



CONTRACTS & GRANTS OFFICE

SANTA BARBARA, CALIFORNIA 93106-9490

May 16, 2018

Re: Protections of Personally Identifiable Information (PII) - Requirement to report suspected breach  
To: GGSE all-academic, GGSE all-students

Good morning - See below for new NSF requirements regarding reporting breach of information but also a reminder of required process for any suspected breach of human subjects Personally Identifiable Information (PII).

Dear Colleagues,

Effective March 1<sup>st</sup> 2018, NSF has implemented [new Research Terms and Conditions](#) potentially affecting research projects at UC Santa Barbara. Article 35 of the [Agency Specific Requirements](#) state that,

***“Grantees that use or operate a Federal information system or create, collect, use, process, store, maintain, disseminate, disclose, or dispose of Personally Identifiable Information (PII) within the scope of an NSF award, must have procedures in place to respond to a breach of PII. These procedures should promote cooperation and the free exchange of information with NSF, as needed to properly escalate, refer and respond to a breach. Grantees will notify NSF upon learning that a breach of PII within the scope of an NSF award has occurred.”***

PII can generally be defined as any information/data that could potentially be used to identify a specific individual. Examples of PII include, but are not limited to, names, SSNs, driver’s license numbers, medical information, etc.

This notification serves to inform you that any suspected breach of PII within the context of **an NSF supported award (research, contract, or training grant)**, should be reported to the Office of Research as soon as possible. **This includes PII that is collected as a part as an IRB approved research study at UCSB or at a sub-awardee collaborator’s site, AND also includes any PII collected about participants or trainees in an NSF Training Grant.**

**A PII breach can be defined as a security incident in which sensitive, protected or confidential data is suspected to have been copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.**

We want to remind all human subjects researchers that under the context of an IRB approved protocol, a breach of PII, regardless of funding source, would also constitute an adverse event/unanticipated problem (i.e., loss of confidentiality) and thus, according to the [Unanticipated Problems or Adverse Events SOP](#), be reported to the HS Office within 1 week of PIs knowledge of the incident.

Examples of data breaches include, but are not limited to:

- Loss/theft of device/computer/server storing PII or documents with PII
- Hacking of device/computer/server storing PII including any suspected malware or ransomware infection of device
- Insecure electronic transmission of PII (e.g., using email to transmit confidential information)

- Loss/theft of passwords or password storing software
- Insecure or unauthorized disposal of devices/computers or documents with PII

For more information about protecting the confidentiality of UC information and data please go to the [UCSB Information Security website](#).

For any questions or concerns about this notification please contact Research Integrity Programs Manager, Melodie Blakemore at [melodie\\_simoni@ucsb.edu](mailto:melodie_simoni@ucsb.edu).

If you suspect a breach of any data or information has occurred at UC Santa Barbara, please contact the Chief Information Security Officer immediately at [security@ucsb.edu](mailto:security@ucsb.edu).

Thanks,  
Melodie Blakemore, CPIA  
Research Integrity Programs Manager, UCSB  
Office of Research, 3227 Cheadle Hall  
Santa Barbara, CA 93106-2050  
805-893-4286 (Office)  
805-893-2166 (Fax)