



# Types of Sensitive Data: Personal Information: Quick Reference



In recent years, governments, consumers, and the general public have become increasingly concerned about the privacy and security of personal information.

## PERSONAL INFORMATION DEFINED

Personal information is any information that can be used to contact, locate, or otherwise identify an individual.

## PROTECTED HEALTH INFORMATION (PHI) DEFINED

Protected health information (PHI) is a particularly sensitive type of personal information used in the healthcare industry. It includes any personally identifiable information in medical records, including conversations between medical professionals about treatment.

## PRIVACY LAWS

In most countries in which Abbott conducts business, there are laws and regulations in place designed to protect personal information, including protected health information. These differ from one country to the next, but often embrace the same core principles.

## ABBOTT'S PRIVACY BY DESIGN PRINCIPLES

Abbott's data privacy and protection policies and procedures are organized around the following principles:

### Notice

Notice is about letting people know what personal information is being collected and explaining in clear, precise, and unambiguous language how we plan to use that information.

### Consent

Consent is about providing individuals with the opportunity to agree to the collection and use of their personal information.

### Data Integrity

Data Integrity is about taking reasonable measures to ensure that the personal information we retain is accurate, complete, and current.

## Access and Correction

Access and Correction is about providing individuals with reasonable access to their data and the opportunity to exercise their rights in connection with this data.

## Disclosure and Use

Disclosure and Use is about controlling who has access to personal information and limiting use to specific purposes.

## Disposition

Disposition refers to what happens to data once it is no longer actively being used. Activities may include deletion, archiving, or retaining for legal hold purposes.



## Types of Sensitive Data: Confidential Business Information: Quick Reference



Most of the business information we use in our day-to-day work activities is considered confidential.

### CONFIDENTIAL BUSINESS INFORMATION

#### DEFINED

Confidential business information is a broad category. It includes sales information, such as customer lists, sales projections, forecasts, and strategies. It also includes purchasing information, such as bids for contracts, supplier lists, and costing information.

In addition, certain types of confidential business information require greater care than normal because improper disclosure or use of this information can cause serious harm to the company. Examples include trade secrets, clinical and regulatory data, and financial data that has not been released to the public.

### CONFIDENTIALITY TEST

A good way to confirm whether the business information you are using is confidential is to ask yourself a simple question:

Is this Abbott information publicly available?

If the answer is no, then the information should be considered confidential and appropriate steps must be taken to protect it.

### INSIDER INFORMATION

Insider information is any non-public, material information that, if publicly disclosed, could reasonably be expected to affect the market value of a company's securities, or influence investors' decisions on whether to buy or sell securities. If you are aware or in possession of insider information, it is illegal to trade in, or recommend others to trade in, Abbott securities.



# Your Role in Protecting Sensitive Data: Quick Reference



Here is what you can do to help protect sensitive data.

## ACCESSING AND USING SENSITIVE DATA

Before using any sensitive data, make sure your job role and responsibilities permit you to access the data. If you have permission to access sensitive data, only use it for the specific purpose for which you have been granted access.

## SHARING SENSITIVE DATA

Before sharing sensitive data, make sure the person you plan to share with has proper authorization. Always:

- Confirm the identity of the person making the request;
- Confirm the person's need to access the information;
- Verify that the information can be used for the purposes they are requesting; and
- Share only the amount of information required to meet the need, not more.

## RETAINING AND DISPOSING OF SENSITIVE DATA

Always archive or dispose of sensitive data in a manner consistent with Abbott's data management, retention, and disposal requirements.

If you receive a legal hold order, never discard, destroy, or delete any information covered by the hold.

## RESPONDING TO INADVERTENT OR IMPROPER DISCLOSURES OF PHI

In response to any inadvertent or improper disclosure of a patient's protected health information (PHI), you should immediately report the disclosure to both:

- The source of the information, and
- OEC or a member of the Global Privacy team.

## RESPONDING TO INADVERTENT OR IMPROPER DISCLOSURES OF CONFIDENTIAL BUSINESS INFORMATION

In response to any inadvertent or improper disclosure of Confidential Business Information, you should immediately report the disclosure to both:

- Your immediate supervisor, and
- OEC or a member of the Global Privacy team.

## BEING ALERT TO EXTERNAL THREATS

If you suspect your computer may be infected with malware, contact your local Global Service Desk immediately. Never attempt to deal with the virus yourself.

If an email seems suspicious, click the "Report Phishing" button in Outlook or forward the email as an attachment to [phishing@abbott.com](mailto:phishing@abbott.com).

## REPORTING A DATA INCIDENT

Any event involving a potential compromise of information security, including a lost or stolen mobile device, should be reported immediately to your local Global Service Desk.

If you have any concerns about a potential violation or want to report a potential privacy incident, contact OEC or a member of the Global Privacy team.

