RESEARCH ADVISORY BOARD
December 18, 2018 8:30-10:00 a.m.
Medical Sciences Building: S-30 & Zoom

AGENDA

Topic	Presenter	Time
1. Export Control	Joan Doherty Campbell	8:30 – 8:40 am
2. Conflict of Interest	Joan Doherty Campbell	8:40 – 8:55 am
3. General European Data Protection Requirements	Tom Poon	8:55 – 9:05am
4. Help with Predatory Journals	Georgina Lopez	9:05 – 9:25am
5. Open discussion		

Remaining 2018 Meetings:

- December 18

2019 Meetings: 2nd Tuesday of each month

- *January 8*
- *February 12*
- *March 12*
- *April 9*
- *May 14*
- *June 11*
- *July 9*
- *August 13*
- *September 10*
- *October 8*
- *November 12*
- *December 10*

RESEARCH ADVISORY BOARD
December 18, 2018 8:30-10:00 a.m.
Medical Sciences Building: S-30 & Zoom
MINUTES

Present: Clarice Estrada, John Ellis*, MC Gaisbauer*, Vanessa Jacoby, Julene Johnson, Marguerita Lightfoot, Georgina Lopez, Irene McGlynn*, Teresa Moeller, Suzanne Murphy, Michael Nordberg, Christine Razler, Elizabeth Sinclair*, Brian Smith, James Sorensen, Matthew Springer, Winona Ward*. Joan Doherty & Tom Poon (guests). Irene Broderick (staff). *=by phone

1. **Export Control**** — Joan Campbell

The goal of export control is to protect U.S. national security and intellectual property; 4 main university activities are affected (UCSF focuses on items 1 & 2):

1. Transfers of controlled information, including technical data, to persons/entities outside the United States (U.S.);
2. Shipment of controlled physical items, such as scientific equipment, that require export licenses from the U.S. to a foreign country;
3. Verbal, written, electronic, or visual disclosures of export-controlled scientific and technical information to foreign nationals ("deemed exports"), even within the U.S.;
4. Travel to sanctioned or embargoed countries for purposes of teaching or performing research

Export Control is governed by 3 governmental agencies:

- Commerce: Bureau of Industry and Security (BIS): Export Administration Regulations (EAR): for Dual-Use, special software
- State: Directorate of Defense Trades Controls (DDTC): International Traffic in Arms Regulations (ITAR): military grade technology, lasers (missile & disease conditions)
- Treasury: Office of Foreign Assets Control (OFAC): Office of Foreign Assets Control (OFAC): work conducted in Cuba or Iran

UCSF's Export Control Policy was issued in June 2018. Recruitment is underway for an export control officer. The UCSF Export Control Workgroup will be reconstituted in 2019. Visual compliance is a critical software tool used by UCSF to verify persons are not on the "restricted party list"; OSR, Procurement, and Finance, currently use this software.

Current issues include the Export Control Reform Act of 2018 as part of the National Defense Authorization Act of 2019 (scrutiny of Huawei, ZTE, Dahua); Department of Defense initiatives directed at universities in the area of cybersecurity; and reconstitution of the federal Emerging Technology and Research Advisory Committee as a new interagency body.

Peili Zhu, UCSF Biosafety Officer focuses on shipping and biosafety issues. Contact Joan Campbell prior to doing any business travel to US-sanctioned countries (such as Cuba). See the UCSF Clinical Research Resource HUB and UCSF Global Health Science & UC Go, contact Joan Campbell, or send an email to export@ucsf.edu for information.

2. **Conflict of Interest**** — Joan Campbell

The Chancellor's Conflict of Interest Advisory Committee (COIAC) consists of UCSF faculty members, ex-officio members ("advisors"), and one public member. Under California law, academic decisions by faculty with outside financial interests must be reviewed by an independent substantive review committee ("ISRC"). At UCSF, the ISRC is known as the COIAC, which acts in an advisory capacity to the EVC/Chancellor.

UCSF Rule 11 currently states that faculty who have, or participate in, a privately sponsored clinical study shall not concurrently receive any compensation from the sponsor, including honoraria and consulting fees, during the course of the study. They shall not have any investment in, or serve in a decision-making capacity, or be an officer or employee of the company sponsoring the study. The only UC campus with this rule is UCSF: it originated in 1994 in the Academic Affairs office. UCSF faculty feel that Rule 11 makes it very difficult for active clinical investigators to work with pharmaceutical companies other than as an investigator which puts them at a disadvantage as researchers.

A UCSF review committee is looking at Rule 11 and propose it be modified to state that faculty who have, or participate in, a privately sponsored clinical study *requiring Institutional Review Board (IRB) approval* shall not concurrently receive any compensation (*with the exception of research-related travel payments*) from the sponsor, including honoraria and consulting fees, during the course of the study (*while IRB approval is required*). The workgroup's report will be presented to the Academic Senate Committee on Research and the EVCP this year.

The Conflict of Interest (COI) Program is currently implementing an electronic disclosure management system to consolidate all COI disclosure types into a single system, offer a shorter annual questionnaire, provide metrics and reporting, and automate several manual processes. The COI is working with the IRB & RMS to analyze intake points, funding streams. The new electronic system will also help manage California Public Records Requests.

3. General European Data Protection Requirements (GDPR)** Tom Poon

GDPR deals with personal data. Effective May 15, 2018, the GDPR deals with the rights of study subjects and strengthens the protection and privacy of personal data for residents domiciled within the EU, including permanent residents, visitors and expatriates. It is broad scope and expands the fundamental rights of a data subject for the life cycle of their personal data; GDPR fines and reporting rules are very strict. UCSF researchers soliciting subjects from EU are subject to GDPR; GDPR impacts data subjects' behavior where the behavior takes place. UC is in the midst of mapping out a system-wide GDPR strategy.

Personal data covered is *any* information relating to an identified or identifiable natural person ('data subject'); select information, such as genetic or biometric data, have elevated protection. Fundamental data rights include that data must be secure, accurate and current, kept in a form permitting identification for no longer than necessary, and collected for specified, explicit and legitimate purposes.

Entities may request data erasure; UCSF must respond in writing within 30 days and the requestor must reply in writing within the following 30 days else the case may be closed. Erasure means *everywhere* data exists. If an investigator receives a destruction request, they should contact the Privacy Office; Privacy will work with IT to determine the data's location, then send out a data destruction notice. Data subjects must be notified in writing of a breach "without undue delay" and where feasible, within 72 hours. UCSF complies with US, not European, law and does not delete medical data.

4. Help with Predatory Journals Georgina Lopez

A UCSF investigator mistakenly submitted an article to the incorrect journal for publication; the journal would not return her article unless she paid them a fee. Open access journals can be the most predatory: they post false information, and use their own ranking systems and impact factors to entice people. This is also a risk for investigators submitting to conferences (AHA, for example). This situation is not unique and happens more often than people realize. For information, view the library web page https://www.library.ucsf.edu/open-access/publishers/; other resources available include http://thinkchecksubmit.org/check/, New Employee Orientation, etc.

5. Open discussion

Deferred due to time constraints.

**Contains excerpts from PowerPoint; see PowerPoint for detail.

UCSF
University of California
San Francisco

Export Control and **Conflict of Interest** (COI) Updates

Research Advisory Board

Joan Doherty Campbell
Associate Director, Office of Ethics and Compliance

Export Control

What are Export Controls?

