

Checklist for Successful Completion of Annual WOC Packet – October 2008

Complete (Everyone)	HIPAA (VHA Privacy Policy Training) => https://www.ees-learning.net
Complete (Everyone)	VA Information Security Awareness Training => https://www.ees-learning.net
Complete (Everyone)	VA Information Security 201 for R&D Personnel => https://www.ees-learning.net
Complete (Everyone)	VA National Rules of Behavior (Print Form)
Complete (lab workers only)	Lab Worker Safety Training Checklist (Print Form; supervisor must sign)
Complete (If you participate in Human Studies)	Human Subjects Research Training => https://www.citiprogram.org AND Scope of Practice Form -> (Print Form)
Complete (If you participate in Animal Studies)	Animal Studies Training => https://www.citiprogram.org ----- Occupational Health & Safety Survey (Print Certificates)

When you have completed the forms and the education print off your training certificates and bring all appropriate forms and certificates to the Research Office to either Linda Starks or Bob Pollock.

If you have any questions, please feel free to contact us.

a. R&D Coordinator: Linda Starks at 845-5602

b. Human Studies Coordinator: Doug Feldman at 845-3440

c. Animal Studies + Research Safety Coordinator: Cathy Kaczmarek at 845-3439

d. ePROMISE Master: Bob Pollock at 845-5600

May 10, 2007

Requirement for credentialing of all research staff

This requirement applies to all research staff including those that are compensated by the VA, those that are appointed as Without Compensation (WOC), and those appointed by the Intergovernmental Personnel Act Mobility Program (IPA). The staff may be full time, part time, or fee basis.

Credentialing

Credentialing is the systematic process of screening and evaluating qualifications and other credentials, including licensure, registration, certification, required education, relevant training and experience, and current competence.

Unlicensed staff

All staff that by virtue of their education and training is eligible to obtain licensure, registration, or certification is required to be credentialed through Vetpro even if they do not hold an active license, registration, or certification at the time they are appointed.

Unlicensed nurses, physicians, pharmacists, clinical psychologists, and others requiring licenses, registration, or certifications for clinical practice cannot be hired into those occupations unless they obtain an active license, registration, or certification for the occupation and qualify under VA qualification standards. If they do not obtain the license, registration, or certification they must be hired under some other occupational category for which they qualify. If this other occupational category allows a scope of practice to perform procedures AND there is no requirement for licensure or certification, then with a duly exercised scope of practice after the appropriate credentialing could be processed. *Note: See VHA Directive 2006-067 for a list of all effected occupations.*

VetPro: Staff that must be credentialed in VetPro

- All health care professionals who claim licensure, certification or registration as applicable to their position within VHA.
- All research staff that holds a degree that may make them eligible for licensure, registration, or certification. Such persons would include but is not limited to: nurses, physicians, Foreign Medical Graduates, Clinical Psychologists, and pharmacists that do not have a current active license. *Note: See VHA Directive 2006-067 for a more complete list.*
- All research staff including research administrative personnel, who by the nature of their position have the potential to assume patient care-related duties, or oversee the quality or safety of the patient care delivered, e.g. Research Assistants, Project Officers, etc..

May 10, 2007

Scope of Practice or Functional Statement

A Scope of Practice or Functional Statement outlines all the duties of employees. These duties must: 1) be consistent with the occupational category under which they are hired, 2) allowed by the license, registration, or certification they hold, 3) consistent with their qualifications (education & training), and 4) be agreed upon by the person's immediate supervisor and the ACOS. *Note: When working on specific research protocols, the Principal Investigator for each protocol must also agree.*

Clinical Privileges

If the person's license allows for independent practice and the facility chooses to allow independent practice, privileges must be granted in accordance with VHA Handbook 1100.19 and the facility's Medical Staff Bylaws, Rules and Regulation prior to performing the interventions covered under the privileges they have been granted.

Points to consider

Individuals must not practice beyond the occupation they are hired/appointed into and their Scope of Practice or Functional Statement.

Principal Investigators are responsible for the overall conduct of their research protocols including ensuring that all research staff for the protocol are working within their Scope of Work or Functional Statement.

The appropriate background check as defined in VA Directive and Handbook 0710 must also be completed. *Note: For those employees working with Select Agents or Toxins, additional background investigations must be completed. See VHA Handbook 1200.06 for more information.*

Trainees from our academic affiliates must have a Resident/Trainee Credentials Verification Letter (RCVL) prior to any interactions with research subjects. VHA Handbook 1400.1 contains further information regarding residents and trainees.

