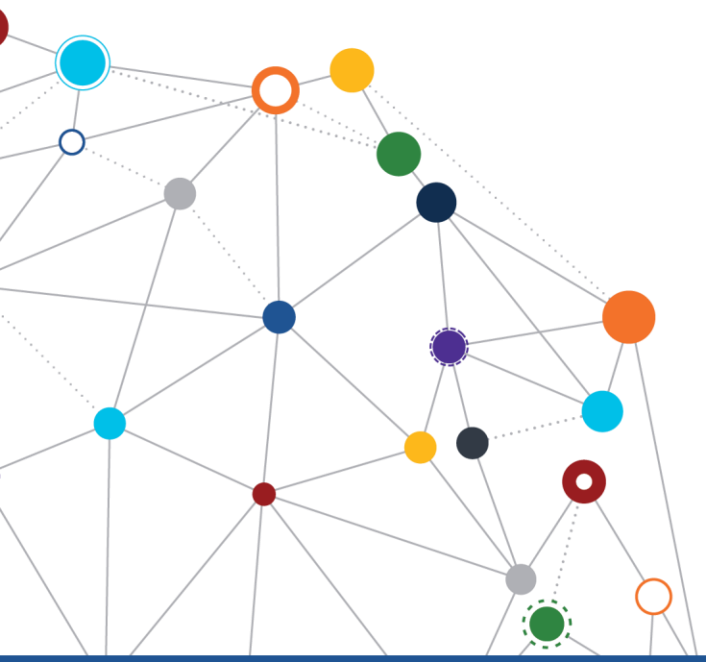
OFFICE OF
INFORMATION
AND TECHNOLOGY

3D Printing Enterprise Design Pattern

Data Security

July 2019 | Enterprise Program Management Office



VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	2/2019	3D Printing Segment 2: Data Security
2.0	6/2019	Updated to include description of capabilities that will be part of the immediate, interim, and future state; adjudication of stakeholder comments.

1 Context

Current practice at the Department of Veterans Affairs (VA) is to anonymize the personally Identifiable Information (PII) and protected health information (PHI) among the text included in the digital imaging and communications in medicine (DICOM) files, before sending them to a 3D printing software (SW) modeling tool for processing. The method used to remove or modify PII and PHI varies between a set of automated operations at some VA Medical Centers (VAMCs), and less effective manual operations at others.

2 Problem

The VA 3D Printing Advisory Committee has discussed maintaining PII/PHI within DICOM files and associated 3D data model files in the future as a measure to ensure Veteran patient traceability, a principal concern for patient safety. With 3D data models expected to be stored in an image repository for both the interim and future state, additional data security measures are necessary. The security of the PII and PHI that are contained in image files must be ensured when transporting files to and from the VA Enterprise Cloud (VAEC).[1] This includes consideration for how to delete PII and PHI from the 3D printer when it is replaced or removed from the VA premises.

Figure 1 illustrates three key pillars for establishing an agile architecture that can advance the current 3D printing technology landscape at VA, as the number of 3D printers increase in quantity at VA hospitals and facilities. Since VA requires enterprise guidance on the consistent security of PII and PHI for 3D printing, this Enterprise Design Pattern (EDP) document focuses on the area that is highlighted in red. Each pillar is addressed in a separate *3D Printing* EDP segment document.[2]

[1] Refer to the VAEC SharePoint Site at https://vaww.portal.va.gov/sites/ECS/SitePages/Home.aspx.
[2] Refer to the *3D Printing* EDPs at https://www.oit.va.gov/library/recurring/edp/index.cfm.

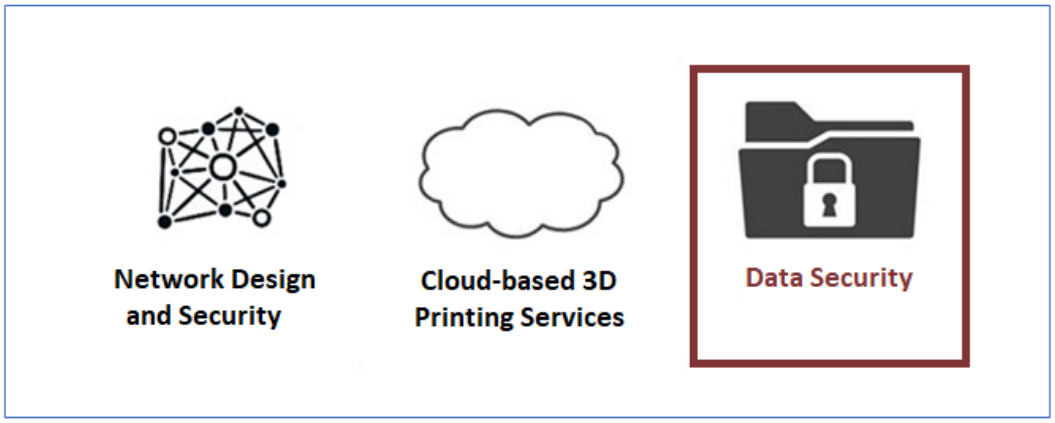


Figure 1: VA 3D Printing Pillars[3]

