|  |  |  |
| --- | --- | --- |
| ID | SOURCE | TARGET |
| [Screen 0](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=1_C_1)  [1\_C\_1](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=1_C_1) | Protecting Sensitive Data  Click the forward arrow to begin. | Beschermen van gevoelige gegevens  Klik op het pijltje vooruit om te beginnen. |
| [Screen 1](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=2_C_2)  [2\_C\_2](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=2_C_2) | At Abbott, we rely on data to make decisions - often that data contains sensitive information.  For us to fulfill our mission of helping people live their best lives through good health, it is essential that we keep this data secure and comply with the laws and ethical standards that Abbott upholds. This course is designed to give you the skills needed to support this task. | Bij Abbott vertrouwen we op gegevens om beslissingen te kunnen nemen, maar die gegevens bevatten vaak gevoelige informatie.  Voor ons is het onze missie om mensen te helpen het beste uit hun leven te halen via een goede gezondheid waar te kunnen maken van groot belang om deze gegevens veilig te houden en de wetten en ethische normen waar Abbott voor staat na te leven. Deze cursus is opgezet om de vaardigheden te bieden die nodig zijn om deze taak te ondersteunen. |
| [Screen 2](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=3_C_3)  [3\_C\_3](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=3_C_3) | After completing this course, you will have a better understanding of:   * What sensitive data is, * How we protect this data at Abbott, * Your role in protecting sensitive data, and * What to do if you think sensitive data may have been improperly disclosed or compromised. | Na het voltooien van deze cursus heeft u meer inzicht in:   * Wat gevoelige gegevens zijn, * Hoe we deze gegevens bij Abbott beschermen, * Uw rol bij het beschermen van gevoelige gegevens en * Wat u moet als u denkt dat gevoelige gegevens mogelijk op onjuiste wijze zijn bekendgemaakt of gecompromitteerd. |
| [Screen 3](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4)  [4\_C\_4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4) | 1 | Personal Information  Here you will learn how governments, consumers, and the public have become increasingly concerned about the privacy and security of personal information.  12 Minutes  Section 1 | Personal Information  Recognizing Personal Information  Legal, Regulatory and Contractual Requirements  Abbott’s Privacy by Design Principles  Review  2 | Confidential Business Information  Here you will learn how most of the business information we use in our day-to-day work activities is considered confidential.  5 Minutes  Section 2 | Confidential Business Information  Recognizing Confidential Business Information  Cost of Not Protecting Confidential Business Information  Insider Information  Review  3 | Protecting Sensitive Data  Here you will learn what you can do to help protect sensitive data.  8 Minutes  Section 3 | Your Role in Protecting Sensitive Data  Accessing and Using Sensitive Data  Sharing Sensitive Data  Retaining and Disposing of Sensitive Data  Responding to Improper Disclosures  Review  4 | Knowledge Check  Assess your understanding of the key concepts and principles of this course.  5 Minutes  Section 4 | Knowledge Check  Assessment  Click the panel to get started.  Click the yellow play button to begin.  This content is not yet available. You must complete Section{a} {b}. | 1 | Persoonlijke informatie  Hier krijgt u informatie over hoe overheden, consumenten en het grote publiek zich steeds meer zorgen gaan maken over de privacy en veiligheid van persoonlijke informatie.  12 minuten  Hoofdstuk 1 | Persoonlijke informatie  Persoonlijke informatie herkennen  Wet- en regelgeving en contractuele vereisten  Abbott's principes van ingebouwde privacy (Privacy by Design)  Opnieuw bekijken  2 | Vertrouwelijke bedrijfsinformatie  Hier krijgt u informatie over hoe de meeste zakelijke informatie die we bij ons dagelijkse werkactiviteiten gebruiken als vertrouwelijk wordt beschouwd.  5 minuten  Hoofdstuk 2 Vertrouwelijke bedrijfsinformatie  Vertrouwelijke bedrijfsinformatie herkennen  De kosten voor het niet beschermen van vertrouwelijke bedrijfsinformatie  Voorkennis  Opnieuw bekijken  3 | Beschermen van gevoelige gegevens  Hier krijgt u informatie over wat u kunt doen om gevoelige gegevens te helpen beschermen.  8 minuten  Hoofdstuk 3 |Uw rol bij het beschermen van gevoelige gegevens  Toegang tot en gebruik van gevoelige gegevens  Gevoelige gegevens delen  Gevoelige gegevens bewaren en verwijderen  Reageren op ongepaste openbaarmakingen  Opnieuw bekijken  4 | Kennischeck  Beoordeel uw begrip van de belangrijkste concepten en principes van deze cursus.  5 minuten  Hoofdstuk 4 | Kennischeck  Toets  Klik op het paneel om te beginnen.  Klik op de gele afspeelknop om te beginnen.  Deze inhoud is nog niet beschikbaar. U moet Hoofdstuk {a} {b} afronden. |