Human Resource Management (HRM) responsibilities

HRM has the primary responsibility for verifications of a candidate's qualifications including education, relevant training and experience, and current competence to hold the position. HRM is also responsible for checking US citizenship or visa status.

ACOS/R&D and/or AO/R&D responsibilities

Either the ACOS/R&D and/or the AO/R&D must ensure that all research staff:

- Have been credentialed prior to appointment. If not, they must be credentialed ASAP. *Note: Credentialing for those who are covered by Directive 2006-067*

May 10, 2007

and VHA Handbook 1100.19 must be credentialed through VetPro. Staff that hold a degree that may make them eligible for licensure, registration, or certification related to in health care must also be credentialed through VetPro.

- Have a Scope of Practice or Functional Statement that is consistent with their education, licensure, or certification, and
- Have been granted the appropriate privileges, if applicable under the facility's Bylaws,

In addition, the following must be done:

- Annually ascertain compliance with these requirements.
- Maintain records that will adequately show these responsibilities have been fulfilled.

VHA Policies regarding credentialing

- VHA Directive 2006-067 December 22, 2006 “Credentialing of Health Care Professionals”
- VHA Handbook 1100.19 March 6, 2001 “Credentialing and Privileging”
- VHA Handbook 1400.1 July 27, 2005 “Resident Supervisions”
- VA handbook and Directive 0710, September 10, 2004 “Personnel Suitability and Security”
- VA Handbook 5005 April 15, 2002 “Staffing”

Research Credentialing Verification

Name:	Email address:
Principal Investigator	Phone No.

Please answer the following questions after you have read "Requirement for credentialing of all research staff"

1. Do you hold a degree that may make you eligible for licensure, registration or certification?

Yes No

2. If yes, list specific Degrees that apply (MBBS, MD, RN, MSW, RRT, PhD ---specify area of study for the PhD)

3. Please list all current or past licensure, registration, or certification (no matter State or specialty this was held in).

4. By the nature of your position at the VA, do you have the potential to assume patient care-related duties or oversee the quality or safety of the patient care delivered, e.g. Research Assistants, Study Coordinators, etc.

Yes No

5. Are you currently credentialed through Vetpro? Yes No

Employee Signature	Date	Principal Investigator Signature (Required)	Date

Department of Veterans Affairs (VA) National Rules of Behavior**1. Background**

a. Section 5723(b)(12) of title 38, United States Code, requires the Assistant Secretary for Information and Technology to establish “VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department’s missions and functions.” The Office of Management and Budget (OMB) Circular A-130, Appendix III, paragraph 3(a)(2)(a) requires that all Federal agencies promulgate rules of behavior that “clearly delineate responsibilities and expected behavior of all individuals with access” to the agencies’ information and information systems, as well as state clearly the “consequences of behavior not consistent” with the rules of behavior. **The National Rules of Behavior that begin on page G-3, are required to be used throughout the VA.**

b. Congress and OMB require the promulgation of national rules of behavior for two reasons. First, Congress and OMB recognize that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g. digital, paper), are essential aspects of their job. Second, individuals must be held accountable for their use of VA information and information systems.

c. VA must achieve the Gold Standard in data security which requires that VA information and information system users protect VA information and information systems, especially the personal data of veterans, their family members, and employees. Users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information. The Golden Rule with respect to this aspect of an employee’s job is to treat the personal information of others the same as they would their own.

d. Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using “due diligence” and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives.

2. Coverage

a. The attached VA National Rules of Behavior must be signed annually by all VA employees who are provided access to VA information or VA information systems. The term VA employees includes all individuals who are employees under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees. Directions for signing the rules of behavior by other individuals who have access to VA information or information systems, such as contractor employees, will be addressed in subsequent policy. VA employees must initial and date each page of the copy of the VA National Rules of Behavior; they must also provide the information requested on the last page, sign and date it.

b. The VA National Rules of Behavior address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management

and system administrators, and serves to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

c. The VA National Rules of Behavior use the phrase “VA sensitive information”. This phrase is defined in VA Directive 6500, paragraph 5q. This definition covers all information as defined in 38 USC 5727(19), and in 38 USC 5727(23). The phrase “VA sensitive information” as used in the attached VA National Rules of Behavior means:

All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information, financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information, information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege, and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

d. The phrase “VA sensitive information” includes information entrusted to the Department.