3 Approach

This section addresses solutions for the immediate, interim, and future state of 3D printing at VA.

3.1 Data in Motion/Data at Rest

Capability for the Immediate, Interim, and Future State

PII and PHI must be protected, whether in motion or at rest, in accordance with VA Handbook 6500, *Risk Management Framework for VA Information Systems*.[4] The following guidance addresses actions used to protect PII and PHI when using 3D printing.

- The system architect and network security administrator must ensure that image files containing PII and PHI utilize Transport Layer Security (TLS) when they are transmitted across the VA network and the VAEC.
- The system architect and network security administrator must ensure the use of Federal Information Processing Standards (FIPS) Publication 140-2 validated encryption[5] when files containing PII and PHI are stored.

[3] Source: Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) Enterprise Design Pattern (EDP) Team from information obtained from VA Subject Matter Experts (SMEs).
[4] Refer to VA Handbook 6500, *Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program*, March 10, 2015. at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.
[5] Refer to FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, a computer security standard authored by the National Institute of Standards and Technology (NIST) that is used to approve cryptographic modules, at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf. The Initial publication, dated May 25, 2001, was last updated on December 3, 2002.

- PII/PHI must be erased from the 3D printer memory when the printer is removed from the VA premises by utilizing a SW-based data sanitization method. SW-based data sanitization tools must be compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 Revision 1 guidelines.[6]
- SW-based data sanitization tools must be approved (or approved "with constraints") by the VA Technical Reference Model (TRM).[7] Contact the 3D Printing Advisory Committee if compliance cannot be met.

3.2 Anonymization

Capability for the Immediate, Interim, and Future State

Anonymization is the primary method currently utilized to protect PII and PHI that is contained within image files.[8] To ensure that anonymization is implemented in a timely and uniform manner, the system architect must ensure that the process is *automated*. Options to automate this process include the use of existing DICOM viewers that have an anonymization capability built into the system; and separate DICOM anonymization tools.

3.3 Data Loss Prevention

Capability for the Interim and Future State

An internal image repository, hosted on the VAEC to help enhance collaboration between doctors, contains data that must be properly protected. Additional security layers should be established to ensure the control of data in the repository, extending beyond the access permissions that are established through role-based access control (RBAC).

- The system architect and network security administrator should ensure the use of a data loss prevention (DLP) tool to monitor data moving into, residing, and departing from the image repository.
  - The DLP tool should restrict the movement of 3D printing model files (1) to and from the image repository, and (2) to computers that host the print preparation SW that is connected to the 3D printers.

[6] Refer to NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, February 5, 2015, at https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization.
[7] Refer to the VA TRM to identify approved applications and standards on the internal VA network at http://trm.oit.va.gov/. External vendors may utilize a less comprehensive site at https://www.oit.va.gov/services/trm/.
[8] Anonymization is defined as the process that removes the association between the identifying dataset and the data subject (NISTIR 8053 – De-Identification of Personal Information).

- The system architect and network security administrator must ensure that the DLP tool is able to detect violations of security data policies and trigger an enforcement response. The enforcement responses include the following:
    - Alert & Log – This option allows the file to be transferred, while a log entry of the transaction is recorded, and a notification is sent to a designated person (e.g. the data owner, a 3D printing administrator).
    - Block – This option stops the file transfer and sends a notification. It is essential to carefully test this capability because it disrupts the workflow.
    - Encrypt – This allows the file transfer, but only after the file is encrypted. The requesting party must have the means to decrypt the file for use.

3.4 Integrity Checking

3.4.1 File Integrity Checking

Capability for the Immediate, Interim, and Future State

When 3D printing activities are internal, there is assurance that VA will provide security for 3D print files. Conversely, if some 3D print jobs are outsourced, the ordering physician should ensure that verification of the 3D model file is performed. Design specifications, manufacturing parameters, and materials should be confirmed as correct prior to printing.