Goal: to protect U.S. **national security** and **intellectual property**

Four main types of university activities:

1. **Transfers of controlled information**, including technical data, to persons/entities outside the United States (U.S.);
2. **Shipment** of controlled **physical items**, such as scientific equipment, that require export licenses from the U.S. to a foreign country;
3. Verbal, written, electronic, or visual disclosures of export-controlled scientific and technical information to **foreign nationals** (“**deemed exports**”), even within the U.S.;
4. **Travel to sanctioned or embargoed countries** for purposes of teaching or performing research.

Source: https://www.ucop.edu/ethics-compliance-audit-services/compliance/international-compliance/export-laws.html

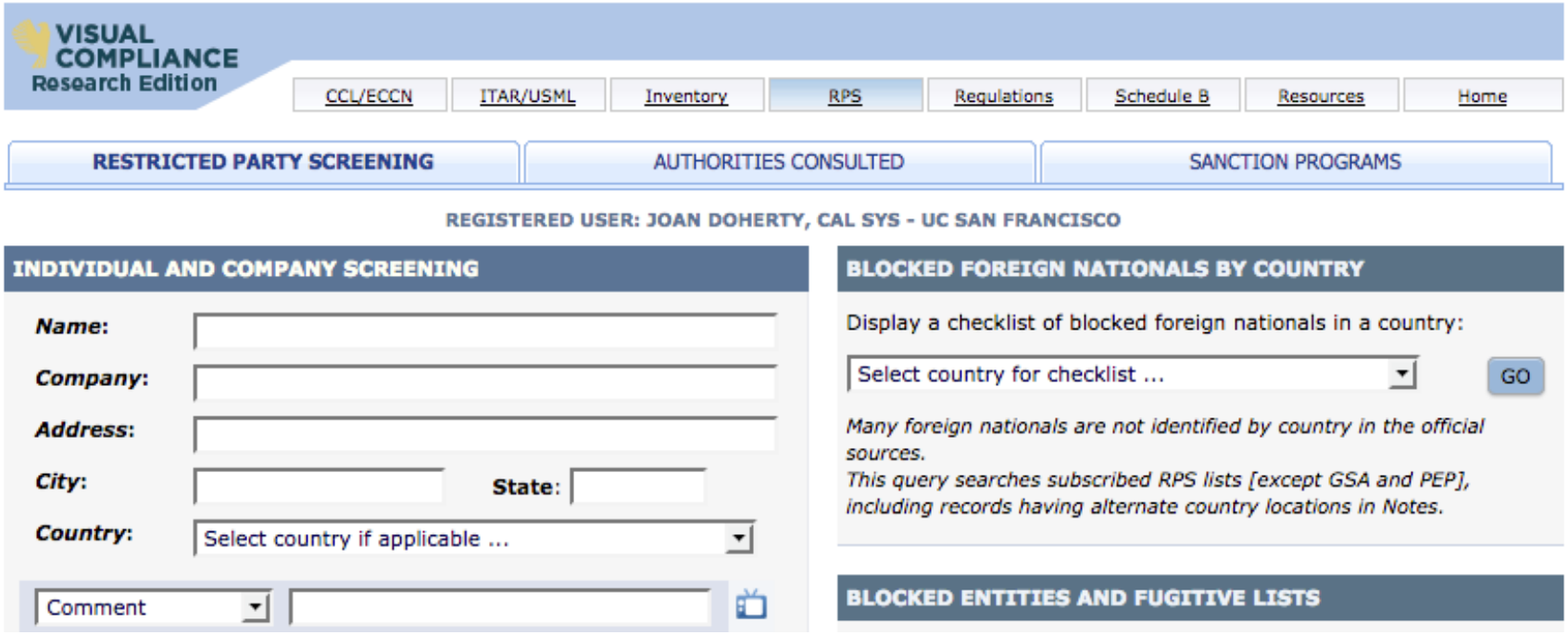
Three Sources of Legal Requirements:

Commerce Department: Bureau of Industry and Security (BIS)	State Department: Directorate of Defense Trade Controls (DDTC)	Treasury Department: Office of Foreign Assets Control (OFAC)
EAR – Export Administration Regulations	ITAR – International Traffic in Arms Regulations	Country-specific sanctions and regulations (*e.g.*, Iran, Cuba)
Commerce Control List	U.S. Munitions List	List of Specially Designated Nationals and Blocked Persons

Source: https://www.ucop.edu/ethics-compliance-audit-services/compliance/international-compliance/export-laws.html

Key Tool: Visual Compliance

Restricted Party Screening for procurement, finance, purchasing, subawards:



UCSF employees can register: https://www.ucop.edu/ethics-compliance-audit-services/compliance/international-compliance/international-screening-tools.html

Export Control Update: Peer Assessment (2017)

Assessed technology controls and compliance:

- Management commitment to the Export Control Program
- Organizational Governance (Export Control Officer, workgroup)
- Policies and Procedures
  - Restricted party screening: individuals, service agreements, shipments, foreign funding, vendors, disbursements.
  - Contract reviews: sponsored research, NDAs, MTAs, sales/service.
  - Technology control plans
  - Process for discovery, escalation, disclosure, and remediation of compliance issues
- Outreach and Training
- Recordkeeping practices
- Self-assessments

Export Control Updates 2018

Addressing recommendations from the peer assessment:

- Implementation of the UC Export Control Policy (June 21, 2018): https://policy.ucop.edu/doc/2000676/ECP
- UCOP training for export control contacts
- Appointment of an Export Control Officer
- Hiring a full-time Export Control Officer

Hot topics:

- Export Control Reform Act of 2018 as part of the National Defense Authorization Act of 2019 (scrutiny of Huawei, ZTE, Dahua);
- Department of Defense initiatives directed at universities in the area of cybersecurity;
- Reconstitution of the federal Emerging Technology and Research Advisory Committee as a new interagency body (seeking comments).

Export Control 2019

Identify subject matter experts for UCSF Export Control Workgroup:

- Controller's Office
- EH&S
- Global Health Sciences
- Government & Business Contracts (GBC)
- Human Resources
- Industry Contracts (ICD)
- Information Technology Services (ITS)
- International Students & Scholars Office (ISSO)
- Legal Affairs
- Mail Services
- Office of Ethics & Compliance
- Office of Technology Management (OTM)
- Police
- Research Management Services (RMS)
- Risk Management
- Supply Chain Management
- Other?

