**Office of Research Oversight**

***Research Information Security***

**CHECKLIST**

Version: August 2023

**PURPOSE:**

This Checklist is provided to assist VHA research programs with maintaining compliance with certain statutes, regulations, and policies for the protection of VA research information.

**BACKGROUD:**

The statutes, regulations and policies in the Checklist provide foundational information protection processes at a VHA research program. ORO recommends Research Service staff consult with relevant facility subject matter experts, including the OIT Area Manager, Information System Security Officer, Privacy Officer, and Records Manager, when completing the Checklist. Familiarization with resources cited in this Checklist is encouraged when reviewing and addressing the questions.

**DIRECTIONS:**

Each Element pertains to an event (e.g., action or circumstance) encountered in research, and if that event occurs (or has occurred) at the facility, additional related questions are provided in subsequent columns to assist in assessing whether the events are compliant with policy and regulatory requirements. Questions related to policy clarifications should be directed to the appropriate facility point of contact or the office responsible for the policy publication.

Note: References to “research personnel” refer to all persons with a VA appointment – whether full or part-time, WOC, or IPA – engaged in VA research, including but not limited to PIs, co-PIs, co-investigators, coordinators, and students.

**ACRONYMS, TERMS, and DEFINITIONS:**

Relevant lists are provided in Appendix A and Appendix B.

