



Evangelical Lutheran Church in America

God's work. Our hands.

Congregation Identity Theft Education Program



Evangelical Lutheran Church in America
God's work. Our hands.

Definition - PII

- ❑ Personal Identity Information (PII) is defined as any data that can be used by a third party to steal an individual's or **entity's** identity and use it to fraudulently establish financial obligations in the name of the victim.
- ❑ PII includes full names, Social Security numbers, TIN numbers, addresses, birth dates, financial data, and bank account or credit card numbers.



Identity Theft Statistics

1. Identity theft complaints have grown from 230,000 in 2000 to over 1.2 million in 2008 (a 530% increase), even with enhanced data security technology.

2. Defensive technology **reacts** to new fraud tactics.

3. Sources of Fraud and Identity Theft:

Internet/Email	63%
Mail	14%
Phone	7%
Other	16%



Data Security Quiz

- Question - What are these things, and what do they have in common?
 - HIPAA - Health Insurance Portability & Accountability Act
 - GLBA - Gramm-Leach-Bliley Act
 - SOX - Sarbanes-Oxley
 - Red Flag –Red Flag Rules Compliance
 - PCI – Payment Card Industry Data Security Standards
- Answer – They are all government and industry attempts to protect Personal Identity Information (PII).



What Thieves Do with Congregation's PII Data

- ❑ Open new credit card accounts in the congregation's or congregants' names.
- ❑ Create counterfeit checks using the congregation or congregants' names or account numbers – quickly draining bank accounts.
- ❑ Open a bank account and write bad checks.
- ❑ Take out a loan in victim's name.



Data Security Risks

- ❑ Incoming and outgoing Internet traffic
- ❑ Cyber Space – Website and WI-FI connections
- ❑ Remote access
- ❑ Outbound email
- ❑ Garbage cans
- ❑ Portable media devices (i.e. laptops, flash drives, CDs)



Data Security Defenses

- ❑ Firewalls/Anti-Virus/Spyware and/or passwords.
- ❑ Routine monitoring of remote users and employee systems access.
- ❑ Internet restrictions.
- ❑ Identification and classification of high risk data (PII).
- ❑ Policies & procedures covering use of high risk data residing in:
 - Desktop computers
 - Emails
 - Paper documents
 - Portable media devices (disks, flash drives and laptops)
 - Disposed documentation



Managing PII - Data Classification

- ❑ Restricted – Can be shared at data owner's discretion.
- ❑ Public – Published without restrictions.
- ❑ Confidential – PII - Only given to those who need information to complete job functions and never shared beyond congregation.



Managing PII – Systems Access

1. Set employee systems access commensurate with job duties (via password protection). Avoid passwords that allow access to entire system.
2. Review employee access on a periodic basis, ensuring all terminated employees' access have been removed & all active access is appropriate.
3. If temporary access is required, ensure it is revoked in a timely manner.



Managing PII – Handling Data

1. Do not download PII or confidential information unless it is absolutely necessary.
2. Set desktop screen containing PII to require a sign in after three minutes or sooner.
3. Never leave reports containing PII data in an unsecured area, even in your office, if you are not there.
3. Upon disposition, all documentation containing PII must be shredded.



Where PII Resides

- ❑ Your desktop computer
- ❑ Email
- ❑ Remote access
- ❑ Portable media devices (disks, flash sticks, and laptops)
- ❑ In “Cyber Space”
- ❑ Paper reports
- ❑ In your garbage can
- ❑ Archives and records retention



PII on Your Desktop

1. Ensure confidential data residing on your desktop is protected by backup procedures.
2. Do not disable any passwords needed to access your desktop. Use hard-to-guess passwords for your personal login. *Do not share your password!*
3. Set your default security screen to automatically engage after three minutes of non-activity.
4. *Never download PII to your desktop unless it is absolutely necessary for the task at hand!*



PII Contained in Email

1. Be aware that emails or attached documents can include PII. If not essential to the purpose of the email, do not include this information.
2. If a document containing PII must be emailed, add a password to electronic documents (encryption is best).
3. *Remember, control of PII and confidential data is lost when emailed unless it is password protected.*



Remote Access to PII

- ❑ Create remote access policy & ensure all staff is educated in remote access use.
- ❑ Ensure remote access is critical to executing job requirements.
- ❑ If temporary access is required, ensure it is revoked in a timely manner.
- ❑ Remote access should be reviewed by management on a periodic basis to ensure all terminated employees have been removed and all active employee's access is appropriate.



PII Residing on Portable Media Devices

- 1. Never download PII data to a portable media device!!!*
2. If you must...inform appropriate level of management of your intentions to download PII data and obtain permission.
3. Password and/or encryption protect the PII data.
4. Eliminate all downloaded PII related data when no longer needed.



PII Residing in Cyber Space

1. PII or confidential data should *never* be placed on your Website.
2. Even if not placed on your Website, verify your webmaster has engaged the proper security controls so that browsers can not gain access to PII or confidential data residing “behind” the Website.
3. Never use WI-FI technology when you are working on PII or confidential data. Anyone in the area can “grab” your information in cyber space and immediately download it to their computer.



PII in Paper Form

- 1. Do not print anything containing PII or confidential information unless it is absolutely necessary !!!*
2. Ensure that all print-outs containing PII or confidential data are stored in a locked file cabinet when not in use, and shredded when no longer needed.
3. If a report containing PII data needs to be distributed, ensure that it is distributed on a “need to know” basis and the recipient understands its confidential nature.



PII Residing in Your Garbage Can

- ❑ Never throw away documents containing PII! These documents must be shredded!!!
- ❑ Anyone coming in contact with this documentation may use the data to perpetrate an identity theft or other fraud.



PII & Records Retention

1. Ensure all PII or confidential data that is no longer needed on site, but must be retained for a period of time, is sent to the archives or a secured location in a timely manner.
2. Ensure all documentation containing PII or confidential data which is no longer needed is shredded in the presence of a staff member.



Questions?

- If you have any questions or suggestions about data security, please feel free to contact:

Mike McKillip, Director for Internal Audit

Telephone: (773) 380-2768

michael_mckillip@elca.org