3. Rules of Behavior

a. Immediately following this section is the VA approved National Rules of Behavior that all employees (as discussed in paragraph 2a of Appendix G) who are provided access to VA information and VA information systems are required to sign in order to obtain access to VA information and information systems.

Department of Veterans Affairs (VA) National Rules of Behavior

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

- a. I understand that when I use any Government information system, I have NO expectation of Privacy in VA records that I create or in my activities while accessing or using such information system.
- b. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), VA, and law enforcement personnel.
- c. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.
- d. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.
- e. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.
- f. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my supervisor, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

g. I understand that the VA National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

h. I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

i. I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

b. I will follow established VA information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.

e. I will secure VA sensitive information **in all areas** (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).

f. I will properly dispose of VA sensitive information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.

j. I will not store any passwords/verify codes in any type of script file or cache on VA systems.

k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system.

m. I will not auto-forward e-mail messages to addresses outside the VA network.

n. I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.

o. I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p. I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.,

q. I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized **in writing** by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.

r. I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.

s. I will protect Government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connected to any VA network.

u. If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure

the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v. I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb. I understand that remote access is allowed from other Federal government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

cc. I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I must use VA-provided IT equipment for remote access when possible. I may be permitted to use non-VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

dd. I agree that I will not have both a VA network connection and any kind of non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my local CIO.

ee. I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff. I will obtain my VA supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA's protected environment..

gg. I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location pursuant to an approved telework agreement with VA sensitive information that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii. I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj. I will use VA-provided encryption to encrypt any e-mail, including attachments to the e-mail, that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

3. Acknowledgement and Acceptance

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

[Print or type your full name]

Signature

Date

Office Phone

Position Title

Research Service (11R)

RESEARCH EMPLOYEE SAFETY TRAINING CHECKLIST

Employee Name:	Supervisor:	WOC Employee <input type="checkbox"/>	Start Date:
		VA Employee <input type="checkbox"/>	

All research personnel must have annual safety training. Complete this form with your supervisor, sign, date and return this form to the research office (11R) within seven (7) days of employee's start date. This form is used to document mandatory annual safety training requirements.

<input type="checkbox"/>	1. Location and use of Life Safety Equipment:	<input type="checkbox"/>	5. MSDS Sheets (Material Safety Data Sheets) - location and use
<input type="checkbox"/>	a. Fire Safety 1. Fire Emergency Plan - RACE 2. Pull Stations - location & fire codes 3. Fire Extinguishers - location & usage	<input type="checkbox"/>	6. Review the Hazardous Materials Management Plan MCM # S-2 http://www1.va.gov/aavaresearch/docs/S2_2005.doc
<input type="checkbox"/>	b. Minimum Accessibility Requirements 1. Maintain a 48" corridor width 2. Storage at least 18" from sprinkler heads 3. Maintain a 36" semi-circle of access to electrical panels	<input type="checkbox"/>	7. Safety Management Program MCM #S-3 http://www1.va.gov/aavaresearch/docs/S3.doc a. Inspection tags on Equipment b. Elec. Shock Hazards
<input type="checkbox"/>	c. Showers, Eye Washes (location, how to use & check functioning & monthly update of inspection tags for eye washes)	<input type="checkbox"/>	8. Exposure Control Plan for Bloodborne Pathogens MCM #S-4 http://www1.va.gov/aavaresearch/docs/S4.doc a. To work with human blood/body fluids b. Post Exposure Evaluation and Follow-up
<input type="checkbox"/>	d. Spill Kits for Acid, Caustic, Flammable, Blood & Body fluids (how to use, fully stocked kits) 1. Replacement supplies	<input type="checkbox"/>	9. Emergency Preparedness Plan MCM #S-5 http://www1.va.gov/aavaresearch/docs/S5.doc a. Horizontal Evacuation
<input type="checkbox"/>	e. Safety equipment specific to your lab including personal protection equipment 1. Lab coats 2. Eye, Face, Hand, Foot, Head	<input type="checkbox"/>	10. Operation of equipment (such as sterilizers and centrifuges) a. Location of operation Manual b. Documented User Training
<input type="checkbox"/>	2. Medical Center Safety Policies Manual (review location and check documentation that each person who works in the lab has reviewed manual) (Also located on "T" Drive; Public/Policies/Policies-Current/Safety	<input type="checkbox"/>	11. VHA Handbook for Safety of Personnel in Research 1200.8 http://www1.va.gov/aavaresearch/docs/1200_8.doc
<input type="checkbox"/>	3. VA Research Safety Manual On-Line http://www1.va.gov/aavaresearch/page.cfm?pg=4	<input type="checkbox"/>	12. Specific job related hazards a. Gas cylinder storage and handling b. Moving chemicals to storage c. Glass d. Chemical inventory e. Biohazard
<input type="checkbox"/>	4. Radiation Safety and ALARA MCM #S-1 http://www1.va.gov/aavaresearch/docs/S1_ALARA.doc (Annual Training will be scheduled by the VA Radiation Safety Officer)	<input type="checkbox"/>	NO FOOD OR DRINKS IN LABS No eating or drinking in labs No coffee cups or pop cans on benches No food in laboratory refrigerators VIOLATORS WILL BE FINED \$500