|  |  |
| --- | --- |
| VA Facility: |  |
| Reviewer(s): |  |
| Review Date: |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section A. DOCUMENTATION AND USE OF NON-VA (EXTERNAL) INFORMATION SYSTEMS** | | | | | |
|  |  | **N** | **Y** | **N/A** | **References** |
| A1 | Do researchers utilize non-VA (external) information systems to process, store, or transmit research data during procedures approved as part of a VA research protocol? If so, the following are utilized: |  |  |  | VHA Directive 1200.01(1) §3.d  VHA Directive 1200.01(1) §3.f |
| A1a | Non-VA networks that are not directly connected to the VA network (also known as an air-gapped network)? If so: |  |  |  | VA OIT OIS KS §AC-20, CCI-002332  VA OIT OIS KS §AC-20(1), CCI-002334, CCI-002335, CCI-002336  VA Handbook 6513 §5.e |
| 1. Are terms and conditions documented for all uses of non-sensitive VA information? |  |  |  |
| 1. Are security controls documented for all uses of sensitive VA information? |  |  |  |
| A1b | Non-VA networks that are directly connected to the VA network (also known as a system interconnection)? If so: |  |  |  | VA OIT OIS KS §CA-3, CCI-000257, CCI-000259, CCI-000260 |
| * 1. Are terms and conditions documented for all uses of non-sensitive VA information (e.g., in an MOU/ISA)? |  |  |  |
| * 1. Are security controls documented for all uses of sensitive VA information? |  |  |  |
| A1c | Non-VA devices associated with the non-VA networks (e.g., laptops, desktops, removable media)? If so: |  |  |  | VA OIT OIS KS §AC-20, CCI-002332; VA OIT OIS KS §AC-20(1), CCI-002334, CCI-002335, CCI-002336  VA OIT OIS KS §MP-6, CCI-002579, CCI-001028  VA Handbook 6513 §5.d  VA Directive 6500 §2.b(5)(g) & (i) |
| 1. Are terms and conditions documented for all uses of non-sensitive VA information? |  |  |  |
| 1. Are security controls documented for all uses of sensitive VA information? |  |  |  |
| 1. Is there a sanitization and disposal process in place to ensure the VA sensitive information is removed from the device(s) prior to disposal/release from VA control? |  |  |  |
| A1d | Non-VA storage resources (e.g., affiliate owned servers, non-VA REDCap, Google Drive, AWS, Azure, Dropbox, One Drive, or other cloud-based resources)? If so: |  |  |  | VA OIT OIS KS §AC-20, CCI-002332  VA OIT OIS KS §AC-20(1), CCI-002334, CCI-002335, CCI-002336  VA Directive 6517 §2.c. |
| 1. Are terms and conditions documented for all uses of non-sensitive VA information? |  |  |  |
| 1. Are security controls documented for all uses of sensitive VA information? |  |  |  |
| A2 | Non-VA portable and mobile storage devices are used to store VA sensitive research information? If so: |  |  |  | VA OIT OIS KS §AC-19, CCI-000082, CCI-000083, CCI-000084, CCI-002326 VA OIT OIS KS §AC-19(5), CCI-002329, CCI-002330, CCI-002331  VA Information Security Rules of Behavior, §4. |
| * 1. Are the devices approved for such use by the OIT Area Manager? |  |  |  |
| * 1. Are the devices appropriately encrypted? |  |  |  |
| A3 | Are VA research records (electronic or hard copy) maintained at non-VA locations or on non-VA devices? If so: |  |  |  | VHA Directive 1200.01(1) §15  VHA Directive 1200.05(3) §5.g(15)  VA Handbook 6300.1 Chapter 5 §1.a  VHA RCS 10-1, Section IV, Part 3, Chapter 8, Code 8300 §6  VA OIT OIS KS §CP-9, CCI-000534, CCI-000535  VHA Handbook 1200.12 §16.d. |
| 1. Are they stored in a manner that allows their ready retrieval? |  |  |  |
| 1. Is documentation in place establishing the official file location? |  |  |  |
| 1. Are processes in place to ensure that VA data/records contained on non-VA devices is appropriately backed-up? |  |  |  |
| A4 | Is equipment owned by an affiliated institution, or purchased by such institution from grant funds, and used by a VA investigator in a research project at the VA facility? If so: |  |  |  | VA Handbook 7002 §11.3.a.  VA Handbook 7002 §§8.5.a. and 8.5.b.  VA Handbook 7002, Appendix I §14 |
| 1. Is it accounted for on an EIL contained in the facility property management system? |  |  |  |
| 1. Has the non-VA IT equipment been inventoried within the past year? |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section B. DOCUMENTATION AND USE OF VA INFORMATION SYSTEMS** | | | | | |
|  |  | **N** | **Y** | **N/A** | **References** |
| B1 | VA researchers utilize the following VA storage devices and services for VA research data: |  |  |  | VHA Directive 1200.01(1) §3.d  VHA Directive 1200.01(1) §3.f |
| B1a | VA Medical Center Service line or similar VA network shared folder storage? If so: |  |  |  | VA OIT OIS KS §AC-3, CCI-000213, CCI-002165 |
| 1. Is access to research data limited only to approved individuals? |  |  |  |
| B1b | VA SharePoint, VA REDCap, VA Box, or OneDrive based storage. If so: |  |  |  | VA OIT OIS KS §AC-3, CCI-000213, CCI-002165 |
| 1. Is access to research data limited only to approved individuals? |  |  |  |
| B1c | VINCI workspace-based storage? If so: |  |  |  | VHA Handbook 1200.12 Appendix C §§1.b. and 6.  VINCI Workspace User Guide  (August 9, 2022) §1.  VINCI DART User Guide (May 2023) Appendix A |
| 1. Is subject level data transferred from VINCI servers to non-VINCI servers? If so, |  |  |  |
| 1. Is the transfer approved through the DART application and Research Data Request Memorandum (e.g., to local servers) or DUA (e.g., for non-VHA servers)? |  |  |  |
| B1d | Other VA storage resources such as a device that may be specific to a research group(s) (e.g., HSR&D server, lab group server/NAS device)? If so: |  |  |  | VA OIT OIS KS §CM-5, CCI-001813, CCI-000343, CCI-000344  VA OIT OIS KS §AC-6, CCI-002226  VA OIT OIS KS §CP-9, CCI-000534, 000535  VHA RCS 10-1, Section IV, Part 3, Chapter 8, Code 8300 §6 |
| 1. Are all device(s) on the VA network? |  |  |  |
| 1. Has the manager(s) of the devices(s) been approved for elevated privileges through the OIT approval process? |  |  |  |
| 1. Are processes in place to ensure that VA data is appropriately backed-up and retained by VA? |  |  |  |
| B2 | Are VA mobile, portable, or standalone devices used to process and store VA research data? If so: |  |  |  | VA OIT OIS KS §AC-19, CCI-000084, CCI-002326, CCI-002329, CCI-002330, 002331  VA OIT OIS KS §PS-4, CCI-001526  VA OIT OIS KS §IA-3, CCI-001958  VA OIT OIS KS §CP-9, CCI-000534, CCI-000535  VA OIT OIS KS §MP-5, CCI-001027  VHA RCS 10-1, Section IV, Part 3, Chapter 8, Code 8300 §6.  VA Directive 7002, Part 13, §§5 and 10 |