Export Control 2019

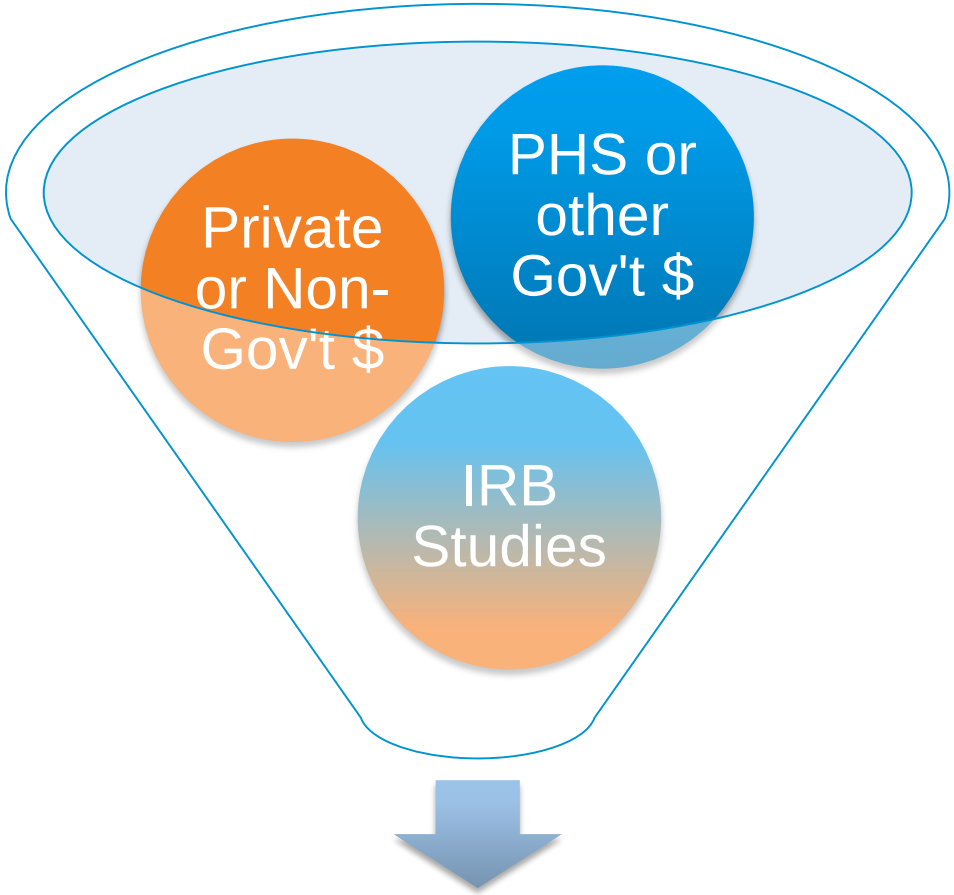
UC campuses are hosting the annual conference of the Association of University Export Control Officers (AUECO) in San Diego:

Conflict of Interest (COI) in Research

The Chancellor's Conflict of Interest Advisory Committee (**COIAC**) consists of **UCSF faculty** members, ex-officio members ("advisors"), and one public member… Under **California law**, academic decisions by faculty (including research and teaching decisions) with outside financial interests must be reviewed by an **independent substantive review committee ("ISRC")**. The President of the University of California delegated this responsibility to the chancellors of the ten campuses. At UCSF, the Chancellor delegated the responsibility to the Executive Vice Chancellor for Research (EVC). The **ISRC is known as the COIAC**, which acts in an **advisory capacity to the EVC/Chancellor**.

Source: COI Advisory Committee Composition and Procedure

Common COIAC review types



COI Rule 11:

11. **Faculty** who have, or participate in, a **privately** sponsored clinical study shall not **concurrently** receive any **compensation** from the sponsor, including honoraria and consulting fees, **during the course of the study**. In addition, they shall not have any **investment** in, or serve in a **decision-making capacity** for (such as service on the Board of Directors or management committee), or be an **officer** or **employee** of the **company** sponsoring the study.

Source: A Faculty Handbook for Success: Advancement and Promotion at UCSF (Appendix IV, UCSF Guidelines on Conflict of Interest)

Does UCSF need "Rule 11"?

- Faculty raised concerns:

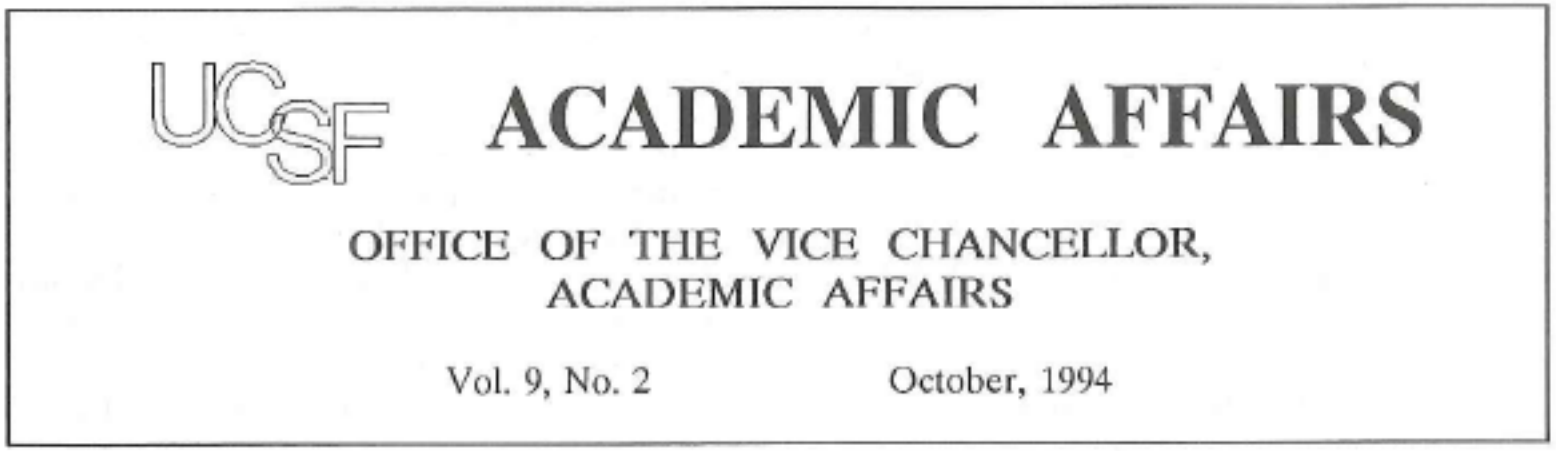
  Between the interpretation of Rule 11 and the COMP plan for clinical faculty, it appears to have become ***virtually impossible for active clinical investigators to work with pharmaceutical companies*** *other than as an investigator…*

  …*it is* ***putting UCSF faculty at a distinct disadvantage as researchers…***

- COIAC response:
  - In April 2018 the COIAC began reviewing the origin/authority of Rule 11, its current utility, and whether it should be revised or discarded.
  - Planned to report back to the Committee on Research after six months.

Historical Background

A search for documentation from October 1994 yielded the following:



UCSF ACADEMIC AFFAIRS

OFFICE OF THE VICE CHANCELLOR,
ACADEMIC AFFAIRS

Vol. 9, No. 2 October, 1994

UCSF GUIDELINES ON CONFLICTS OF INTEREST PERTAINING TO RECEIVING OR DISBURSING RESEARCH FUNDS

The following guidelines, written by the Chancellor's Advisory Panel on Relations with Industry (CAPRI) and approved by the Academic Senate and the Academic Vice Chancellor, are offered to help faculty understand and manage their relationships with the private, for-profit sector. They may be amended or revised from time to time to reflect changes in policy.

1. When a faculty member accepts a full time appointment at the University it is understood that he or she will accord the University his or her primary professional effort and will arrange outside professional obligations, financial interests, and activities so as not to conflict or interfere with this commitment to the University.

Faculty Concerns

- Need to be able to travel to investigator meetings, but sponsors wish to avoid transaction costs associated with amending clinical trial agreements.
- Need to be able to participate in broad discussions of future research that are not associated with a specific protocol (*i.e.*, “we should have a seat at the table”).

