PRIVACY ACT BASICS

What You Need to Know About Protecting Personally Identifiable Information (PII)

DEFINITIONS: WHAT IS PII?

PII stands for Personally Identifiable Information.

- Definition: Information which can be used to identify a person uniquely and reliably, including but not limited to name, social security number (SSN), address, telephone number, e-mail address, mother's maiden name, etc.

YOU NEED TO KNOW ABOUT PRIVACY BECAUSE…

- It's information we are collecting, maintaining, distributing, and disposing of about you!
- It also requires you to take precautions when collecting, maintaining, distributing, and disposing of PII required by your job.
- It's a factor in developing best business practices.
- It contains both civil and criminal penalties for noncompliance.

IHS PRIVACY ACT (PA) RESPONSIBILITIES

- Establish rules of conduct for collecting, maintaining, distributing, and disposing of personal information.
- Publish PA system of records notice in the Federal Register for all approved privacy collections of information.
- Ensures collection of data that is only authorized by law.
- Data is only shared with those individuals having an official need-to-know.

IHS PA RESPONSIBILITIES

- Establish and apply data safeguards to protect information from unauthorized disclosure.
- Allow individuals to review records about themselves for completeness and accuracy.
- Allow individuals to amend their personal records regarding factual information that is in error.
- Keep a record of disclosures made outside of IHS to authorized “routine users” described in the PA system notice.

What is Privacy Sensitive and Requires Protection

- Financial, credit, and medical data
- Security clearance level
- Leave balances; types of leave used
- Home address and telephone numbers (including home web addresses)
- SSN
- Mother's maiden name; other names used
- Drug test results and the fact of participation in rehabilitation programs
- Family data
- Religion, race, national origin
- Performance ratings
- Names of employees who hold government-issued travel cards, including card data

WHY DO WE COLLECT PII ABOUT YOU?

We need it to

- Hire you
- Retain you
- Pay you
- Separate you
- Compensate you
- Locate you
- Educate you
- Discipline you
- Rate you
- Provide services to you

YOU HAVE THE RIGHT TO:

- Request copies of the records we are maintaining on you
- Designate a person to have access to information about you: parent, spouse, friend, attorney, congressman, colleague, etc.
- Seek amendment of any factual inaccuracies (not opinions)
- Understand how long records will be maintained before being accessioned or destroyed
- Appeal any denial of information

WHEN MOVING FROM PAPER TO ELECTRONIC: THINK PRIVACY

- Moving from a paper process into an electronic process requires you to identify any risks that would subject personal information to compromise. In other words, yesterday's medical record, when moved from paper to an electronic means, may open us up to a potential privacy breach.

- For example, using a DOD/Navy Scenario: Promotion lists for FLAG OFFICERS containing full names and SSNs were sent to Congress in paper form and placed in the Congressional Record which was not readily available/accessible. Once the Congressional Record was placed on the Internet, its contents were available for all to see. This resulted in credit cards being opened up on those FLAG OFFICERS which resulted in identity theft.

  Result: DOD had to change their business practice.
  IHS is/will be changing their business practice on transmission of PII/PHI via email – HOW: *Encryption*

MORE BEST PRACTICES

- When you receive an email and it contains personal information about another individual, do not forward that document to others without first assessing whether each recipient has an official need to know.

- Use training to educate your personnel on Privacy.

  - Ensure all newly assigned personnel receive orientation training on the Privacy Act so they fully understand their role in ensuring that personal information is protected from unauthorized disclosure.
  - Ensure all personnel receive refresher training once a year or more often should they be involved in a breach (loss) of personal information.
  - Ensure that new supervisors and employees take Privacy Act training
  - Ensure all personnel who deal with personal information contained in a Privacy Act system of records are properly trained on the systems notice and the safeguards addressed therein and the restrictions regarding access to the information.

PROTECTING PII

- Think about ways to ensure that PII is properly protected.
- Think about your computer, memory stick, PDA, etc., and which PII information you store on it. What would you do if they were stolen?
- Think about emails – if you receive emails that contain PII – are they properly marked alerting you to treat them as FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE? Any misuse or unauthorized access may result in both civil and criminal penalties. Do you properly mark your emails?
- Think privacy when you create documents. Do you need to include the entire SSN, or will the last four digits work?

PROTECTING PII (continued)

- Think privacy and do not include the entire SSN in the subject line of an email for all to see.
- Think privacy and do not place PII in public folders in Outlook for others to see.
- Think privacy and do not place PII information on public Web sites.
- Think privacy and identify ways to ensure PII is not compromised!