3.4.2 Physical Model Integrity Checking

Capability for the Immediate, Interim, and Future State

Verifying the physical object is also essential due to the potential risk associated with hacking the 3D printer's firmware, with the intent to introduce changes that will cause failure to parts.

- The technician should utilize a form of physical model integrity verification (e.g. acoustic, spatial, or materials verification) to ensure that the model is accurate.
    - Currently, there are no standards for physical model integrity verification; however, there are resources published by VA doctors that describe various verification techniques.[9]

Compliance with the standards outlined in Section 3 of this document applies to the following scenarios:

- Storing or accessing image files from the image repository
- Removing a 3D printer from the VA premises
- Initiating a request for a 3D print model

[9] Refer to *3D Printing in Medicine* at https://threedmedprint.biomedcentral.com/articles/10.1186/s41205-019-0043-1.

4 Use Case

The following use case illustrates how the *data security guidance* from Section 3 of this document can function with the 3D cloud-based services that are described in the *3D Printing* Segment 2 EDP, *Cloud-based 3D Printing Services*.[10]

4.1 Storing and Accessing Data Images from the Internal 3D Printing Repository – Immediate Solution

Assumptions

- Whenever a new image is stored to the VistA Imaging System, a copy will be sent to the Image Repository.
- The segmentation and printing will be performed at the same VA hospital/facility.
- The technician is part of the 3D printing user group and has proper RBAC permissions to access the 3D printing SW tools (i.e., segmentation SW, 3D Print Job Management System) and the image repository.

Use Case Description

- The technician logs in to the segmentation SW tool that is hosted on the VAEC.
- The technician utilizes the SW tool's DICOM Query/Retrieve (Q/R) capability to retrieve the DICOM file from the image repository.
- The connection between the image repository and the segmentation SW tool that is hosted on the VAEC is secured using TLS.
- The technician generates a 3D model that is suitable for printing, using the SW modeling tools hosted on the VAEC.
- The technician sends the 3D model and associated native files, such as stereolithography (STL)[11] and computer-aided design (CAD), to the image repository for storage.
- The DLP server examines the 3D model and associated native files for PII/PHI data, replaces this data with an identifier that links the model to the patient, and stores and encrypts the relation between the PII/PHI data and the identifier.
- The 3D model and associated native files, such as STL, CAD, etc., are stored in the:
    - Image repository
    - VistA Imaging (to maintain a copy with the patient's EHR)
- The technician accesses the image repository and downloads the 3D model file.

[10] Refer to the *3D Printing, Cloud-based 3D Printing Services* EDP at https://www.oit.va.gov/library/recurring/edp/.
[11] STL is a commonly used file format in 3D printing describing the surface geometry of a 3D object without any representation of color or texture. For more information, refer to https://3dprintingforbeginners.com/stl-and-obj-files-101/.

- The DLP server examines the 3D model file and the identity of the user downloading the file to determine if the user is permitted access. If access is permitted, the download proceeds.
- The connection between the image repository and the local computer 3D model file download is secured using TLS.
- The 3D model is downloaded to a local computer that hosts the 3D printer's print preparation SW.

Figure 2 illustrates the use case that describes how data security is performed during 3D model file storage and when 3D model files are accessed from the internal 3D printing file repository. Data security is part of the workflow for printing a 3D model.

