PII Compliance Guidelines

Personally Identifiable Information (PII): Individually identifiable information from or about an individual customer including, but not limited to: (a) a first and last name or first initial and last name; (b) a home or other physical address, which includes at least street name and name of city or town; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number with expiration date; (g) date of birth; (h)a driver's license number; or (i) any other information from or about an individual customer that is combined with (a) through (h) above.

Sensitive Personally Identifiable Information (SPII): Information owned or licensed by the organization that consists of an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: (1) driver's license or state identification number; (2) Social Security number; or (3) account numbers (such as bank, credit or debit card numbers) when combined with any required security code, access code or password that would permit access to an individual's financial account.

Privacy and Information Security Framework

1. Does your organization have a privacy and information security framework that includes administrative, physical and technical safeguards?
2. Is it standards based? (ISO, CoBiT, NIST, CIS, FFIEC, AICPA, etc…)
3. Does your organization base your framework on any separate, proprietary criteria such as customer, employee or vendor credentialing?

Inventory and Access to PII and SPII

1. Does your organization have written policies/procedures that address collection, use and dissemination of PII and SPII?
2. Does your organization have a policy for restricting access to personal information to only those employees, subcontractors and/or agents who need it as part of their job responsibilities?
3. Does your organization take inventory on where PII and SPII is stored?
4. Is your inventory updated on a regular basis?
5. Does your organization limit access to SPII?
6. Does your organization truncate and/or mask SPII wherever possible? Incoming and outgoing?
7. Does your organization have controls in place to limit SPII transmission via e-mail?

Credentialing (Background Screening)

Employees

1. Does your organization credential its employees?
2. Does the credentialing process require criminal, and credit checks?
3. Does your organization have a re-credentialing program for employees that includes a criminal background check at least every three years?

Customers

1. Does your organization credential its customers?

2. Does your organization centralize its credentialing of customers to ensure consistency and security of the process?
3. Does your organization follow a credentialing checklist or process that verifies each customer's legitimacy and permissible purpose? Is there a scoring process?
4. Does your organization require and conduct site inspections of its customers? Is there a scoring process?
5. Does your organization require that each customer pass its credentialing process?
6. Does your organization require that each customer pass its site visit process?
7. Does the credentialing process/checklist undergo a separate quality control review for each customer?
8. Does your organization re-credential its customers?

Vendors

1. Does your organization assess/credential its vendors?
2. Does your organization re-credential its vendors? How frequently?
3. Does the credentialing process for vendors who will have access to sensitive information require background checks?

Corporate Accountability

1. Does your organization have an office or function dedicated to privacy? Compliance?
2. Does your organization's privacy and/or compliance function report directly to an independent body in the organization (e.g., Board of Directors)?
3. Does your organization have committees at various levels of the organization that set, direct and implement information security and privacy strategy, policy and initiatives?
4. Does your organization have a committee that includes senior leaders who are accountable for administrative, technical and physical privacy and information security safeguards?
5. Does your organization have a committee responsible for creating privacy and information security policies?
6. Does your organization have policies that document accountability for each of the committees/working groups?
7. Does your organization have assigned representatives within each of its business functions to assist with the implementation of privacy, information security and compliance policies and procedures?

Policies, Procedures and Guidelines

1. Does your organization have published privacy principles or a published privacy policy?
2. Does your organization have policies, procedures and guidelines that address compliance with privacy and information security laws and/or regulations?
3. Does your organization have Web site privacy policies for its Web sites?
4. Are customer-facing Web sites certified?
5. Does your organization have policies that govern data access?
6. Does your organization have policies that govern data protection?

7. Does your organization have policies that govern data transfer?
8. Does your organization have policies that govern data transport?
9. Does your organization have policies that govern data restriction?
10. Does your organization have policies that govern data retention?
11. Does your organization have policies that govern data deletion and destruction?
12. Does your organization have policies that govern data classification?
13. Does your organization have policies that govern breach response and notification?
14. Does your organization have a policy on incident response?
15. Does your organization require its employees to adhere to a code of conduct?