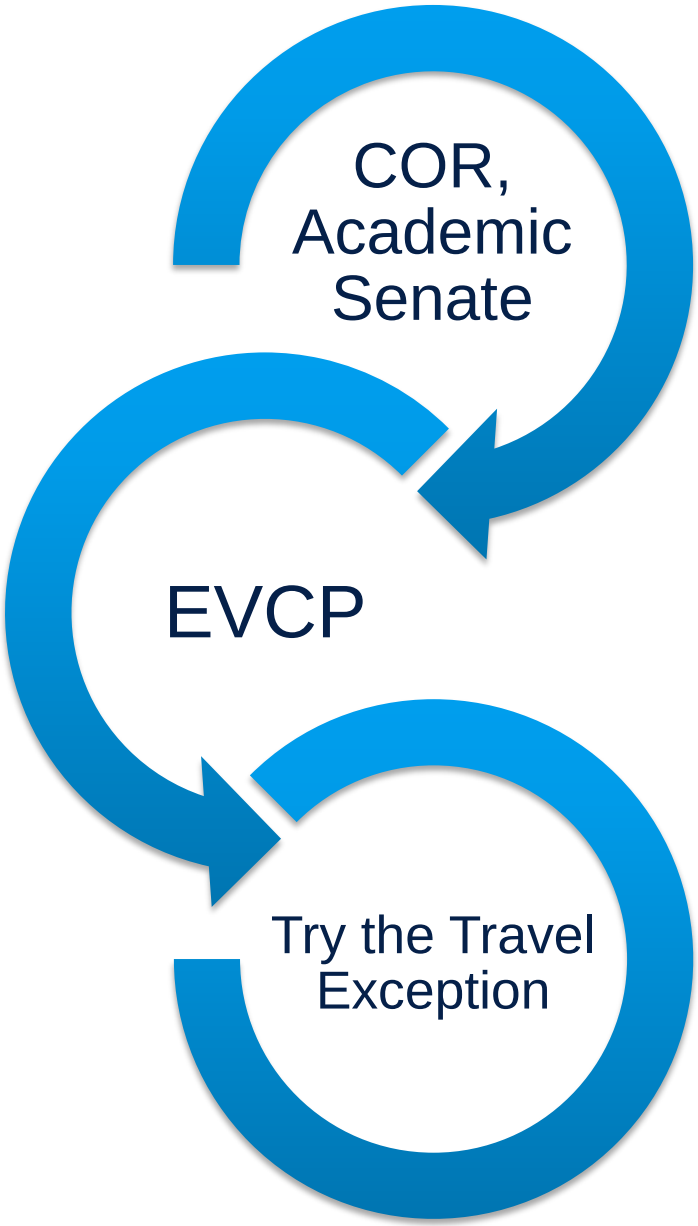
Clarifications

- **Scope**: Payments incorporated into a clinical trial agreement are NOT personal payments to the investigator, so Rule 11 is not implicated.
- **Contracts**: Changes in contracting practices require that consulting agreements formerly executed on behalf of the Regents must now be signed by individual faculty, which implicates Rule 11.
- **Travel**: Many potential Rule 11 conflicts could be eliminated if “compensation” did not include travel payments.

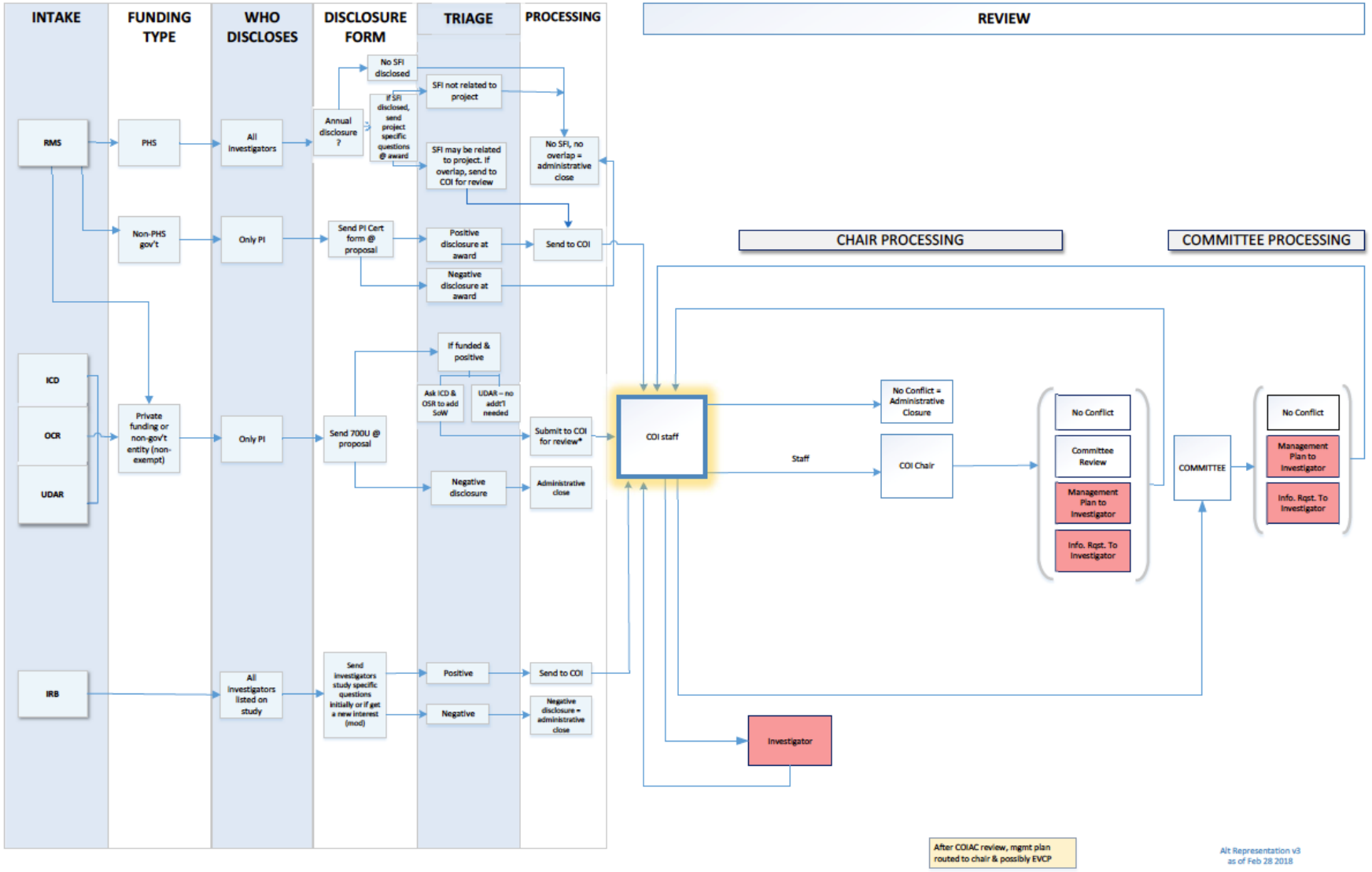
Proposed clarifications:

11. Faculty who have, or participate in, a privately sponsored **clinical study** **requiring Institutional Review Board (IRB) approval** shall not concurrently receive any **compensation** (with the **exception of research-related travel payments**) from the sponsor, including honoraria and consulting fees, during the **course of the study** (**while IRB approval is required**). In addition, they shall not have any investment in, or serve in a decision-making capacity for (such as service on the Board of Directors or management committee), or be an officer or employee of the company sponsoring the study.

