

# Security Awareness and Protecting PII and PHI



**CMS Eligibility Support  
Project Management Office**  
*For Internal Government Use Only.*

**CLOSE HOLD - DO NOT SHARE INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW:** This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

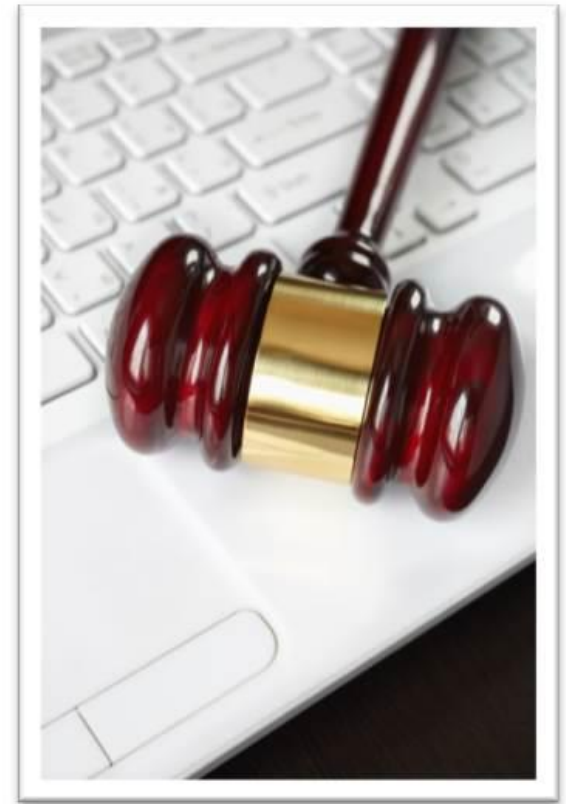
# Privacy and Security

# What is Information Privacy?

- It is the privacy of personal information collected, stored, and shared
- Privacy concerns exist wherever personally identifiable information (PII), protected health information (PHI) or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise
- Laws, regulations, and standards provide the specific rules we must follow when dealing with PII or PHI

# Privacy Laws

- **E-Government Act 2002, Title II and III**  
Requires federal agencies to assess and control the effect on privacy of systems that collect information about members of the public.
- **Privacy Act of 1974**  
Provides guidance for collecting, using, managing, and disclosing personal information by federal agencies.



## Privacy Laws, continued

- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule**  
Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

# Why is this Important to Us?

- We are *entrusted* with the personal information of people for who we provide **our interpretation services**
- **Our contract** with CMS specifies that we will protect consumer information according to CMS and Federal requirements
- **Our business** depends on reliable and secure operation

# Need-to-Know

Do not discuss classified, confidential, or controlled information with family members or anyone else without establishing a confirmed need-to-know

- Your role as an interpreter
- Security clearance (if applicable)
- Contract, sensitive, or proprietary Information
- Technology



# PII/PHI Overview

- As an interpreter, you routinely come into contact with sensitive data such as names, Social Security numbers, and financial information





# What is PII?

PII is information that can be used to distinguish or trace an individual's identity

- Alone (biometrics), or
- When combined with other personal or identifying information that is linked or linkable to a specific individual (full name and DOB)

# Biometrics

Are distinctive, measurable characteristics that can be used to identify an individual; examples include but not limited to:

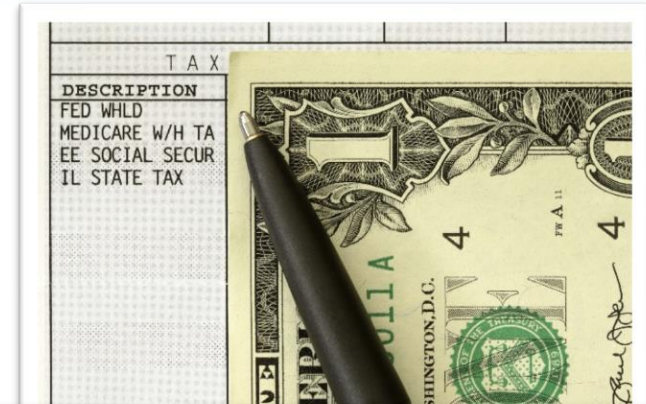
- Fingerprints
- Retina
- DNA
- Iris
- Voice
- Hand/finger vein patterns