| 1. Are processes in place to ensure that VA data contained on the VA devices is appropriately backed-up and retained? |  |  |  |
| 1. For VA thumb drives, is there a process in place to track the devices from purchase to disposal? |  |  |  |
| 1. Are any devices used to store VASI? If so: |  |  |  |
| * 1. Are the devices appropriately encrypted? |  |  |  |
| * 1. Have the devices been approved for storage of VASI by the OIT Area Manager? |  |  |  |
| B3 | Is VA sensitive research data transported outside the VA protected environment on VA devices? If so: |  |  |  | VA OIT OIS KS §MP-5, CCI-001020, CCI-001021, CCI-001022, CCI-001023, CCI-001024, CCI-001025  VA Handbook 7002, Part 13 §5 |
| 1. Are appropriate approvals in place? |  |  |  |
| B4 | Are all VA IT devices/systems (e.g., computers, data storage equipment, smart phones, tablets) used, at least in part, for VA research included on an appropriate EIL and inventoried annually? |  |  |  | VA OIT OIS KS §CM-8 CCI-00418  VA OIT OIS KS §PM-5 CCI-000207  VA Directive 7002, Part 13 §§6 and 7  VA Handbook 7002, Part 8 §5.b(1), (3), and (5) |
| B5 | Does the facility have a sanitization and disposal process for portable and mobile devices used for the processing and storage of VA research information in accordance with VA policies? |  |  |  | VA OIT OIS KS §MP-6, CCI-001028, CCI-002579  VA Directive 6500, §2.b(5) |
| B6 | Have research-related POAMs been entered for identified information systems deficiencies as required according to OIT policies? |  |  |  | VA OIT OIS KS §CA-5, CCI-000264 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section C. RESEARCH INFORMATION SECURITY/PRIVACY PROTOCOLS and PROCEDURES** | | | | | |
|  |  | **N** | **Y** | **N/A** | **References** |
| C1 | Do investigator protocols contain a sufficient description of the research to allow the R&DC and/or its subcommittees to fully review all procedures, plans for statistical analysis of the data, plans for the confidentiality and security of the data, and plans for maintaining confidentiality of the information? |  |  |  | VHA Directive 1200.02(1) §14.a(3)(c) |
| C2 | For research involving collaboration with non-VA institutions, does the protocol, addendum, and/or IRB of Record application describe how the data are to be transmitted to those collaborators? |  |  |  | VHA Directive 1200.05(3) §15.b  VHA Directive 1200.01(1) §10.b |
| 1. If yes, do those transmission methods meet VA information security requirements? |  |  |  |
| 1. Do all protocol documents and agreements pertaining to collaborative research with non-VA institutions address VA data issues such as disclosure, transmission, and ownership? |  |  |  |
| C3 | Are appropriate DUAs obtained when required by policy, and adhered to, including: |  |  |  | VHA Directive 1153 §§5.k(6), 5.l, 7.c(3)  VHA Handbook 1200.12 Appendix C §§1.b and 1.c  VHA Directive 1605.01 §§3.b(5), 3c(6), 41.ff, 13.a(10), and 13.a(11) |
| 1. When CMS and/or USRDS data is obtained from VIReC? |  |  |  |
| 1. When VA enterprise data is obtained through VINCI? |  |  |  |
| 1. When a researcher shares data with a non-VA entity who is serving as a contractor or collaborator on the PI's VA-approved protocol? |  |  |  |
| 1. When a limited data set is shared and the DUA is the HIPAA authority for the disclosure? |  |  |  |
| C4 | Do researchers utilize data from a National Data Set (CMS, CDW, NDS, etc.)?  If so, does the PO ensure: |  |  |  | VHA Directive 1605.03(2), Appendix D, §1.k(9) |
| 1. The data is accessed only by individuals approved to use the information? |  |  |  |
| 1. That a DUA is in place if required, and if so: |  |  |  |
| * 1. The data are stored in accordance with the DUA? |  |  |  |
| 1. That reasonable safeguards are implemented for the data? |  |  |  |
| 1. There is a defined plan for protection of the data until it reaches its disposition date according to VHA RCS 10-1? |  |  |  |
| C5 | If subject contact information (e.g., name, address, SSN, phone number) is collected/used, is it maintained in a separate file at the VA and linked with the remainder of the subject’s data only when it is necessary to conduct the research? |  |  |  | VHA Handbook 1200.12 §14.c(1)(e)1.*NOTE* |
| C6 | Before using the individually identifiable health information of non-employee subjects for research purposes, do research personnel obtain: |  |  |  | VHA Directive 1605.01 §13.a  VHA Directive 1200.05(3) §17.i.*NOTE*  VHA Directive 1605.01 §13.a(12)-(13) |
| 1. Written AUTHORIZATIONS from the subjects? OR |  |  |  |
| 1. An IRB-approved WAIVER of authorization, such as for screening, recruiting, or determining eligibility for research protocols? OR |  |  |  |
| 1. A DUA for a Limited Data Set? |  |  |  |
| C7 | Does the PO review all VA research-related HIPAA authorizations and waivers of HIPAA Authorization? |  |  |  | VHA Directive 1200.05(3) §23.a(3)  VHA Directive 1605.03(2) Appendix D §1.k(5)(a)-(b) |
| C8 | Do informed consent documents include a statement describing the extent to which confidentiality of records identifying the subject will be maintained? |  |  |  | VHA Directive 1200.05(3) §17.d(5) |
| C9 | Is VA sensitive research information encrypted during transmissions outside of VA-owned or managed facilities, Medical Centers, CBOCs, etc.? |  |  |  | VA OIT OIS KS §SC-13, CCI-002449, CCI-002449 |
| 1. Do all eCRFs and sponsor websites used to transmit data employ VA approved encryption in end-to-end connections? |  |  |  |
| C10 | Do researchers transport VASI outside of the VA facility? |  |  |  | VHA Directive 1605.01 §4.b(7)  VA Handbook 7002, Part 13 §10.a(4)  VA OIT OIS KS §AC-17 |
| 1. If yes, have approvals been obtained from their supervisor(s)? |  |  |  |
| C11 | Is written notification of all apparent information security or privacy incidents provided to the appropriate research subcommittee(s) within five business days for their review and determination of whether the incident constitutes a systemic deficiency, serious noncompliance, or continuing noncompliance? |  |  |  | VHA Directive 1058.01 §§6 and 11 |