Next Steps

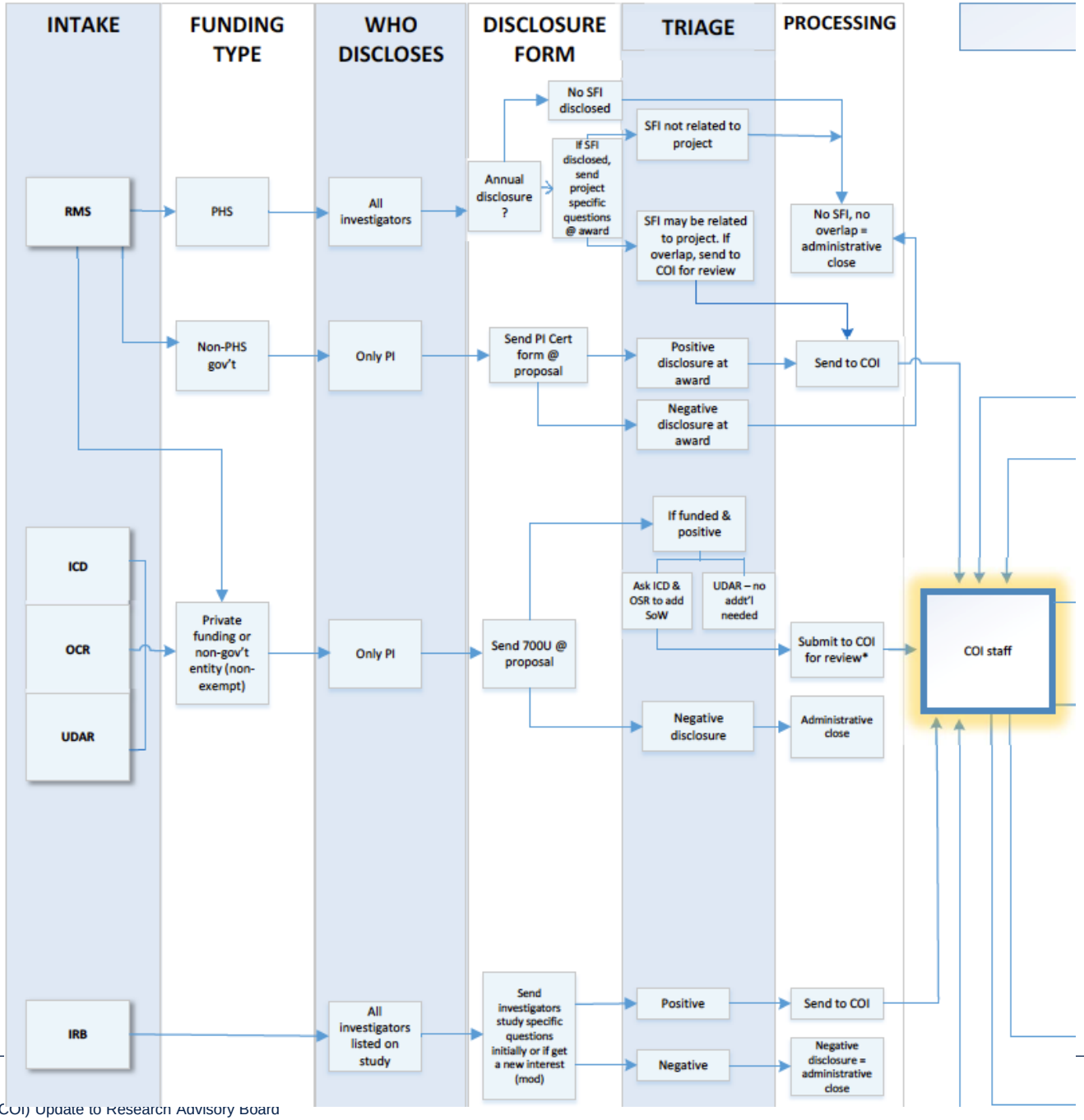


What do we need from a COI disclosure system?



Integrate COI disclosures into the grants/contracts/gifts and IRB workflows

COI staff worked with key stakeholders from RMS and IRB to design integration points

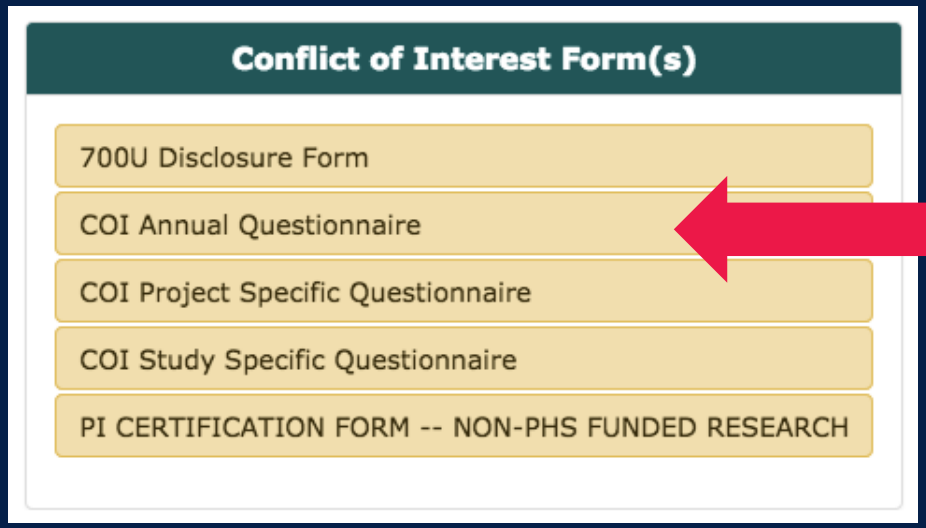


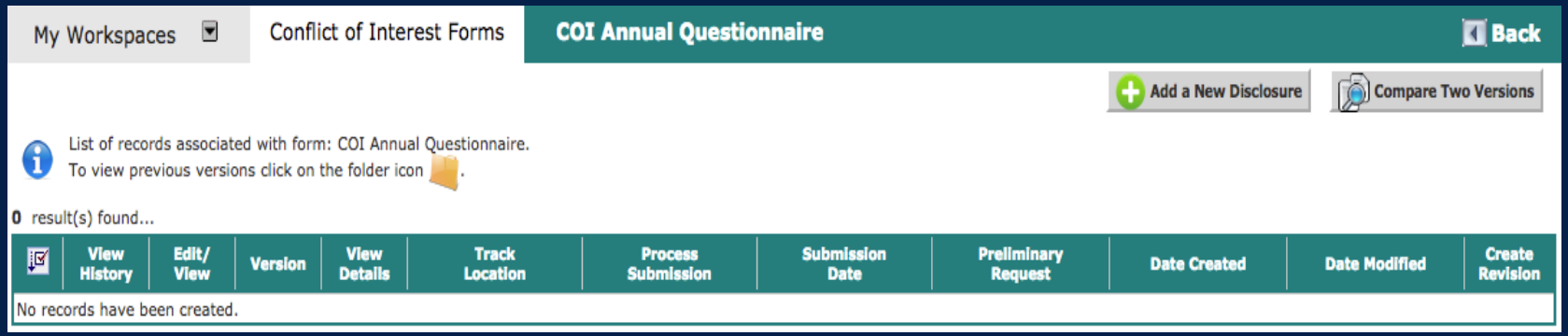
Key Enhancements

- **Consolidation** of all COI disclosure types into a single electronic system;
- **Shorter Annual Questionnaire**, designed to obtain the minimum PHS-required information at the time of proposal submission;
- **Electronic 700-U Form** for privately-sponsored research and **PI Certification Form** for non-PHS government funded research;
- In-depth questions about the relationship of a discloser's financial interests to a specific project will be **deferred until UCSF receives notice of a funding award** (Project-Specific Questionnaire);
- **Improved reporting** on key metrics to better track turnaround times.
- Investigators added to an IRB application (initial or modification), will **automatically receive a brief COI questionnaire** to address financial interests **related to the specific IRB** protocol;
- Research Services Coordinators and IRB Coordinators can **check a single page for the status of COI reviews for all investigators** related to a specific funding proposal (in eProposal) or IRB protocol (in IRB iRIS);
- **Communication** between investigators and the COIAC will be managed within the system, with automatic email notifications issuing to UCSF email addresses.