<i>Employee Signature:</i>	<i>Date:</i>	<i>Investigator Signature:</i>	<i>Date:</i>
----------------------------	--------------	--------------------------------	--------------

VA HUMAN SUBJECTS RESEARCH TRAINING POLICY

1. All new study team members must complete The Scope of Practice Survey Form
http://www1.va.gov/aavaresearch/docs/scope_of_practice.rtf
2. Human Subjects Research Education Policy
 - a. All new human research study personnel must complete the VA IRB Human Subjects Research Education requirements prior to engaging in research projects at the VAAAHS.
 - b. All continuing Investigators and Study Team Members must retake a VA-approved training course at least once every 365 days. If you fail to comply with the VA IRB Human Subjects Education Policy you must cease all work with human subjects in the research setting.

Primary Course Choice

VA CITI COURSE AT CITIPROGRAM.ORG

1. Web-Link = <https://www.citiprogram.org/default.asp>
2. Select Your Institution: **Veterans Affairs -> Ann Arbor, MI-506**
3. **Select a Course Group:** => **Question #1 > Choose one answer**
 - bullet #1 'O'** select this bullet if you completed VA training on the CITI website in the past year.
(Hint: Stage 2: Refresher 1 Course = 9 "101 Refresher modules" + 7 "GCP modules"
(Hint: Stage 3, Refresher 2 Course = 11 "Required Modules" + 1 "Elective Module")
 - bullet #2 'O'** select this bullet if you never completed VA training on the CITI website.
(Hint: Stage 1: Basic Course = 14 modules to complete)
4. **Alternate Accepted Course Choice**
Corresponding training at the University of Michigan (PEERRS) from past 6 months

VA ANIMAL STUDIES RESEARCH EDUCATION POLICY

1. Web-Link = <https://www.citiprogram.org>
2. **Select Your Institution:** **Veterans Affairs -> Ann Arbor, MI-506**
3. **Selecting the Correct Course Groups:**
 - Question #2 => Yes if you are a IACUC Member
 - Question #3 => Yes (Working with the VA IACUC)
 - Question #4 => Check EACH species utilized in your animal research activities
 - Question #5 => Yes if you perform or supervise survival surgery in rodent species
 - Question #6 => Yes if you are a new research laboratory worker (VA Biosecurity Training)
4. WOC Personnel Working with Animals

NEW VA RESEARCH LABORATORY WORKERS

If you work in a VA Research Laboratory, you must complete the following:

"Introduction to VA Biosecurity Concepts" course and exam at this web site:

1. Web-Link = <https://www.citiprogram.org>
2. **Select Your Institution:** **Veterans Affairs -> Ann Arbor, MI-506**
3. **Selecting the Correct Course Groups:**
 - Question #6 => Yes if you are a new research laboratory worker (VA Biosecurity Training)

If you have any questions, please feel free to contact us.

