



**PRIVACY  
POLICY**

**CAN I SHARE THIS  
SENSITIVE PII WITH  
COWORKERS AND  
OTHERS?**

October 2015

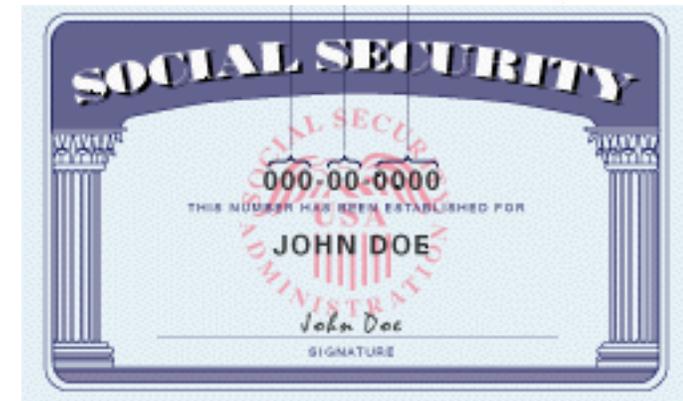
# WHAT IS PRIVACY?

“The rights and obligations of individuals and organizations with respect to the collection, use, disclosure and disposal of personal information.” Generally Accepted Privacy Principles.



# WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)?

All information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information, Federal Tax Information, Payment Card Industry data, etc. PII is contained in public and non-public records.



# YOUR PII CHART™

Take time to inventory the identity relationships you have with the companies, organizations, and individuals you entrust with your personally identifiable information or PII. See how your identity is a PII Chart™, a picture of relationships you've created. Once you visualize the slices of your PII, managing your identity assets becomes easier.

## LEGEND

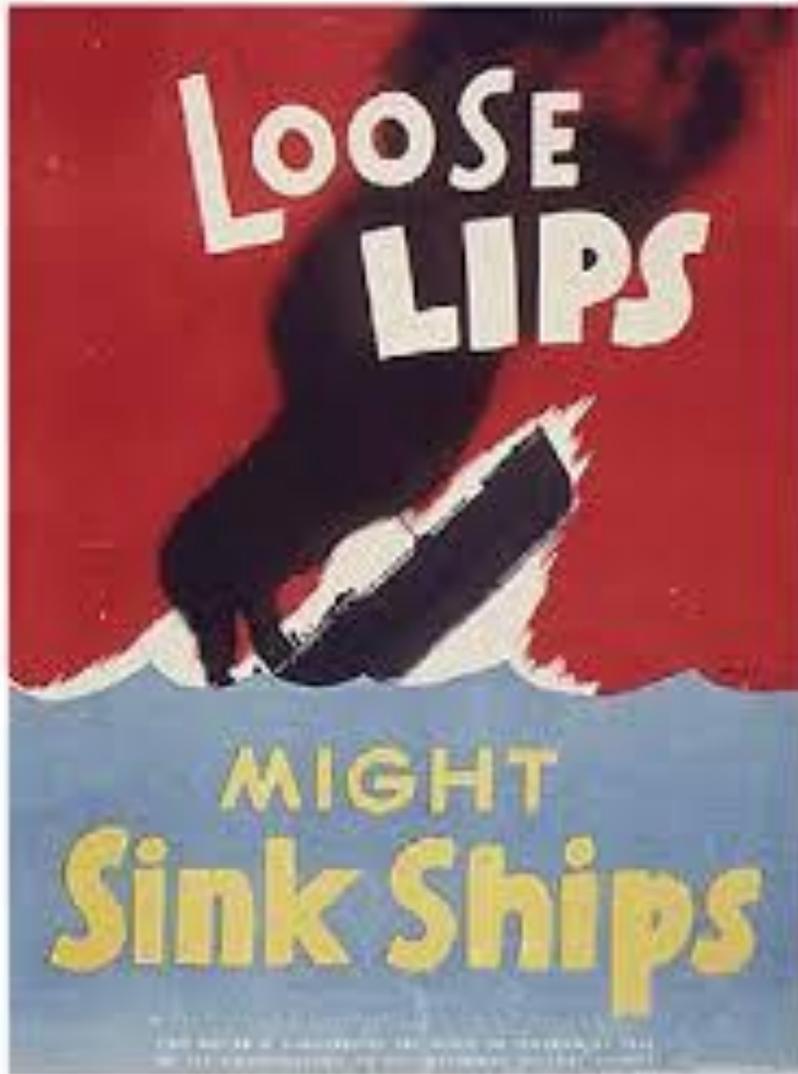
- SSN SOCIAL SECURITY NUMBER**
- CONTACT INFORMATION**  
(email address, physical address, telephone and mobile numbers)
- GOVERNMENT-ISSUED IDENTIFICATION**  
(driver's license, passport, birth certificate, library card)
- BIRTH DATE, BIRTH PLACE**
- WWW ONLINE INFORMATION**  
(Facebook, social media, passwords, PINs)
- GEOLOCATION**  
(smartphone, GPS, camera)
- VERIFICATION DATA**  
(mother's maiden name, pets' and kids' names, high school, passwords)
- MEDICAL RECORDS INFORMATION**  
(prescriptions, medical records, exams, images)
- ACCOUNT NUMBERS**  
(bank, insurance, investments, credit cards)