ANNUAL QUESTIONNAIRE (PHS)

iMedRIS **Annual Questionnaire** + **Project-Specific** if needed





700-U FORM (private & non-gov't sponsor)

Future: iMedRIS 700-U Questionnaire

All Tasks | Study Tasks | Project Tasks

Task List: All

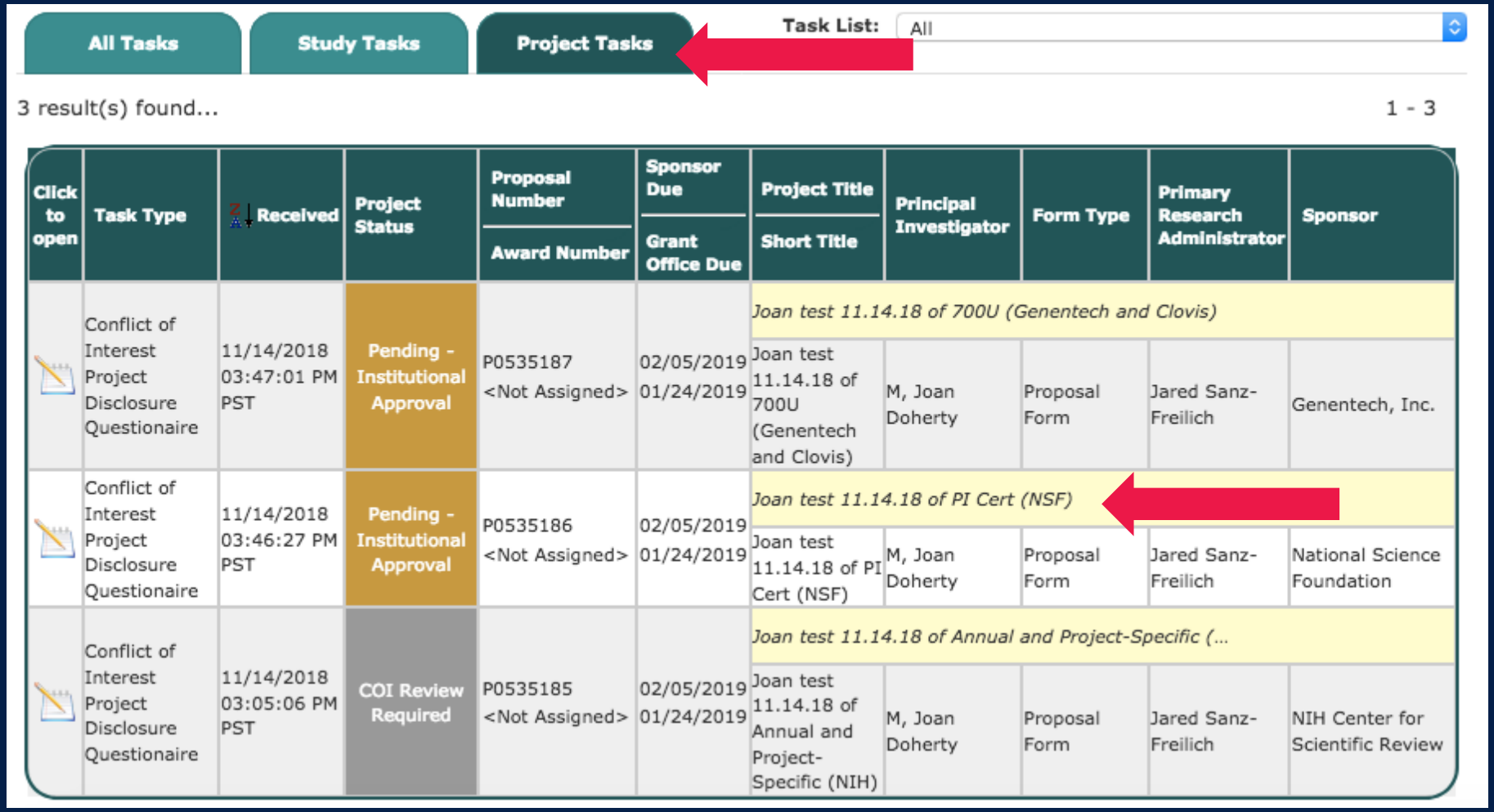
3 result(s) found... 1 - 3

Click to open	Task Type	Received	Project Status	Proposal Number / Award Number	Sponsor Due / Grant Office Due	Project Title / Short Title	Principal Investigator	Form Type	Primary Research Administrator	Sponsor
	Conflict of Interest Project Disclosure Questionaire	11/14/2018 03:47:01 PM PST	Pending - Institutional Approval	P0535187 <Not Assigned>	02/05/2019 01/24/2019	*Joan test 11.14.18 of 700U (Genentech and Clovis)* / Joan test 11.14.18 of 700U (Genentech and Clovis)	M, Joan Doherty	Proposal Form	Jared Sanz-Freilich	Genentech, Inc.
	Conflict of Interest Project Disclosure Questionaire	11/14/2018 03:46:27 PM PST	Pending - Institutional Approval	P0535186 <Not Assigned>	02/05/2019 01/24/2019	*Joan test 11.14.18 of PI Cert (NSF)* / Joan test 11.14.18 of PI Cert (NSF)	M, Joan Doherty	Proposal Form	Jared Sanz-Freilich	National Science Foundation
	Conflict of Interest Project Disclosure Questionaire	11/14/2018 03:05:06 PM PST	COI Review Required	P0535185 <Not Assigned>	02/05/2019 01/24/2019	*Joan test 11.14.18 of Annual and Project-Specific (...* / Joan test 11.14.18 of Annual and Project-Specific (NIH)	M, Joan Doherty	Proposal Form	Jared Sanz-Freilich	NIH Center for Scientific Review

UCSF

PI CERTIFICATION (NSF, DOD, NASA)

