

Content Recaps

Download and save this PDF to your desktop, and open it in Adobe Acrobat to activate the hyperlinks.

Confidential Information & Personally Identifiable Information (PII)

Confidential Information

Confidential Information is any information that's not generally available to the public, in any form, which Deloitte receives during the course of business.

Some examples of Confidential Information include:

- Data provided by clients
- Information we discover or create
- Tools and methodologies we use
- Deliverables we create
- Deloitte internal training materials

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any information that could be used to identify a person or relates to an identified person.

Examples of PII include:

- Name, address, date of birth, personnel number, government identifier, usernames with passwords
- Sensitive PII like race, political position, biometric information
- Protected Health Information (PHI) like medical or health insurance information




PII is also **Confidential Information**, whether or not it is available to the public.

Document and Email Classifications

As you handle Confidential and Personal Information, it's critical to understand the nature of the information. Higher-risk information may require additional protections. Classification is required for all Microsoft documents (PowerPoint, Word, Excel) and Outlook emails:

Public	Confidential	High Risk Confidential	Personal Information (PI)
Information available to the public or intended for public sharing	Information not known to the public that relates to our business or that we receive during the course of business from other Deloitte personnel, our clients, or third parties (includes Business Contact Information; excludes all other Personal Information)	Information not known to the public, of a highly regulated or sensitive nature, that requires a higher duty of care (excludes all Personal Information)	Information relating to an identified or identifiable natural person (excludes Business Contact Information)

Confidential Information & Personally Identifiable Information (PII)

What you want to do...	What you should do...
 Print from home	Add a printer to the list of printers on your Deloitte laptop.
 Use your home monitor	Connect your Deloitte laptop to your home monitor. You can get an adapter cord from your local ITS walkup.
 View files on your personal iPad	Employees eligible for Deloitte's wireless program may also sync with their personal iPads. However, you must follow our policies to protect Deloitte, client, and third-party data.

Reporting Incidents

- Report any potential incident immediately through the online reporting system on DNet or by calling 1-800-DELOITTE (US/USI) — even if you are still investigating the incident.
- The US Confidentiality & Privacy Incident Management team will review your report and guide you through the incident management process.
- The US Confidentiality & Privacy Incident Management team will consult with the relevant stakeholders to assess the risk and provide guidance regarding corrective actions.
- Potential incidents should be kept confidential. Knowledge of the incident should only be shared with engagement leadership and the US Confidentiality & Privacy team.

A Confidentiality or Privacy Information incident is any event where there is knowledge or reasonable belief that there has been actual or **potential** unauthorized disclosure, use of, or access to confidential or private information.

Lean Data Tips

Minimize risk with some simple practices

- Schedule a recurring time to review your email messages. Retain or delete messages as appropriate. Any email messages or attachments that are Official Records, per Deloitte records retention policy (APR 601), should be archived. Any messages subject to a legal hold should not be deleted.
- Consider keeping an email folder of items you need to keep for businesses purposes versus a correspondence folder with items you delete at the end of the project.
- Deploy Outlook mailbox clean up tools like deleting duplicate conversations.
- Minimize the number of documents you retain on your laptop, especially those with Confidential Information or PII.
- Notify collaboration site owners to take action when you no longer need access.
- You can't lose or expose data that you don't have.

Extra tip: Help reduce your email AND increase good security hygiene practices: Avoid using your Deloitte email address to access third-party sites, such as online shopping or personal banking websites. This minimizes the risk of a potential malicious attack on your Deloitte account.