# PRIVACY PRINCIPLES

- The Privacy Program is based upon these six **Privacy Principles**, consistent with law and policy.
- Compliance is required for all Executive Branch Departments.
- Additional information on the Privacy Principles can be obtained on the West Virginia State Privacy Office website:  
<http://www.privacy.wv.gov/Pages/default.aspx>





## Sensitive PII (SPII)

Those elements of PII that must receive heightened protection due to legal or policy requirements.

### Examples:

- Social Security numbers
- Credit card numbers
- Health and Medical data
- Driver license numbers
- Individual financial account numbers
- Discipline or grievance information

# QUESTION 1



Is the info you want to share SPII?

## QUESTION 2



Did you verify that sharing the SPII is allowed?

Hint: Check out the Security Safeguards and Minimum Necessary and Limited Use Policies at [www.privacy.wv.gov](http://www.privacy.wv.gov)

## QUESTION 3



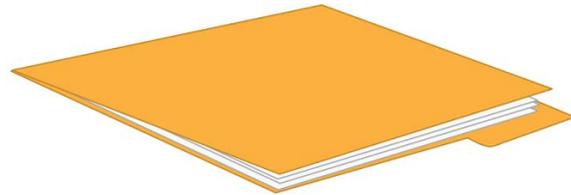
Have you verified that everyone you are sharing the SPII with has a business need to know?

## QUESTION 4

Patient's entire  
medical history



What you  
actually need



Will you share only the  
minimum amount of SPlI to  
accomplish the business  
need?



# **The End is Near!**

**Learn these secrets  
before it's too late.**



# HYPOTHETICAL

An HR Director has been asked by the Cabinet Secretary to review employees' use of sick leave and evaluate whether there are abuses.

The report that the HR Director creates to answer the Secretary's question pertains to employees supervised by 9/10 of the Secretary's managers. Managers are interested in receiving this information.

How should the HR Director share the information requested by the Secretary?



# HYPOTHETICAL

A trainer is enrolling 100 employees from across the Executive Branch in mandatory training.

It is possible that there will be multiple people with the same name.

The trainer is required to generate a report to the Governor's Cabinet showing which employees have been trained.

What PII should the trainer collect to identify the employees enrolled in the training?

What PII should go on the report to the Cabinet? Is there a difference?



# HYPOTHETICAL

In its systems, the State has PII on every employee, including SSN, DLN, DOB, home address, maiden name, education, financial account numbers, etc.

Let's assume that the State is implementing a new system that will seamlessly direct deposit employees' paychecks into their accounts.

How should the new system owners collect each employees' financial account numbers? Or should they?

