Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. §641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted.
6. All questions of interpretation or compliance with the terms of this Agreement should be referred to the VHA official name in item 18 (or his or her successor).
7. Authority for VHA to share this data for the purpose indicated is under the HIPAA Privacy Rule, is 45 CFR 164.512(k)(6)(ii), under the Privacy Act is routine use 30 in VA system of records, 121VA19, entitled National Patient Databases-VA and under 38 USC 5701(b)(3) and (e).
8. On behalf of both parties the undersigned individuals hereby attest that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Director, Software Development Services Date**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Facility CIO/IRM Chief Date**

<Organization Receiving Data Transfer>

# Software/Patch Information for Change Control Board (CCB) Template

|  |  |
| --- | --- |
| **Project Name:** | <Fully spell out the project name and provide its acronym (e.g., Managing Scanning Failures [MSF]).> |
| **Portfolio Name:** | <Fully spell out the portfolio name (e.g., Health Provider System [HPS]).> |
| **Project Management:** | <Insert Name, Organization.> |
| **Date:** | <Insert the date found on the Memorandum of Understanding (MOU).> |

## Section I –Software/Patch Information

|  |  |
| --- | --- |
| **Date Decision Needed By:** | <Insert the date the Change Control decision is required by so that the project is not negatively impacted.> |
| **Software/Patch Description:** | < Provide a description of the changes the Software/Patch will introduce> |

## Section II – Impacts

|  |  |
| --- | --- |
| **Impact of Implementing Software/Patch:** | <Detail the specific impacts of implementing this Software/Patch.> |
| **Impact of NOT Implementing Software/Patch:** | < <Detail the specific impacts of not implementing this Software/Patch.> |
| **Clearly describe all impacts to other projects and the effect of this Software/Patch on those projects:** | <Detail the impacts to other projects.> |

## Section III – Cross Dependencies

| Name of project/organization | Relationship | Impact |
| --- | --- | --- |
| <List the name of the affected project and/or organization.> | <Describe its Relationship.> | <Describe the impact of the cross dependencies.> |

## Section IV– Supporting Documents

|  |  |
| --- | --- |
| **1.** |  |
| **2.** |  |
| **3.** |  |

Template Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| November 2015 | 1.7 | Updated link to Displaying Sensitive Data Guide and Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules | Process Management |
| May 2015 | 1.6 | Reordered cover sheet to enhance SharePoint search results | Process Management |
| October 2014 | 1.5 | Changed an organizational title from AAC to CDCO in 3 locations. | Process Management |
| March 2014 | 1.4 | Upgraded to MS Office 2007-2010 format, updated to latest ProPath documentation standards, and edited for Section 508 conformance. Modified content to clarify responsibilities. | Process Management |
| April 2012 | 1.3 | Standardized formatting | Process Management |
| March 2011 | 1.2 | Changed OI&T to OIT | Process Management |
| March 2011 | 1.1 | Updates to reflect changes to IOC | MInao Murphy |
| March 2011 | 1.0 | Initial Version | MInao Murphy |

Place latest revisions at top of table.

The Template Revision History pertains only to the format of the template. It does not apply to the content of the document or any changes or updates to the content of the document after distribution.

The Template Revision History can be removed at the discretion of the author of the document.

Remove blank rows.