Future: iMedRIS PI Certification Questionnaire



All Tasks | Study Tasks | Project Tasks — Task List: All

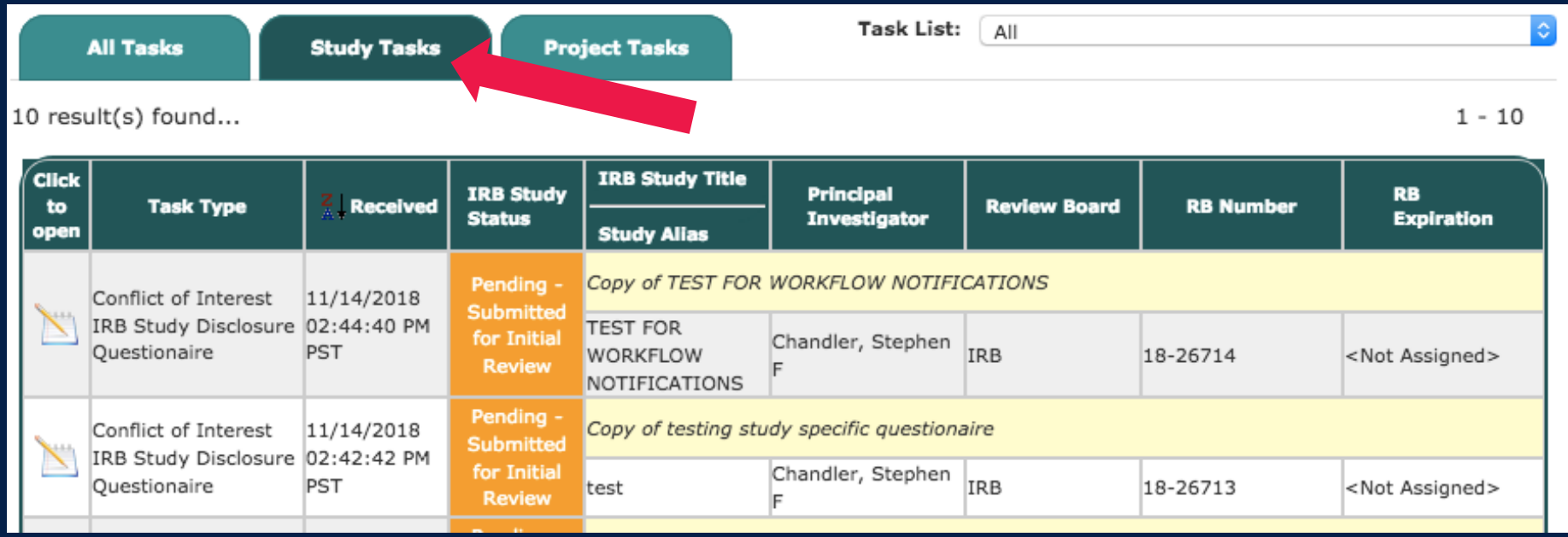
3 result(s) found... 1 - 3

Click to open	Task Type	Received	Project Status	Proposal Number / Award Number	Sponsor Due / Grant Office Due	Project Title / Short Title	Principal Investigator	Form Type	Primary Research Administrator	Sponsor
	Conflict of Interest Project Disclosure Questionaire	11/14/2018 03:47:01 PM PST	Pending - Institutional Approval	P0535187 <Not Assigned>	02/05/2019 01/24/2019	*Joan test 11.14.18 of 700U (Genentech and Clovis)* / Joan test 11.14.18 of 700U (Genentech and Clovis)	M, Joan Doherty	Proposal Form	Jared Sanz-Freilich	Genentech, Inc.
	Conflict of Interest Project Disclosure Questionaire	11/14/2018 03:46:27 PM PST	Pending - Institutional Approval	P0535186 <Not Assigned>	02/05/2019 01/24/2019	*Joan test 11.14.18 of PI Cert (NSF)* / Joan test 11.14.18 of PI Cert (NSF)	M, Joan Doherty	Proposal Form	Jared Sanz-Freilich	National Science Foundation
	Conflict of Interest Project Disclosure Questionaire	11/14/2018 03:05:06 PM PST	COI Review Required	P0535185 <Not Assigned>	02/05/2019 01/24/2019	*Joan test 11.14.18 of Annual and Project-Specific (...* / Joan test 11.14.18 of Annual and Project-Specific (NIH)	M, Joan Doherty	Proposal Form	Jared Sanz-Freilich	NIH Center for Scientific Review

UCSF

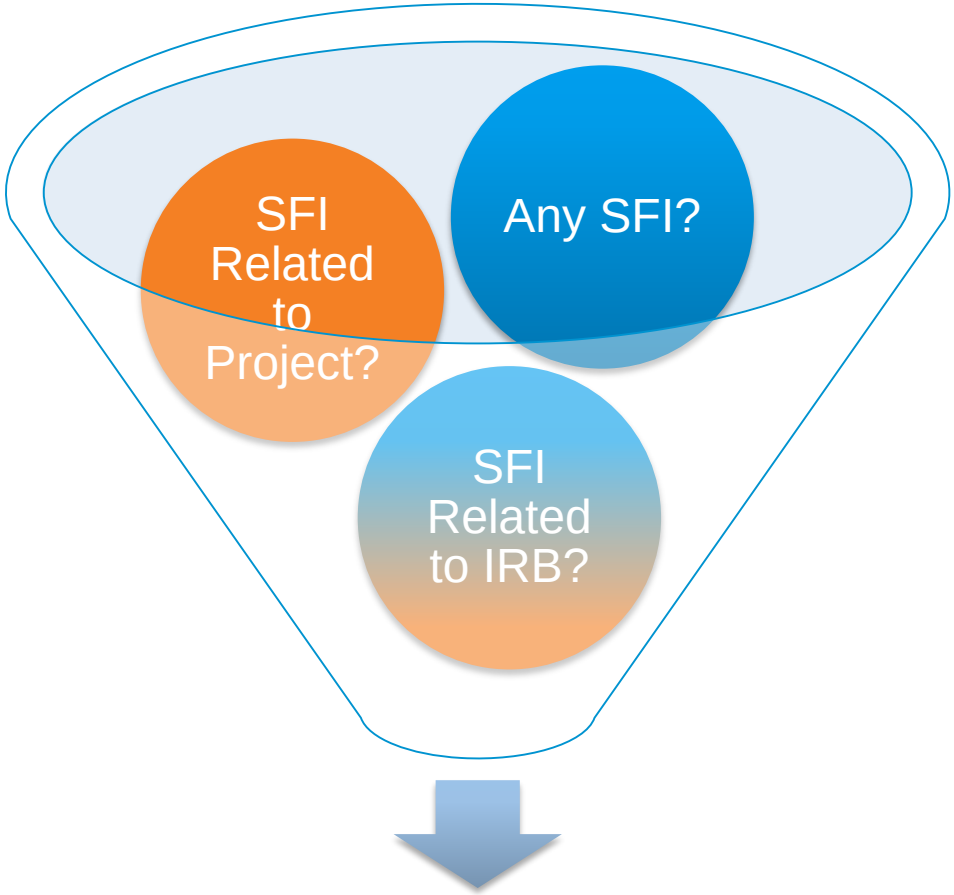
IRB-RELATED COI DISCLOSURE

Future: Each investigator answers a brief iMedRIS COI Questionnaire



Click to open	Task Type	Received	IRB Study Status	IRB Study Title / Study Alias	Principal Investigator	Review Board	RB Number	RB Expiration
	Conflict of Interest IRB Study Disclosure Questionaire	11/14/2018 02:44:40 PM PST	Pending - Submitted for Initial Review	*Copy of TEST FOR WORKFLOW NOTIFICATIONS* / TEST FOR WORKFLOW NOTIFICATIONS	Chandler, Stephen F	IRB	18-26714	<Not Assigned>
	Conflict of Interest IRB Study Disclosure Questionaire	11/14/2018 02:42:42 PM PST	Pending - Submitted for Initial Review	*Copy of testing study specific questionaire* / test	Chandler, Stephen F	IRB	18-26713	<Not Assigned>

Goal: Funnel the disclosures for COI review



We need YOU for user acceptance testing!