Audit and Compliance

1. Does your organization have a written annual audit plan and methodology?
2. Does your organization conduct audits to verify compliance with your organization's policies and procedures?
3. Are audits conducted regularly on all policies? How often? At least annually?
4. Does your organization review, audit and update its online privacy policies? How often?
5. Does your organization conduct audits to ensure compliance with federal and state laws and regulations?
6. Does your organization undergo third-party audits by outside accredited third parties? How many per year?
7. What types (e.g., SAS70)?
    - SAS 70 is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
8. Does your organization annually review and update its compliance program?

Physical Security

1. Does your organization have appropriate physical security controls to safeguard data?
2. Does your organization monitor employee access to buildings?
3. Does your organization require escorting of visitors?
4. Does your organization have physical security policies that require employees and contractors maintain a "clean desk" to protect exposure of sensitive data?
5. Does your organization have policies and procedures designed to help protect property and assets from unauthorized acquisition, loss or damage?
6. Does your organization restrict access to removable and mobile media for employees?
7. Does your organization require all laptops to be encrypted?

Technology Solutions

1. Does your organization utilize technology enhancements to aid in network security?
2. Does your organization monitor access to sensitive information?
3. Does your organization utilize technologies such as encryption and data classification to protect sensitive information?
4. Are all databases and other data repositories containing sensitive information, including all organizational servers, secured behind firewalls?
5. Does your organization run anti-virus software, and does it have a minimum compliance level of more than 95% at any given time?
6. Does your organization run at least weekly vulnerability scans of your critical infrastructure and have strict requirements on addressing issues found?
7. Does your organization have an independent network security assessment performed at least annually?
8. Does your organization maintain a patch management program that is designed to address desktop and server patches within days of patch release?
9. Does your organization maintain technical standards for system setup and configuration and assess a sample of systems against these standards every month?
10. Does your organization prohibit employee access to certain categories of Web sites?
11. Is your organization compliant with the Payment Card Industry standards for credit card data protection?
    - The PCI Security Standards Council is an independent body formed to develop, enhance, disseminate and assist with implementation of security standards for payment account security.
12. Does your organization assess employee passwords for strength at least quarterly, and force password changes on weak accounts?
13. Does your organization implement intrusion detection systems at your Internet perimeter, and monitor these devices 24/7 for malicious activity?
14. Does your organization have an established Web vulnerability assessment program that focuses on finding and eliminating risks with Web-based applications?
15. Does your organization have tools and processes that help automate the user identity management lifecycle (e.g., removing access immediately on employee termination)?
16. Does your organization ask employees a secret security question in the event they are locked out of their computers?

Training, Education and Outreach

1. Does your organization have a program for internal and external outreach and communication regarding privacy and information security?
2. Does your organization require that employees dedicated to privacy and security obtain appropriate certifications (e.g., IAPP /CIPP, CISM)?
    - International Association of Privacy
    - Professionals/Certified Information Privacy
    - Professional, Certified Information Security Manager

3. Does your organization require annual mandatory training for all employees on privacy?
4. Does your organization require annual mandatory training for all employees on information security?
5. Does your organization require annual mandatory training for all employees on code of conduct?
6. Does your organization require annual mandatory training for record retention and deletion?
7. Are employees required to pass each training program with a certain percentage of questions answered correctly?
8. Are there consequences for not successfully completing training?
9. Are privacy and information security policies communicated to employees on a regular basis? How?
10. Does your organization send out regular privacy reminders to its employees?
11. Does your organization have a program to notify stakeholders on key privacy and information security programs and enhancements?
12. Does your organization have hotlines for employees, customers and consumers to report suspicious behavior? What are they?
13. Does your organization have liaisons with regulators? Law enforcement? Privacy advocates?
14. Please describe.

Transparency with Customers

1. Does your organization have a customer advocacy office that enhances interaction with customers?
2. Do customers and consumers have easy access to your organization through customer-friendly and/or dedicated Web sites?
3. Do customers have the ability to request certain information available about them? Is there a cost to obtain this information?
4. Does your organization provide a vehicle for correction should a customer wish to dispute the accuracy of information contained in a report?
5. Does your organization provide easily accessible tools (e.g., a video, Web site) to answer questions and explain the benefits that customers receive as a result of your organization's services?