DISPOSAL OF PII

- Don't assume that documents containing PII that are placed in a recycle bin are being shredded prior to being recycled..
- Best practice – cross-cut shredding.
- Dispose of PII in a manner that does not result in a privacy breach.

MAINTAINING INFORMATION

- If you maintain information that is retrieved by a person's name and/or personal identifier, you must identify a Privacy Act system of records that permits that collection and follow the rulemaking set forth in the systems notice.
- All IHS PA systems of records notices are listed at http://www.ihs.gov

  Click on Resources for IHS Management
  Click on Privacy Act

IHS PA RESPONSIBILITIES

- Upon written request, provide a copy of the record to the subject of the file.
- Maintain only accurate, timely, and complete information.
- When directly soliciting personal information, provide a PA Statement that addresses the authority for the collection, purpose for the collection, routine uses that will be made of the information, and whether collection is voluntary or mandatory.

WHAT ARE YOUR RESPONSIBILITIES?

As an employee, you play a very important role in assuring IHS complies with the provisions of the Privacy Act. Accordingly,

- *Do not* collect personal data without authorization.
- *Do not* distribute or release personal information to other employees unless they have an official need-to-know.

WHAT ARE YOUR RESPONSIBILITIES? (continued)

- *Do not* be afraid to challenge anyone who asks to see PA information for which you are responsible.
- *Do not* maintain records longer than permitted under records disposal.
- *Do not* destroy records before disposal requirements are met.
- *Do not* place unauthorized documents in PA systems of records.

WHAT ARE YOUR RESPONSIBILITIES? (continued)

- *Do not* commingle information about different individuals in the same file.
- *Do not* transmit personal data without ensuring it is properly marked. Use 'FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE.'
- *Do not* use interoffice envelopes to mail privacy data.
- *Do not* place privacy data on shared drives, multiaccess calendars, the Intranet or Internet that can be accessed by individuals who do not have an official need to know.

WHAT ARE YOUR RESPONSIBILITIES? (continued)

- *Do not* create a new system of records without first consulting your Privacy Officer.
- *Do not* hesitate to offer recommendations on how to better effectively manage privacy data.

  Y*our insight counts! Your dedication to protecting privacy is paramount to our success!*

LET'S RECAP

- Privacy Act of 1974, as amended (5 U.S.C. 552a)
- Twelve Conditions of Disclosures
- Maintain an Accounting of Disclosures (i.e., ROI software application or IHS 505)
- Individual - Rights to Access, Copy, Amend/Correction
- Safeguards

LET'S CONTINUE TO RECAP

- If Collecting PII in a Record Set – Publish a SORN. *No secret records.*
- PA covers U.S. Citizens and Resident Aliens (does not cover illegal aliens, deceased, organization, and Tribal governments)
- SSN is voluntary for MR. If statutes or other authority requires, then collect.

LET'S CONTINUE TO RECAP

- IHS has three PASORN(s) – Go to the IHS Privacy Act Web site for more info
- Civil Remedies
- Criminal Penalties
- HIPAA Privacy Rule Comparison to the Privacy Act and PHI (i.e., IHS Medical, Health, and Billing Records)

Ten Rules to Protect Personal Information

- 1. *Do not* be afraid to challenge anyone who asks to see Privacy Act information that you are responsible for.
- 2. *Do not* maintain records longer than permitted under records disposal.
- 3. *Do not* destroy records before disposal requirements are met.
- 4. *Do not* place unauthorized documents in Privacy Act record systems.
- 5. *Do not* commingle information about different individuals in the same file.

Ten Rules To Protect Personal Information (continued)

- 6. *Do not* transmit personal data without ensuring it is properly marked. Use "**FOR OFFICIAL USE ONLY –PRIVACY SENSITIVE**."
- 7. *Do not* use interoffice envelopes to mail Privacy data.
- 8. *Do not* place privacy data on shared drives, multiaccess calendars, the Intranet or Internet that can be accessed by individuals who do not have an official need to know.
- 9. *Do not* create a new system of records without first consulting your Privacy Office.
- 10. *Do not* hesitate to offer recommendations on how to better effectively manage privacy data.

BOTTOM LINE

- If you collect it…you must protect it
- If in doubt…leave it out
- Just because you've always handled personal information one way…doesn't mean that is the best way.

THANK YOU