

Sample Questionnaire

The following questions can be used as a checklist to plan and reduce the risk associated with handling personal information (PI) encountered during special circumstances. The circumstances could include migrations, retiring legacy systems, mergers, acquisitions, divestitures, office or branch moves, data center relocations, equipment replacement or moving a system to the cloud.

General Questions

- Have you built alliances with the key players within your organization (see reverse)?
- Does your company have a Privacy Policy?
- What is your company's definition of Personally Identifiable Information (PII)?
- Have your retention/disposition schedule(s) been updated to include the current Privacy laws and regulations? Have you included access levels to the PI?
- Is your data map up to date vis-à-vis the personal information in the special circumstance?
- Have you done some sleuthing to locate the less obvious locations of PI (e.g. a multi-function device, fax machine, photocopier machine, scanner)?
- Is the PI located in the United States or Internationally?
- Before commencing the move, conversion, migration or transfer of personal information, have you securely disposed of all expired content?
- Do you have secure methods in place for information access, transfer and destruction of PI?
- Are your contractual provisions up to date for retention and privacy handling?
- Are the data or files/records being handled by a third party?
- Do you have adequate physical security measures in place?
- Do you have adequate cyber / information security measures in place?
- Do you have a check list of items to follow during the move, conversion, migration or transfer?
- Have you effectively trained and communicated the records requirements as they relate to handling personal information?
- Are you auditing the process, including vendors and third party vendors?

System Conversions and Migrations (including moving data to the "Cloud")

- Have you identified and securely eliminated non-records and expired content before the data migration?
- Do you have secure access controls in place for the electronic PI?
- Where is the PI located (e.g. are there multiple document repositories)?
 - metadata fields
 - relational database servers
 - file shares
 - SharePoint sites
 - email archives
- Does the data exist in back-up systems or on back-up tapes?
- Does the data exist in your vital records / disaster recovery sites?
- Can you securely delete the records that have expired from the database without compromising the database?
- Do you have IT policies and procedures in place for giving third party vendors access to your system?
- If transferring data to a new location, such as a different state or out of the country, have you verified with Legal to ensure that you are in compliance with all of the privacy laws?

Job Aid

Office Moves

- Is there a project manager assigned to the move?
- Do you have a checklist of items to follow for the move, including the handing of PI?
- Have you thought about the less obvious sources of PI (e.g. old equipment in a storage closet)
- Have you taken the opportunity for a “Records Cleanup” Day to securely eliminate all non-record and expired content?
- Is your shredding company National Association of Information Destruction (NAID) certified?
- If decommissioning equipment (copiers, old PCs, fax machines, etc) which can potentially contain PI, are they being securely deleted before disposition?
- Do you have custody and control procedures in place for the movement of physical files and records (e.g. bank branch client records or patient medical files) ?
- If outsourcing the physical move, does the vendor have the appropriate security clearances? If they in turn are outsourcing, is the third party vendor also following your contractual terms?
- Have you worked with the Security and Facility groups to oversee the physical move?

Potential Partners within Your Organization

The following functions are potential partners and may be included in an Information Governance Structure, a Privacy Committee Structure or other Committee. It is important to gain a seat at the table and to build alliances with as many of these groups as possible.

<input type="checkbox"/> Audit	<input type="checkbox"/> Information Technology
<input type="checkbox"/> Compliance	<input type="checkbox"/> Legal
<input type="checkbox"/> Facilities Management	<input type="checkbox"/> Procurement
<input type="checkbox"/> Finance	<input type="checkbox"/> Project Management Office
<input type="checkbox"/> Human Resources	<input type="checkbox"/> Records and Information Management
<input type="checkbox"/> Information Privacy	<input type="checkbox"/> Risk
<input type="checkbox"/> Information Security	<input type="checkbox"/> Security (Physical)

Reference Sources:

- International Association of Privacy Professionals Website: <https://privacyassociation.org/>
- Swire, Peter P. CIPP/US and Ahmad, Kenesa, CIPP/US, Foundations of Information Privacy and Data Protection- A Survey of Global Concepts, Laws and Practices
- Swire, Peter P. CIPP/US and Ahmad, Kenesa, CIPP/US, U.S Private-sector Privacy – Law and Practice for Information Privacy Professionals
- Federal Trade Commission Report on Protecting Consumer Privacy: <http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>
- Privacy by Design Website: <http://www.privacybydesign.ca/>
- Jones, Virginia A, CRM, FAI, “Protecting Information Privacy Per US Federal Law” , Information Management Journal, ARMA International, March/April 2014
- Beckles, Cheri-Ann, “An International Perspective on Protecting Personal Information”, IMJ, ARMA International, March/April 2014