PARTNERS HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

Partners Research Compliance/ERIS Standard Operating Procedure (SOP): Federal Sponsored Research Contracts with Information Security Terms

February 2017

Overview: This SOP sets forth a process for identification, review, and implementation of technical security requirements throughout the lifecycle of federal contracts and subcontracts with information security clauses.

I. What are Information Security (IS) Terms?

- *IS Terms may be referenced as "FISMA", FAR Clause 39.201, or HHSAR Clauses 352.239-70 through 352.239-74.*
- These IS Terms require technical security or procedures that are non-standard for Partners or the hospitals, annual reports, employee rosters, training and/or background checks.
- These items require specific technical expertise and will involve increased costs, which should be accounted for and included in the proposed budget, as described below.
  - The Partners Research IT Core provides a breakdown of costs and services here: https://rc.partners.org/research-apps-and-services/security/fisma-security-documentation

II. Proposal Stage

A. Department Review

1. The Principal Investigator (PI) will review the terms of all federal contract Requests for Proposal (RFP) for IS Terms.
2. In the case of a Partners subcontract proposal under a federal contract that will be submitted by a non-Partners institution (Prime), prior to submitting the proposal through Research Management Pre-Award, the Partners PI or Department Administrator will review the RFP to determine whether there are IS terms, If there are IS terms, the Partners PI will proceed as described below.
3. If IS Terms are found, the PI or DA must **immediately contact Brent Richter of the Partners Research IT Core**. For a fee, the Core will assist with these reports and actions. All costs of using the Core must be included in the budget at the proposal stage. *Some contracts may require submission of an initial self-assessment and/or risk assessment with the proposal.*
4. *Alternatively and in rare instances*, the PI may identify department staff with the appropriate technical expertise and who can implement the required procedures and complete technical reports. To use department staff:
   a. The PI must receive approval from the Partners Research Information Security Officer (RISO) *and* the hospital Information Security Officer (ISO) for use of department staff to meet the contract. In this case, the Partners Research IT Core must review *and sign* required technical reports prior to submission to the sponsor.
   b. *Contracts or subcontracts that require information security accreditation or certification must use the Partners Research IT core.* ***Authorization to sign accreditation or certification is limited to Brent Richter.***

B. Research Management Pre-Award Review

1. The Pre-Award Grant Administrator (GA) will review the terms of all contract or subcontract RFPs for IS Terms and, if found, consult with the Pre-Award Director and Associate Director for Contracts. The GA will then confirm that DA and PI are aware of the IS Terms and have budgeted for the use of the Partners Research IT Core, or confirmed alternate plans with the Partners RISO and hospital ISO, as above. The

Agreement Associate (AA) will also review the IS Terms and negotiate with the Sponsor, if required at proposal stage.

2. Any reports or certifications submitted with the proposal must be uploaded to the contract's InfoEd record.

III. Contract Negotiation

1. Prior to contract execution, the AA will review the terms of all contracts or subcontracts for IS Terms.
2. If IS Terms are found, the AA will confirm the requirements of the IS Terms with the PI. The AA will also notify Brent Richter/Partners Research IT Core and entity Research Compliance of receipt of a contract/subcontract with FISMA requirements.
3. The PI must confirm that s/he has planned, or is willing and able, to purchase services from the Partners Research IT Core and meet the security requirements, or has received approval from the RISO and hospital ISO for technical experts within the department to manage the requirements of the IS Terms, as above.
4. **Brent Richter must confirm that the IS Terms requirements can be/have been met before the contract may be signed.**

IV. Contract Compliance

A. Personnel Requirements

The PI and his/her delegate are responsible for ongoing compliance with Personnel, such as staff onboarding, training, or termination requirements (See Appendix A).

B. Annual Reporting

1. On an annual basis, the PI should contact Brent Richter of the Partners Research IT core and Fabio Martins (Partners RISO) or the institution's Information Security Officer 90 days prior to the due date, usually the anniversary of the contract execution, to prepare and submit any required reports under the IS Terms. This includes annual review/updates to the existing security plan.
2. The PI and/or DA must provide a copy of any IS security or related documents submitted to the sponsor to the Post-Award GA for uploading into the
3. InfoEd record.

V. Roles & Responsibilities

	PI	Dept Admin	Pre-Award GA	Post-Award GA	Agmt Assoc	Research IT Core	Hospital ISO	Partners RISO
Review terms of all RFPs for IS Terms	✓	✓	✓					
Confirm PI is aware of special requirements in IS Terms	✓	✓	✓					
Negotiate IS Terms in proposal with Sponsor, if necessary					✓	✓		
Complete reports or certifications required at proposal	✓	✓	✓			✓		
Upload reports or certifications required at proposal to InfoEd	✓	✓	✓					
Budget for use of Partners Research IT Core in proposal	✓	✓	✓					
[*Rarely]* Approve use of department staff to meet contract						✓	✓	✓
Review and confirm compliance with IS Terms prior to contract signature	✓				✓	✓		

Ensure compliance with ongoing Personnel training and roster requirements	✓	✓				✓		
Contact Partners Research IT Core and Partners RISO 90 days prior to annual report and/or security plan update due date	✓	✓				✓		
Prepare annual reports/security plan updates & secure approval of updates from Partners Research IT Core	✓	✓						
Submit to sponsor /prime with a copy to Research Management Post-Award for uploading to InfoEd	✓	✓		✓				