Image source: https://goo.gl/images/teSH59

UCSF

University of California
San Francisco

UCSF

University of California
San Francisco

The General Data Protection Regulation (GDPR)

Privacy Compliance Steering Committee (PCSC)

Tom Poon, CHPC
Privacy Office

12/18/2018

Disclaimer

- GDPR is an evolving topic, with multiple/competing goals
- Regulators are updating guidance
- UC is in the midst of mapping out a system-wide strategy
- The level of impact to UC (and to UCSF) is being studied and will drive investment
- ***Whether GDPR impacts a unit is dependent upon whether it applies to the data being processed, taking into consideration scale and intent***

The EU/EEA General Data Protection Regulation (GDPR)

- What is the GDPR?
- Scope of GDPR
- Special Categories of Data
- Fundamental Rights
- Roadmap Ahead
- Breach Notification
- Fines/Penalties and Damages
- GDPR in One Slide
- Questions

What is the GDPR?

- A comprehensive **data protection law** that repeals and replaces national data protection laws in the European Union (EU)/ European Union Economic Area (EEA) with a single set of rules, directly enforceable in each EU member state (plus Norway, Iceland and Lichtenstein). UK will enact same/similar regulation.
- Strengthens the protection and privacy of **personal data** for residents domiciled within the EU, including **permanent residents, visitors** and **expatriates**
- Applies to **processors** and **controllers** of personal data
- Applies to organizations outside the EU **that offer goods or services** to EU citizens or **monitor the behavior** of EU data subjects
- Took effect on May 25, 2018

What is the GDPR?

USA

- Laws create a right of privacy where it is needed – sectoral approach
  - Health: HIPAA
  - Students: FERPA
  - Financial: GLBA, FCRA
  - Marketing: TCPA, TSR, CAN-SPAM
- State laws like CMIA - The Confidentiality Of Medical Information Act (CMIA)
- Thinking: Does anything say we can't?

EU/EAA

- Privacy is a fundamental and uniform right
- Umbrella regulation
  - Broad scope
  - Broad responsibilities
- Thinking: You can't unless something says specifically you can

Source: Robert Smith, UCOP

Scope of GDPR

- Addresses:
  - What types of data may be collected under specific circumstances
  - How data must be secured
  - How data must be disposed
  - Expands **fundamental rights** of a data subject for the life cycle of their personal data
- Imposes:
  - Obligations and penalties
  - Strict breach notification rules

Scope of GDPR

- An **"establishment"** in the EU
  - Operating an office in the EU
- Processing activities related to:
  - Offering of **goods or services** to data subjects in the EU
    - Recruiting students, faculty, staff
    - Consultative services to health care providers or patients
    - Financial aid
    - Online learning, **websites**
  - **Monitoring data subjects' behavior** where the behavior takes place in EU
    - Research of individuals located within the EU
- Transfer of personal data from EU to outside the EU (in the US)

Scope of GDPR

- **Personal data** - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- Examples:
  - IP addresses and cookie identifiers
  - Contact information
  - Behavioral information
  - ID numbers

Special Categories: Elevated Protection

Processing of personal data revealing:	Prohibited unless:
• Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data • Data concerning health • Sexual orientation • Data concerning a natural person's sex life	**Explicit consent**
	Vital interests of data subject where incapable of giving consent
	Related to personal data made public by the data subject
	Substantial public interest
	Preventive or occupational medicine
	Public health
	Archiving purposes in the public interest, **scientific or historical research**, statistics

Fundamental Rights

Personal data must be:

Processed pursuant to a lawful basis	• 6 possible “lawful bases” • Examples: consent, necessary for performance of a contract, compliance with a legal obligation, public interest
Collected for specified, explicit and legitimate purposes; no further processing	• Right to restriction of processing • Transparency • Specific and minimal processing
Adequate, relevant and limited to what is necessary	• Right of access • Specific and minimal processing
Accurate, kept up to date	• Right to rectification • Right to erasure
Kept in a form permitting identification for no longer than necessary	• Right to object • Right to erasure
Secure	• Implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk • Examples: encryption, pseudonymisation, backups

Breach Notification – Supervisory Authority

- To the supervisory authority:
  - Notification of a data breach must take place "without undue delay, and, where feasible, not later than **72 hours** after having become aware of it."
  - If all info not feasible in 72 hours, can provide in phases
- Required elements of notification:

  (a) The nature of the personal data breach including the categories/number of **data subjects** and of personal **data records** concerned;

  (b) Name, contact details of contact point for more info;

  (c) Description of likely consequences of the breach;

  (d) Description of the measures taken/proposed to be taken to address the breach and any risk mitigation measures

Breach Notification – Data Subject

- To the affected data subject(s):
  - Notification of a data breach must take place “without undue delay.”
- BUT can avoid notice to data subject if:
  - Data accessed/lost/used was encrypted;
  - Controller took subsequent measures to ensure the risk to the data is no longer likely to materialize;
  - Would involve disproportionate effort. Alternative: Public communication or other similar measure

Breach Notification – Data Subjects (cont'd)

- Required elements of notification:
  - Description in clear and plain language the nature of the breach
  - Name, contact details of contact point for more info;
  - Description of likely consequences of the breach;
  - Description of the measures taken/proposed to be taken to address the breach and any risk mitigation measures

Fines/Penalties and Damages

- Fines for noncompliance may go up to €20M ($28M+) or 4% of annual revenue, whichever is greater
- Non-profit and public interest bodies may claim compensation on data subjects' behalf
- Data subjects who suffer material or non-material damage as a result of a breach or violation of the GDPR have the right to receive compensation from the controller or processor of the data for damage suffered

Roadmap Ahead: UCSF

- UCSF Privacy is convening a GDPR Task Force to examine the impact of GDPR at UCSF, develop compliance strategies and implement a compliance program
- UCSF Privacy website (https://hipaa.ucsf.edu) will have a GDPR-specific segment with resources by June 15
- Information sessions will be held on GDPR with attendance by UCOP:
  - Mission Bay Auditorium: Friday, June 22 – 9:30-10:30
  - Parnassus HSW 301: Friday, June 22 – 11:30-1:00
- UCSF Privacy will be emailing notices, information via Managers' Weekly and other widely distributed newsletters

GDPR in One Slide

- Effective date – May 25, 2018
- Core principles
  - Lawfulness (legal basis)
  - Transparency
- Participants
  - Data subjects = natural persons in EEA
  - Data controllers
  - Data processors
  - Supervisory Authorities
- All personal data – special rules for 'sensitive data'
  - Broader than US – e.g., IP address
- Explicit consent freely given & revoked
- Data subjects have rights
  - Transparency, Erasure, Rectification, Specific and Minimal, Portability
- Limits automated processing impacting individuals
- GDPR follows the data!
  - Impacts big data where ID is possible
- Data breach notification 72 hours after discovery
- Fines up to €20M ($28M+) or 4% revenue
- Things UC (probably) must do:
  - Inventory and record processing activities
  - Data Impact Assessments for high risk processing
  - Security and data protection by design – process and systems
  - Have contract clauses
  - Create consent forms, notice practices and "lawful basis"
  - Support data subject rights
  - Support notification requirements

Source: Robert Smith, UCOP

University of California
San Francisco