# Common Identifying Information

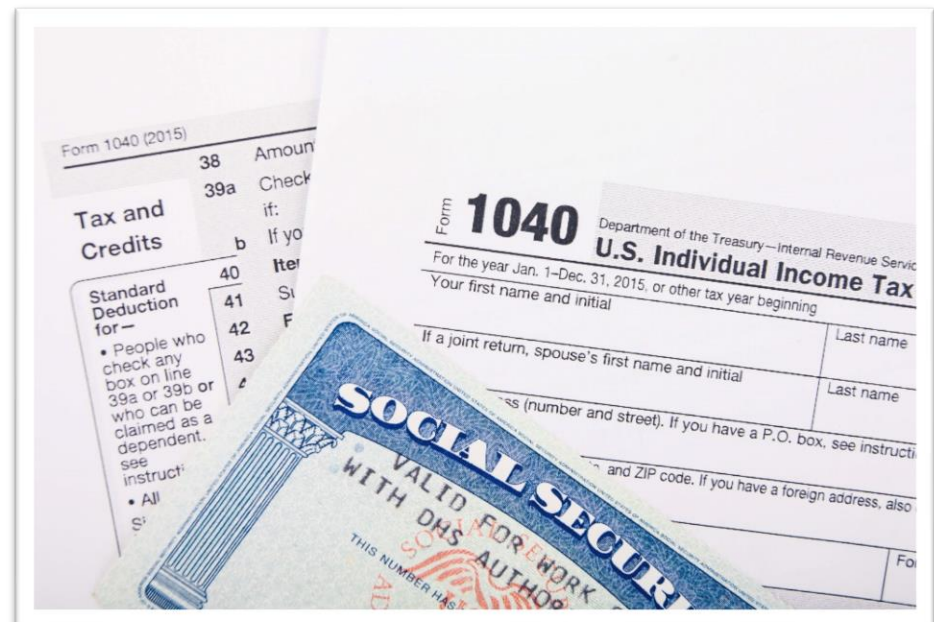
We must protect:

- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Email address
- Driver's license number
- Passport number
- W-2s
- Pay stubs



# PII You May Handle

- SSN–ID number
- Title II–income information
- Financial



# SSNs

Misuse of SSNs can put individuals at risk for identity theft, take appropriate precautions:

- Use the SSN only when required
- Disclose SSNs only to those with a need to know and authorization to receive the information

# What is PHI?

PHI is any personal and health information that is:

- Individually identifiable.
- Created about past, current, or future physical and/or mental health condition of a specific individual.
- PHI often contains PII.

# How We Get It?

During an interpretation, certain hospital and medical records from the consumer may be translated during a live interpretation assignment.



# Examples of PHI

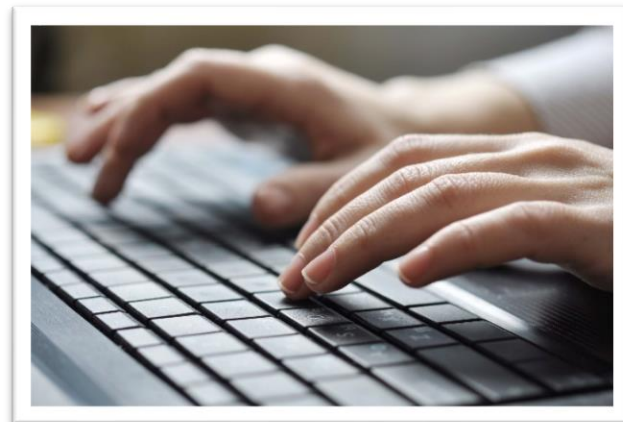
- Information on medical records or bills
  - Any related PII
  - Linkable code or any other unique identifying number
  - All elements of dates\*\* (except year) for dates directly related to an individual, including dates of admission, discharge, or service, and date of birth/death
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Device identifiers and serial numbers
  - Any other unique identifying number, characteristic or code



# Working with PII and PHI

Key aspects of security when processing consumer information:

- Necessity (need-to-know)
- Confidentiality
- Data Integrity
- Quality



# Your Responsibilities

- You must protect consumers' privacy through every step of the application process
- Your responsibility includes:
  - Applying privacy principles while handling PII, PHI and sensitive information
  - Reporting any possible misuse of data as soon as it occurs to: LSA's Compliance Department 215-259-7000 ext 55141

# What is a Data Breach?

A data breach is an incident in which sensitive, protected or confidential data (e.g. PII or PHI) has potentially been viewed, stolen or used by an individual unauthorized to do so.



# Reporting a Breach of Privacy

- Immediately inform your supervisor or LSA's Compliance Department representative of a data breach (or suspicion of a breach)
- Do not investigate the incident on your own
- Anyone can report an incident - it's your responsibility



# Privacy Violations

Can result in but not limited to:

- Suspension and/or termination
- Fines or criminal charges



# Summary

Keeping consumer's information safe is a shared responsibility:

- LSA utilizes numerous security protocols to ensure that PII and PHI is safe and secure at all times
- You applying privacy principles while handling PII/PHI and sensitive information and following Acceptable Use policies



# Knowledge Check

What is Personal Information?

Any information that can be used to distinguish or trace and individual identity.

What is Person Health Information?

Any information about health status, health care or payment of health care.

How do you report a security violation?

Contact LSA's Compliance Department.

- Jodi Bralow [jbralow@LSAweb.com](mailto:jbralow@LSAweb.com) or 215-259-7000 x55141
- Call our Anonymous Hotline at 833-234-4831