**Appendix A: Acronyms**

|  |  |
| --- | --- |
| AWS | Amazon Web Services |
| CBOCs | Community Based Outpatient Clinics |
| CCI | Control Correlation Identifier |
| CDW | Corporate Data Warehouse |
| CIO | Chief Information Officer (the position was retitled at the facility level as IT Area Manager) |
| CMS | Center for Medicare and Medicaid |
| DART | Data Access Request Tracker |
| DUA | Data Use Agreement |
| eCRF | Electronic Case Report Form |
| eduroam | Education Roaming (a wireless network interface) |
| EIL | Equipment Inventory List |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| HSR&D | Health Services Research and Development Service (ORD) |
| IPA | Intergovernmental Personnel Act |
| IRB | Institutional Review Board |
| ISA | Interconnection Security Agreement (also known as System Interconnection Agreement (SIA)) |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| ISP | Internet Service Provider |
| IT Area Manager | Formerly known as the Chief Information Officer |
| MOU | Memorandum of Understanding |
| NDS | National Data Systems (VHA) |
| NIST | National Institute of Standards and Technology |
| OIS | Office of Information Security (VA) |
| OIT | Office of Information and Technology (VA) |
| ORO | Office of Research Oversight (VHA) |
| PI | Principal Investigator |
| PO | Privacy Officer |
| POAM | Plan of Action and Milestones |
| R&DC | Research and Development Committee |
| RCS | Records Control Schedule |
| REDCap | Research Electronic Data Capture |
| SOP | Standard Operating Procedures |
| USRDS | United States Renal Data System |
| VA | Department of Veterans Affairs |
| VA OIT OIS KS | VA OIT Office of Information Security Knowledge Service |
| VASI | VA Sensitive Information |
| VHA | Veterans Health Administration (VA) |
| VINCI | VA Informatics and Computing Infrastructure |
| VIReC | VA Information Resource Center |
| WOC | Without Compensation |

**Appendix B: Terms and Definitions**

The terms and definitions used below may be viewed online in the NIST Online Computer Security Resource Center at the following link: <https://csrc.nist.gov/glossary> or within the applicable VA Directive or Handbooks.

**Air-gap:** An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). (SOURCE: VA Handbook 6513 §5.e). Air-gapped networks such as an academic affiliate network, a private ISP network, the VA Guest wireless, or eduroam wireless may be present in VHA facilities and used by researchers.

**Cloud Computing:** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. SOURCE: NIST SP 800-145

**Control Correlation Identifier:** Allows a high-level statement in a policy document to be ‘decomposed’ and explicitly associated with the low-level security settings that must be assessed to determine compliance with the objectives of that specific statement.

SOURCE: VA Handbook 6500

**External (Non-VA) information system (or component):** A system or component of a system that is used by but is not a part of an organizational system and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness. SOURCE: NIST SP 800-53 Rev. 5

**Information Security Knowledge Service:** The VA’s knowledge service portal for providing cybersecurity and privacy policies, procedures, and guidance. SOURCE: VA Directive 6500.

**Mobile Device:** A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers. SOURCE: NIST SP 800-53 Rev. 5

**Portable Storage Device:** A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio or image data—as its primary function (e.g., optical discs, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks). SOURCE: NIST SP 800-53 Rev. 5

**Sanitization:** A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media. SOURCE: NIST SP 800-53 Rev. 5

**Security Controls:** The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. SOURCE NIST 800-53 Rev. 5

**VA Sensitive Information:** Any information that has not been cleared for public release and has been collected, developed, received, transmitted, used, or stored by VA, or by a non-VA entity in support of an official VA activity. VA Sensitive Information may be a type of Controlled Unclassified Information (CUI), and if so, must follow the VA’s CUI guidance. SOURCE: VA Directive 6500