- a. R&D Coordinator: Linda Delaney at 845-5602
- b. Human Studies Coordinator: Doug Feldman at 845-3440
- c. Animal Studies + Research Safety Coordinator: Cathy Kaczmarek at 845-3439
- d. ePROMISE Master: Bob Pollock at 845-5600

VA Ann Arbor Healthcare System

Scope of Practice for Employees Involved in VA Human Studies Research

Return to VA Research Office (11R), VA Medical Center, 2215 Fuller Road, Ann Arbor, MI 48105, Box 2399

EMPLOYEE NAME	EMPLOYMENT INSTITUTION
EMPLOYEE SIGNATURE	EMPLOYEE E-MAIL ADDRESS
PRINCIPAL INVESTIGATOR (PI)	TITLE OF RESEARCH STUDY

THE SCOPE OF PRACTICE IS SPECIFIC TO THE DUTIES AND RESPONSIBILITIES OF EACH RESEARCH EMPLOYEE AS AN AGENT OF THE LISTED PRINCIPAL INVESTIGATOR. AS SUCH HE/SHE IS SPECIFICALLY AUTHORIZED TO CONDUCT RESEARCH INVOLVING HUMAN SUBJECTS WITH THE RESPONSIBILITIES OUTLINED BELOW. THE SUPERVISOR MUST COMPLETE, SIGN AND DATE THIS SCOPE OF PRACTICE.

Human Studies Research Duties:	Appro ved	Human Studies Research Duties:	Appro ved
1. Study Coordinator for this project.		10. Demonstrates proficiency with VISTA/CPRS computer system by scheduling subjects research visits, documenting progress notes, initiating orders, consults, etc.	
2. Initiates submission of regulatory documents to IRB, VA R&D committee and sponsor.		11. Accesses patient medical information while maintaining patient confidentiality.	
3. Develops recruitment methods to be utilized in the study.		12. Is authorized to obtain informed consent from research subject and is knowledgeable to perform the informed consent "process".	
4. Prepares study initiation activities.		13. Performs computer data entry and/or data base management, of human subjects research results.	
5. Initiates and/or expedites requests for consultation, special tests or studies following the Investigator's approval.		14. Performs statistical analysis of human subject research results.	
6. Screens patients to determine study eligibility criteria by reviewing patient medical information or interviewing subjects		15. Performs venipuncture to obtain specific specimens required by study protocol (requires demonstrated and documented competencies).	
7. Provides education and instruction of study medication use, administration, storage, side-effects and notifies IRB of adverse drug reactions.		16. Initiates intravenous (IV) therapy and administers IV solutions and medications.	
8. Provides education regarding study activities to patient, relatives and Medical Center staff as necessary per protocol.		17. Collects and handles various types of human specimens.	
9. Obtains and organizes data such as tests results, diaries/cards or other necessary information for the study. Maintains complete and accurate data collection in case report forms and source documents.		18. Performs laboratory tests on human specimens.	

PRINCIPAL INVESTIGATOR STATEMENT:

This Scope of Practice was reviewed and discussed with this study team member on the date of _____. After reviewing his/her education, clinical competency, qualifications, research practice involving human subjects, peer reviews, and individual skills, I certify that he/she possesses the skills to safely perform the aforementioned duties/procedures. Both the employee and I are familiar with all duties/procedures granted or not granted in this Scope of Practice. We agree to abide by the parameters of this Scope of Practice, all-applicable hospital policies and regulations.

Principal Investigator

Date

Roger, Grekin MD, ACOS/ Research

Date

WOC Occupational Health & Safety Survey for Personnel with Laboratory Animal Contact

Name:	SSN:
Supervisor:	email:
Lab location:	Lab phone:

Animal Contact

1. What species of animals will you be exposed to? (This includes direct contact with animals, animal tissues and/or wastes, and animal enclosures.)

2. What kind of contact will you have? (Check all that apply.)
 - Direct contact with animals
 - Direct contact with non-fixed or non-sterilized animal tissues, fluids or wastes
 - Direct contact with non-sanitized animal caging or enclosures
 - Service support to animal equipment, devices, and/or facilities

3. Have you had any of the following vaccinations(if so, indicate date of most recent)
 - Hepatitis A --
 - Hepatitis B --
 - Tuberculosis Skin Testing --

4. Do you or will you handle animals that have been given infectious biohazards?
 - Yes No
 If YES, please provide the following information:
 Infectious agent:
 CDC Class of agent:
 Date of infectious biosafety training:

5. Do you or will you handle animals that have been exposed to or given radiation hazards?
 - Yes No
 If YES, please describe the type of radiation hazard (e.g. UV, laser, ionizing):
 Date of radiation safety training:

6. Do you or will you handle animals that have been given chemical hazards?
 - Yes No
 If YES, please describe the chemical hazard:

7. **I participate in the University of Michigan Occupational Health and Safety Program for Personnel Working with Animals.** Yes No
 If NO, I have signed the waiver below. Yes No

