Fermilab Procedures for Protected PII (Personally Identifiable Information)

Background

This document provides the detailed procedures in use at Fermilab to implement the lab policies about protected personally identifiable information (Protected PII). In particular, while it is expected that physical versions of documents containing Protected PII will be protected in similar ways, these procedures apply only to electronic copies of Protected PII.

Definition of 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 identification 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)

This list will be periodically reviewed by the lab information categorization committee, and changes will be communicated to all employees.

Inventory of Protected PII

The information categorization committee carried out an inventory to identify all known locations of Protected PII at the laboratory. All computing systems containing this identified Protected PII are subject to the following procedures. However, it should be noted that the storage of a single incidental or accidental piece of Protected PII referring to a single individual, while highly discouraged, is not enough to cause the entire computing system to be treated as a Protected PII containing system.

PII Procedures

- **General prohibition**

  As a general rule, individuals are not permitted to have any Protected PII on their computers or in data on general use servers. Protected PII is restricted to the specific systems discussed below, each of which is contained within a moderate level Major Application (MA). (Note: a Major Application is a lab defined collection of computing systems with a common set of

risks and security procedures, generally more stringent than the lab baseline. Moderate level specifies a set of NIST defined security controls, again more stringent than the lab baseline.)

There are two separate types of Protected PII containing systems. The first, called "Enterprise Protected PII systems", maintains Protected PII that needs to be accessed from other systems and individuals around the laboratory, normally over the lab network. The second, called "Local Protected PII systems", maintains Protected PII that is only needed by a small number of individuals who can access the system directly, not over the network.

- **Enterprise Protected PII Systems**

Business and operational processes exist at the lab which require users dispersed across the laboratory to access Protected PII from lab-wide systems. While this Protected PII is centralized in a few servers in moderate level Major Applications, network access to the data is required to operate the laboratory.

The primary example of this type of PII is the laboratory financial and human resource management systems operated by the MIS department.

For this type of PII access, the following procedures and controls apply:

1) For each database containing Protected PII, the specific Protected PII data contained therein will be inventoried and documented.

2) User accounts are granted access to these systems according to the "least privilege principle". This means that accounts are not granted access to Protected PII data by default.

3) Remote access allowing a user access to only his/her own, personal Protected PII is exempted from procedures covering remote access to Protected PII. Access controls must be in place to ensure such a user is prevented from accessing any other person's Protected PII.

4) Access allowing a user to view any other person's Protected PII data is defined as privileged access. Privileged access is granted only to a documented list of specific users based on demonstrated business need and with management approval.

5) A list of specific network segments and addresses will be identified in the associated Major Application plan as being permissible for use for privileged access. These network segments and addresses will have additional security controls applied to the network and computers, defined in the Major Application plan, which enforce restricted access to Protected PII. This list of network segments and addresses must be fully contained within the site General Computing Enclave (GCE) accreditation boundary. Network access to Protected PII from these network segments and addresses will not be subject to the two-factor authentication and inactivity timeout remote access requirements.

6) Privileged access from network segments or addresses not identified in the MA plan must conform to the Fermilab requirements for remote access to Protected PII (two factor authentication and 30-min inactivity timeout).

- **Local Protected PII Systems**

There are a small number of additional laboratory systems that contain Protected PII information, but where the information only needs to be accessible to a small number of centralized users. These systems will be contained within the moderate level Protected PII Major Application, which, beside the standard moderate level security controls, will also have the following controls to protect the information:

1) Physical controls: Systems and data are physically controlled by remaining in designated restricted access rooms
2) Network access controls: These systems will not be connected to the lab general use network. Where the system consists of more than one machine, these machines may be connected together by a dedicated, controlled network, but this network may not interconnect to any other networks at any time, nor will modem or other remote access methods be allowed
3) User access controls: System access will be limited to a documented list of user accounts

At the present time this Major Application contains the portion of the radiation badge data base that contains information about specific users (including social security and passport numbers) and the neutron therapy facility (which contains patient medical records).

- **Protected PII Incidents**

Any suspected loss of Protected PII should be reported through the standard channels for urgently reporting a suspected computer security incident (calling x2345). This will result in the FCIRT on-call being paged, who will know how to report the Protected PII incident to CIAC.

- **External delivery of Protected PII**

There exist certain statutory and operational requirements for the lab to deliver Protected PII to outside entities. This includes radiation badge exposure, tax, pension, payroll, and payment data. In these cases, Fermilab will establish acceptable minimal care standards to be exercised in the transmission of Fermilab PII data to the external entity. If the external entity is unable or unwilling to comply with these standards, the entity must provide an explanation for this position in writing to Fermilab. In turn, Fermilab must document a risk assessment applying to PII data exchange with the outside entity that evaluates and accepts the risk of exchanging PII data with the outside entity. This risk assessment must be reviewed and approved by Fermilab management prior to the exchange of PII data with the outside entity.

- **Privacy Committee**

The lab will maintain an information categorization committee, made up of individuals from all divisions and section, appointed by division/section heads, with a chair appointed by the ISSM. This committee will meet at least annually to evaluate information protection policies and procedures, to evaluate any need for moving any additional systems into the Protected PII Major Application, and to determine if items need to be added to the list of Protected PII. However, the onus remains with the owner of any new potential Protected PII containing computing systems to notify the Privacy committee.

- **User Requirements**

All user accounts with access to Protected PII will be granted based on demonstrated business need and with explicit management approval.

All privileged users granted access to Protected PII will sign a statement agreeing not to download any Protected PII to computer systems or portable media. (Download means moving copies of PII to a local machine or portable media where the PII data persists on the machine or media and would be compromised if the machine or media were stolen or lost). Any reports, extracts, or other data summaries containing Protected PII required by users may only be stored on servers within the Major Application.

All users will be required to attend appropriate training on handling Protected PII. There are several levels of user Protected PII training: the first for all lab employees, visitors and contractors; the second for only those individuals who have privileged access to Protected PII; the third for management; and the fourth for anyone who would establish Protected PII data exchange agreements for the laboratory:

1) General user training: this will emphasize the definition of Protected PII, the general prohibition against possession of Protected PII, and the procedures for reporting suspected loss of Protected PII. All users will sign a statement confirming that they have understood this material. Ordinarily it will be part of the regular computer security training classes.
2) Privileged users training: this will emphasize the restrictions against downloading Protected PII to local machines, the procedures for remote access to Protected PII systems, and reporting procedures for suspected loss of Protected PII. Completion of this training will be required before privileged access to systems containing Protected PII is allowed.
3) Management training: this will emphasize management's role in enforcing lab Protected PII policies and being aware of any potential Protected PII on systems for which they are responsible.
4) Contract officer training: this training is required by anyone at the lab with the authority to enter into an agreement for the laboratory that could involve the exchange of Protected PII data with any outside entity. This training would emphasize the restrictions, minimal care standards, and necessary terms and conditions required for any such agreement.