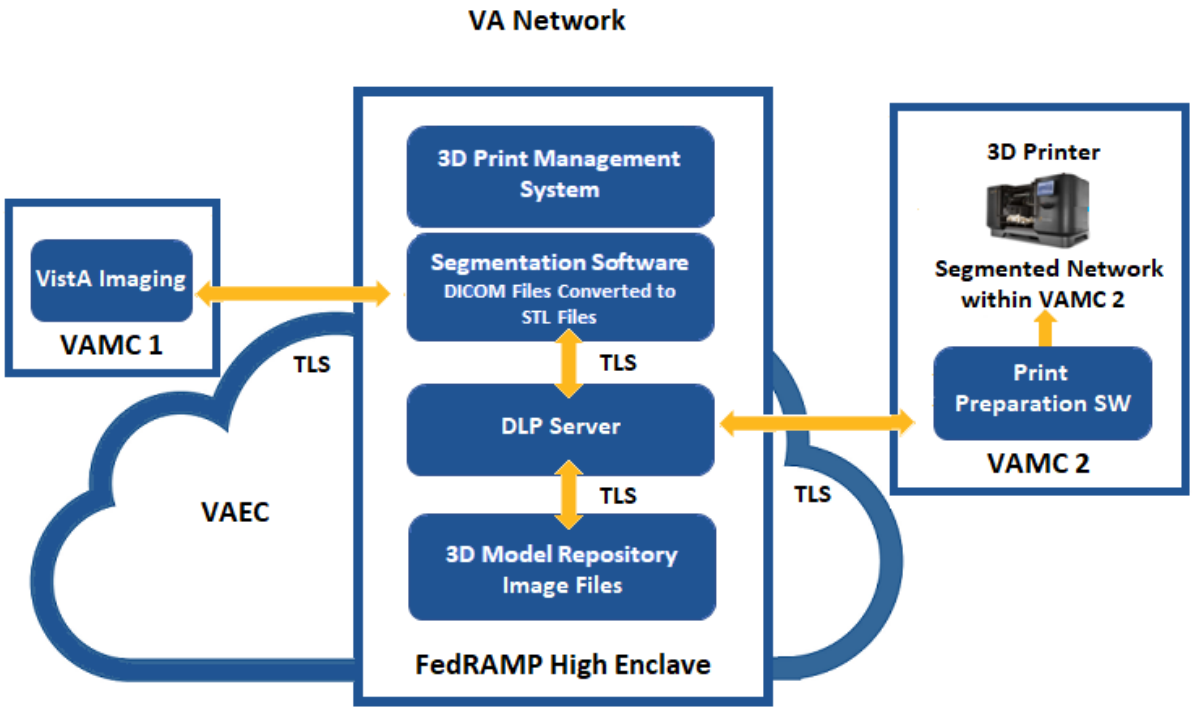


Figure 2: Data Security Architecture for 3D Printing – Interim Solution[12]

5 Impacts

If project teams do not adhere to 3D printing data security guidelines, the following negative impacts may be realized:

[12] Source: Figure 2 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) Enterprise Design Pattern (EDP) Team from information obtained from VA Subject Matter Experts (SMEs).

- Veteran PII and PHI may not be protected in a cloud environment.
- PII and PHI data that is stored in the internal 3D printing file repository may not be secure.

Appendix A: References

- NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
- CSA SecaaS Implementation Guidance – Category 2 // Data Loss Prevention https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_2_DLP_Implementation_Guidance.pdf
- VA Handbook 6500 Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2
- VA Directive 6550 Pre-Procurement Assessment for Medical Device/Systems: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=790&FType=2
- VA Directive 6551 Enterprise Design Patterns: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=829&FType=2
- VA EDPs: https://www.oit.va.gov/library/recurring/edp/
- VA DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/External%20Documents/DEA%20User%20Stories%20v2.3%20(ACTIVE).doc
- VA TRM: http://trm.oit.va.gov/ and https://www.oit.va.gov/services/trm/
- VIP Guide: https://vaww.vaco.portal.va.gov/sites/OIT/epmo/vip/Policy%20%20Guidance/VIP%20Guide%203.2.pdf

Appendix B: Description of Complex Figures

Figure 1: The VA 3D Printing Pillars graphic shows three pillars of agile architecture for 3D printing at VA. The first is titled Network Design and Security. The second image is titled Cloud-based 3D Printing Services, with an outline of a cloud. The third image is titled Data Security, with an image of a lock on a file folder; it is surrounded by a red border to denote that it is the subject of this segment.

Figure 2: The Data Security Architecture for 3D Printing – Interim Solution illustrates the use case that describes how data security is performed during 3D model file storage and when 3D model files are accessed from the internal 3D printing file repository, as described in Section 4.1 of this document. An image of the VA Network is shown with three text boxes: a VAMC 1 text box that includes a DLP server text box and label, pointing to and from the FedRAMP High Enclave text box, shown as part of the VAEC by overlapping the VAEC icon, where the TLS label is inside the cloud, and the VAMC 2 text box. The FedRAMP High Enclave text box includes the 3D print job management system label, followed by a label entitled Segmentation Software – DICOM files converted to STL files. The Segmentation Software label is pointing to and from the DLP Server label by a double-sided arrow, with the TLS label shown adjacent to the arrow, pointing to and from the Image Repository label by a double-sided arrow, with the TLS label adjacent to the arrow. The FedRAMP High Enclave text box also points to and from the VAMC 2 text box by a double-sided arrow, with the TLS label shown adjacent to the arrow. The VAMC 2 text box includes the Print Preparation Software label, which includes text that it is typically printer dependent. An upward arrow points to the label, Segmented Network within a VA hospital, adjacent to an image labeled, 3D Printer.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.