8. I have read and understand the "Occupational Health and Safety Program (OHSP) for Personnel with Laboratory Animal Contact" brochure included in the WOC Registration Packet (yellowbook) Yes

I verify that all information I have provided is accurate.	
Employee Signature: _____	Date: _____
<u>Occupational Health Questionnaire Waiver</u>	
I decline participation in the Occupational Health and Safety Program for animal handlers at this time.	
• I understand the occupational health risks of working with animals	
_____ Signature of Participant	_____ Date

Occupational Health and Safety Program (OHSP) for Personnel with Laboratory Animal Contact

All animal research programs are required to have an OHSP for personnel that have contact with laboratory animals, their tissues, or their allergens. The purpose of this brochure is to explain the components of the OHSP, and provide information on how you can minimize the chance of any adverse health effects from working with laboratory animals.

Who should participate? All personnel who have contact with laboratory animals (including their tissues, body fluids, or wastes) or are exposed to animal allergens in the animal facility on a regular basis should participate in the program. This includes Veterinary Medical Unit staff, investigators, laboratory technicians, and students, and may also include engineering and maintenance personnel, custodial staff, and consultants. To enroll, contact Employee Health.

What is included? The exact services provided depends on the level and type of risk you will encounter. When you enroll in the program and annually thereafter, you will receive a short confidential questionnaire that asks about the extent of your exposure to animals and pertinent aspects of your medical and vaccination history. A health professional will review your responses and may recommend a medical exam, selected immunizations, and tuberculosis screening,

RISKS ASSOCIATED WITH ANIMAL EXPOSURE

The hazards associated with handling animals can be divided into three categories:

1) Physical Hazards. Examples include animal bites and scratches, sharps injuries, injuries associated with moving cages or equipment, and adverse consequences from excessive noise or accidental exposure to workplace . The key to preventing these injuries is proper training and meticulous attention to proper work practices.

•Use appropriate techniques for animal handling and restraint.



•Avoid recapping needles and dispose of sharps in approved containers.

• Be careful when lifting heavy loads or when doing repetitive tasks.

•Wear recommended personal protective equipment such as a lab coat, gloves, and eye protection.

2) Allergies. Allergic reactions are among the most common conditions that adversely affect the health of workers exposed to laboratory animals. Nasal symptoms, itchy eyes, and skin rashes are the most frequent manifestations, but in serious cases, asthma or anaphylaxis can occur. Allergens include urine, dander, and saliva, especially from rodents. Controlling exposure to allergens is the most effective strategy for prevention.

Protect Yourself!

•Work in a clean, well-ventilated environment.

•Wear appropriate personal protective equipment such as a lab coat and disposable gloves, and **never rub your face or eyes**



until you have removed your gloves and washed your hand thoroughly.

•Wear respiratory protection

3) Zoonotic diseases. Zoonotic diseases are those that can be transmitted from animals (or animal tissues) to humans. Although there are a substantial number of animal pathogens that can cause disease in humans, zoonotic diseases are not common in modern animal facilities, largely because of successful efforts at prevention and detection.

Unfortunately some infections of animals may produce serious disease in humans *even when the animals themselves show few signs of illness*. Therefore, you must be aware of possible consequences when working with each species of animal and take precautions to minimize the risk of infection. **In the event that you do become ill with a fever or some other sign of infection, it is important to let the physician caring for you know that you work with animals.**

Prevention. Here are some common sense steps that can be taken to lessen the risk of contracting a zoonotic disease.

• Do not eat, drink, or apply cosmetics or contact lenses around animals.

• Wear gloves when handling animals or their tissues.

• To reduce the risk of needle stick injuries, consider sedating or anesthetizing animals if hazardous materials will be used, or if manual restraint is problematic.

• Work in pairs whenever possible.

• **Do not recap used needles!** Instead, discard them promptly in a biohazard “sharps” container.

• When performing procedures such as bedding changes, blood or urine collections, or necropsies, work in biological safety cabinets or with specialized personal protective equipment.

• **Consult your supervisor, the Safety Officer, or Employee Health if you need additional training at any time.**

WHAT YOU SHOULD KNOW

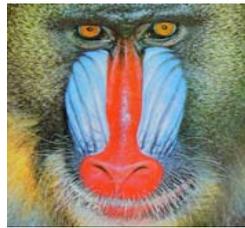
About Bites, Scratches, and other Injuries

Contact Employee Health immediately if you are bitten or scratched, if you injure yourself on animal caging or equipment, or if you experience unusual disease symptoms.

