



Protecting Personal Information at Fermilab: Advanced Refresher Course

Irwin Gaines – Lab Privacy Committee
Chair

What You Will Be Reminded Of

□ Basic training

- You are not allowed to have any PII that “belongs” to Fermilab on your devices or file space, to send any PII through email, or to extract any PII on mobile devices

□ Advanced training

- Certain individuals need to work with Fermilab PII as part of their job responsibilities. You must abide by the restrictions about where this PII resides and how it is processed



Kinds of Personal Information

- PII (Personally Identifiable Information) is any information that specifically identifies an individual; not all needs to be protected (example: my name and email address)
- “Protected” PII is PII that has a significant risk of identity theft if improperly disclosed (such as social security numbers) or significant violations of individual privacy (such as detailed health records); full definition on next slide
- “Laboratory” PII is PII collected and maintained by Fermilab as part of a business process (such as bank account numbers so you can be paid).
- These rules apply to electronic versions of Laboratory Protected PII



What is Protected PII?

- 
- At Fermilab, Protected PII is defined as an individual's name in combination with one or more of the following items:
 - social security number or foreign national ID number
 - passport number or visa number
 - driver's license number
 - personal credit card number
 - bank account number
 - date and place of birth (both together, not one by itself)
 - mother's maiden name
 - security clearance information
 - biometric information (fingerprints, retinal scan, DNA)
 - criminal records
 - detailed personal financial information (not merely salary history)
 - detailed medical records
 - detailed educational transcripts (not merely a list of degrees)

Your Obligations

- ❑ You must not have any Laboratory Protected PII on any of your computers. Even as an “advanced” user who needs to access lab PII, you cannot have any on your own computers, or in email, or on mobile devices.
- ❑ “Your computer” means any computer that you are the sole user of and any file space you have on shared systems or servers. System administrators will NOT examine users’ files; this is the responsibility of each user.
- ❑ These rules apply to all computers, personally or laboratory owned, connected to laboratory networks.
- ❑ Since your job requires you to process lab PII, the rest of the slides discuss the proper ways of processing and protecting this information.





Handling Fermilab PII

- This data is only allowed to be resident on servers that are accessed through our Citrix portal, which requires multifactor authentication (MFA) and is protected by a firewall. This includes PeopleSoft, Oracle Financials, FermiWorks and a secure file server
- Access is restricted to users with a demonstrated business case and with management approval
- All processing of data takes place on the virtual desktops reached through the Citrix portal; **no PII data can be moved outside this portal.**

Example: FermiWorks

- ❑ Most users have accounts which do not allow access to any of the lab PII contained in FermiWorks, so they can log in from any browser on any system and upload and download data as necessary.
- ❑ Even users that need PII access (privileged users) can access FermiWorks from the general internet to do normal work. They will be restricted to only the non-PII areas of FermiWorks.
- ❑ When such users need access to the PII in FermiWorks, they must access FermiWorks through the browser inside the Citrix portal MFA environment. Only when FermiWorks sees you logging in from that location will it allow access to PII. Any reports, extracts, or other data summaries containing Protected PII required by users may only be stored on servers inside the portal (where it can be accessed by other privileged users); it cannot be transmitted through email, downloaded to portable devices, and can only printed on secure printers.





Direct questions to Division/Section Privacy Reps

- AD: Tom Kroc
- CD: Irwin Gaines
- ND: Stephanie Schuler
- PPD: Luz Jaquez
- TD:
- ESH&Q:
- FESS: Odarka Jurkiw
- FIN: Mike Rosier
- WDRS: Heather Sidman