| [Screen 4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7)  [5\_C\_7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7) | At Abbott, one common type of sensitive data we use is personal information.  In recent years, governments, consumers, and the general public have become increasingly concerned about the privacy and security of personal information. | Bij Abbott bestaat een veelvoorkomend type gevoelige gegevens die we gebruiken uit persoonlijke informatie.  In de afgelopen jaren zijn overheden, consumenten en het grote publiek zich steeds meer zorgen gaan maken over de privacy en veiligheid van persoonlijke informatie. |
| [Screen 5](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=6_C_8)  [6\_C\_8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=6_C_8) | Personal information is any information that can be used to contact, locate, or otherwise identify an individual. | Persoonlijke informatie is alle informatie die kan worden gebruikt om contact op te nemen met een persoon, deze te lokaliseren of anderszins te identificeren. |
| [Screen 6](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9)  [7\_C\_9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9) | Kandice | Marketing Manager  Can you give me some examples of personal information?  Personal information can include biographical information, such as name, date of birth, email address and phone number.  It can include information relating to an individual’s appearance, such as hair color or weight.  It can also include information relating to an individual’s personal life, such as photos, browser cookies or location tracking information. | Kandice | Marketing Manager  Kunt u mij enkele voorbeelden geven van persoonlijke informatie?  Persoonlijke informatie kan biografische informatie bevatten, zoals naam, geboortedatum, e-mailadres en telefoonnummer.  Het kan informatie bevatten met betrekking tot het uiterlijk van een persoon, zoals haarkleur of gewicht.  Het kan ook informatie bevatten met betrekking tot het persoonlijke leven van een persoon, zoals foto's, browsercookies of locatiegegevens. |
| [Screen 7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10)  [8\_C\_10](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10) | Jerry | Sales Representative  Does personal information also include protected health information?  Yes, it does.  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. | Jerry | Sales Representative  Bevat persoonlijke informatie ook beschermde gezondheidsinformatie?  Ja, dat klopt.  Beschermde gezondheidsinformatie is een bijzonder gevoelige soort persoonlijke informatie die in de gezondheidszorg wordt gebruikt. Het bevat alle persoonlijk identificeerbare informatie in medische dossiers, inclusief gesprekken tussen medische professionals over behandeling. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=9_C_11)  [9\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=9_C_11) | In most countries in which Abbott conducts business, there are laws and regulations in place designed to protect personal information, including protected health information.  Laws relating to privacy and protection of personal information differ from one country to the next, but often embrace the same core principles.  CLICK EACH OF THE HIGHLIGHTED AREAS ONSCREEN TO LEARN ABOUT THE DIFFERENT TYPES OF PRIVACY LAWS AND REQUIREMENTS IN PLACE AROUND THE WORLD. | De meeste landen waarin Abbott zaken doet, kennen wetten en voorschriften die zijn ontworpen om bepaalde soorten persoonlijke informatie te beschermen, inclusief beschermde gezondheidsinformatie.  Wetten met betrekking tot privacy en de bescherming van persoonlijke informatie verschillen van land tot land, maar omvatten vaak dezelfde kernprincipes.  KLIK OP ELK VAN DE GEMARKEERDE GEBIEDEN OP HET SCHERM VOOR MEER INFORMATIE OVER DE VERSCHILLENDE SOORTEN PRIVACYWETTEN EN -VEREISTEN DIE OP VERSCHILLENDE PLEKKEN TER WERELD GELDEN. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11)  [10\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11) | Europe  In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate. GDPR applies to organizations located within Europe, as well as organizations located outside of Europe that offer goods and services to or monitor the behavior of any individual residing in Europe.  One of the key concepts of GDPR is the right to erasure, also known as the right to be forgotten. This right gives individuals the ability to request that their personal data be erased from an organization's records. If an individual makes such a request, the organization must take steps to erase the data from its systems and prevent its further use or disclosure. There may be exceptions to data subject requests. Nonetheless, Abbott will inform each validated data subject of what action is taken for each request. Violations of GDPR can result in heavy fines for companies, up to 4% of their annual global turnover, or 20 million euros (whichever is greater), for the most serious offenses. | Europa  In Europa behoort de Algemene Verordening Gegevensbescherming (AVG) tot de meest uitgebreide privacywetten en sinds de implementatie ervan in 2018 bepaalt deze verordening de norm voor privacybescherming die andere landen proberen te evenaren. De AVG is niet alleen van toepassing op organisaties binnen Europa, maar ook op organisaties die buiten Europa zijn gevestigd die goederen en diensten aanbieden aan, of het gedrag volgen van in Europa woonachtige personen.  