

Planning an SSN Compliance Campaign

Checklist for Department Heads & Administrators

<http://www.rochester.edu/it/policy/documents/checklist.pdf>

1. Communication

- Present, or invite a privacy officer to present, the SSN-PII policy and related Data Classification and Record Retention policies at meetings of:
 - department administrators
 - department managers
 - department faculty
 - department staff
- Announce the availability of secure paper disposal methods
 - shredders
 - locked toters
- Include SSN-PII disposal in periodic Clean & Go Green days in the department

2. Discovery

- Personnel files (including I-9s) in individual offices and in the department office
- Department-developed forms that currently or have previously required SSN
- Finance files, e.g. salary administration, older cum salary reports
- Research files (especially W-9s) in individual offices and in the department office
- Student records
- HRMS reports or extracts or screen-prints
- Contracts with outside parties who are maintaining a data collection for the department
- Infection case report forms
- Unemployment insurance forms
- Faculty file cards and roster databases
- Archival (dead) storage on-site or at outside location, such as Iron Mountain
- Department-developed applications and databases (a.k.a. shadow systems)
- Saved e-mail, both received and sent
- "Home" directories and department or project file directories on file servers
- Backup tapes from departmental systems
- Microfiche, CDs, DVDs, flash ("thumb") drives, external disk drives
- Ask long-serving employees about past departmental practices that included SSN

3. Reduction

- Review the Record Retention policy and dispose of obsolete records (<http://www.rochester.edu/adminfinance/records.html>)
- Where possible, remove SSN from records that will be retained

- Consolidate storage of SSN records, for example, in the department office or a central file server
- Change department workflow so that copies of SSN are rarely needed
 - Remove SSN from circulating paper files, such as student applications and patient records
 - Minimize e-mailing or faxing records containing SSN
 - Minimize extracting records containing SSN from central databases and information systems
 - Minimize including fields on paper forms that invite the submitter to provide SSN
 - Minimize including fields on Web sites that invite the submitter to provide SSN

4. Protection

- Electronic
 - Move records containing SSN to a file server in the University Data Center and access them there
 - Encrypt records containing SSN that must be outside the University Data Center. This includes records on Departmental servers:
 - Individual computers – desktops and laptops and PDAs
 - Storage devices – flash ("thumb") drives, external disk drives
 - Media – CDs, DVDs
- Paper and microfiche
 - At the end of the work day, these records containing SSN should be stored in a locked cabinet in a locked room

5. Disposal

- Electronic
 - If the record is stored on a file server in the University Data Center, you may just delete the SSN or the record
 - If the record is encrypted, you may just delete the SSN or the record
 - If the record is stored on write-once media, such as CD-R, you must destroy the media
 - Otherwise you must overwrite the record or destroy the media
- Paper and microfiche
 - Shred
 - Securely transfer to an approved secure waste disposal company, for example, via a locked toter for paper disposal

6. Registration

- If you still possess a data collection containing SSN, or you are responsible for determining who is permitted to access a data collection containing SSN, register the collection with a Privacy Officer (SSNRegistry@rochester.edu) of the University.