



# Protecting Personal Information at Fermilab



# Outline

- Why must we protect personal information?
- What is Protected Personally Identifiable Information (Protected PII)?
- What are your obligations?



## Why?

- Identity theft based on improper disclosure of personal information is a serious problem
- Several government agencies have been embarrassed by losses of large quantities of personal data
- Orders from White House --> DOE --> Office of Science mandate more careful treatment of personal information
- Fermilab deeply respects the privacy of employees and users

# 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 Protected PII on any of your computers
- ☞ You will need to sign a statement that you have inspected your computers and deleted any Protected PII you discovered
  
- ☞ “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.



# Examples of PII that must be deleted

- Resumes or transcripts containing social security numbers or other Protected PII
- Conference databases with credit card numbers or visa numbers
- Spreadsheets with credit card or passport numbers of division/section travelers
- Word documents of trip reports or foreign travel forms containing passport numbers or other Protected PII
- Note that it is OK to enter Protected PII into external databases (like FTMS for foreign travel) as long as no local copies of reports containing things like passport numbers are kept on your computer.



## For more information

- ☞ If you need to access any of the Protected PII maintained by the laboratory (for example, in HR or financial databases) you will need additional training about proper procedures
- ☞ If you think you have a business need for keeping PII (or have any other questions) contact your division/section privacy representative



# Division/Section Privacy Reps

➔ AD

➔ CD

➔ PPD

➔ TD

➔ BSS

➔ Directorate

➔ ES&H

➔ FESS

➔ FIN

➔ HR