If you are Pregnant

Working with hazardous agents in general and toxic chemicals in particular is discouraged during pregnancy. Consult Employee Health and your personal physician for advice about working safely during pregnancy.

Toxoplasma is an infectious agent that can be shed in cat feces. It can infect the fetus in women who are exposed during pregnancy and do not have immunity to the agent. To help assess the level of immunity against this agent, serum samples can be tested. Cat feces should be avoided and gloves should be worn when working in areas that are potentially contaminated. Wash your hands thoroughly after handling any potential source of infection.



If you work with Nonhuman Primates

Diseases of nonhuman primates are often transmissible to humans.

Although there are several primate viruses that can cause disease in humans, *Herpesvirus simiae* (B-virus) is of greatest concern. This virus occurs naturally in macaques such as rhesus and cynomolgus monkeys. Infected monkeys usually show no clinical signs, but the virus may cause fatal encephalitis in humans. Transmission to humans occurs via exposure to contaminated saliva, secretions, or tissues. This typically occurs as a result of a bite or scratch; transmission can also occur via splashes that come in contact with mucous membranes or via injuries caused by contaminated equipment. Proper work practices constitute the best protection against infection.

- Wear personal protective equipment, including protective outer garments, gloves, face mask, and eye protection.

- Sedate monkeys whenever possible before handling.
- In the event of possible exposure, obtain medical attention immediately. Instructions for treating wounds and obtaining medical attention are posted in each primate area.

Tuberculosis may be transmitted both from humans to animals and from animals to humans. Nonhuman primates and individuals in contact with them must be TB tested regularly. *Shigella*, *Campylobacter*, *Salmonella*, and *Entamoeba histolytica* cause diarrhea in primate species and can cause similar problems in humans exposed to primate feces. Infection is best prevented by the use of gloves and careful hand washing.

Simian immunodeficiency virus is closely related to HIV, the human AIDS virus, and can, on rare occasions, affect macaques. Some evidence suggests it may infect humans as well, so measures should be taken to prevent contact with monkey blood or blood products.

If you work with Dogs or Cats

The main risks associated with working with dogs and cats are bites and scratches. Bacterial infections can result. Cat scratch disease is caused by a rickettsial organism and is characterized by flu-like symptoms and swollen lymph nodes, and cat bites can result in severe bacterial infections. The likelihood of contracting rabies as a result of a bite is low because dogs and cats are typically vaccinated for rabies or bred exclusively for research. Nevertheless, it is recommended

that persons in contact with dogs or cats be vaccinated against rabies.

If you work with Farm Animals

Q fever, a potentially serious disease caused by *Coxiella burnetii*, is carried by ruminants and shed abundantly from the placental membranes of sheep. This route of exposure may cause Q fever pneumonia and other associated symptoms in laboratory workers. Sheep used in research should be assumed to be infected and measures taken to prevent transmission. All individuals working with pregnant sheep should wear gloves, respiratory protection, and protective outerwear.



If you work with Rodents or Rabbits

Allergies are common among personnel who work with rodents (e.g., mice, rats, guinea pigs, hamsters) and rabbits. If you have pre-existing allergies or if you experience a runny nose, itchy eyes, or skin rashes when working around these species you should report this immediately to Employee Health. Measures can be taken to limit your exposure to allergens, thereby reducing the severity of symptoms and decreasing the likelihood that symptoms will worsen.

Rodents and rabbits obtained from commercial sources do not constitute a significant source of zoonotic diseases.

However, animals caught in the wild can harbor a variety of bacterial, viral, fungal, and parasitic infections that constitute a significant hazard to personnel.



If you work with Hazardous Agents

The proper use of hazardous biological, chemical, and physical agents depends on careful planning, proper training, and careful

attention to prescribed work practices. Signs should be posted indicating the nature of the hazard, necessary precautions, and emergency contact information. The personal protective equipment (PPE) needed depends on the agent in use, but in all cases gloves should be worn and hands should be washed after handling potentially contaminated materials. A biological safety cabinet should be used when handling infectious materials, especially if there is a potential for generation of aerosols, and a fume hood should be used when handling toxic chemicals or radioactive materials.

If you need Further Information

For further information, contact Employee Health, the Veterinary Medical Unit, or the VAMC Safety or Biosafety Officer. More guidance in this area can be found in VHA Handbook 1200.7, "Use of Animals in Research."