Een van de belangrijkste concepten van de AVG is het recht op het wissen van gegevens, ook wel het recht om te worden vergeten genoemd. Dit recht geeft individuele personen de mogelijkheid om te vragen om hun persoonlijke gegevens te wissen uit de records van een organisatie. Als een individuele persoon een dergelijk verzoek doet, moet de organisatie stappen ondernemen om de gegevens uit hun systemen te verwijderen en verder gebruik of bekendmaking ervan te voorkomen. Er kunnen uitzonderingen zijn op verzoeken van de betrokkene. Niettemin zal Abbott elke gevalideerde betrokkene informeren over welke actie voor elk verzoek wordt ondernomen. Schendingen van de AVG kunnen hoge boetes voor bedrijven tot gevolg hebben, tot 4% van hun wereldwijde jaaromzet of 20 miljoen euro (welk daarvan het hoogst is) voor de meest ernstige overtredingen. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11)  [11\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11) | United States  In the United States, there is no single law that protects all personal information. Instead, there are privacy laws and regulations that apply to specific industries and types of data. For example, HIPAA protects the privacy of healthcare data, while the Fair Credit Reporting Act protects credit information.  However, some states have begun enacting their own comprehensive data privacy laws. For instance, California has the California Consumer Privacy Act (CCPA), which gives Californians certain rights to their data, such as the right to know what personal information is being collected about them and the right to delete any personal information collected. The CCPA will be amended by the California Privacy Rights Act (CPRA) in 2023, which will give people even more rights to their data.  Other states that have passed their own data privacy laws include Virginia, Colorado, Utah, and Connecticut. While each state's law is different, they all generally give people rights to their data and require companies to provide certain disclosures about their data processing activities.  Fines for violating state privacy laws can be significant. For example, California can fine companies up to $7,500 USD per violation of the CCPA.  Canada  There are laws at both the federal and provincial levels in Canada that are designed to protect an individual's personal information. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that applies to private sector organizations and is enforced by the Office of the Privacy Commissioner of Canada.  At the provincial level, Quebec, Alberta, and British Columbia have enacted privacy laws that are similar to PIPEDA. Some other provinces also have rules in place that provide similar protections for personal information, including the provinces of Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia, which have enacted health information privacy laws.  These laws are in place to help prevent personal information from being mishandled or collected without the individual's knowledge, and give people the right to access their own information and correct any errors.  Violating these laws can result in significant fines. For example, violating PIPEDA can lead to a fine of up to $100,000. In Alberta, the Personal Information Protection Act (PIPA) allows for fines of up to $10,000 for individuals and $500,000 for organizations. | Verenigde Staten  In de Verenigde Staten is er geen afzonderlijke wet die alle persoonlijke informatie beschermd. In plaats daarvan zijn er privacywetten en -voorschriften die gelden voor specifieke bedrijfstakken en soorten gegevens. De Health Insurance Portability and Accountability Act (HIPAA) bijvoorbeeld beschermt de privacy van gegevens in de gezondheidszorg, terwijl de Fair Credit Reporting Act kredietinformatie beschermt.  Sommige staten zijn echter begonnen met het uitvaardigen van hun eigen alomvattende wetgeving voor gegevensbescherming. Californië heeft bijvoorbeeld de California Consumer Privacy Act (CCPA), die inwoners van Californië bepaalde rechten geeft op hun gegevens, zoals het recht om te weten welke persoonlijke informatie over hen wordt verzameld en het recht om persoonlijke informatie die is verzameld te verwijderen. De CCPA zal in 2023 worden gewijzigd door de California Privacy Rights Act (CPRA), die mensen zelfs nog meer rechten geeft op hun gegevens.  Andere staten die hun eigen wetten voor de bescherming van persoonsgegevens hebben aangenomen zijn Virginia, Colorado, Utah, en Connecticut. Hoewel de wetgeving van elke staat verschilt, geven zij de mensen over het algemeen rechten op hun gegevens en verplichten zij de bedrijven tot bepaalde bekendmakingen over hun activiteiten op het gebied van gegevensverwerking.  De boetes voor het schenden van staatsprivacywetgeving kunnen aanzienlijk zijn. Californië kan bedrijven bijvoorbeeld een boete opleggen van maximaal $ 7,500 per schending van de CCPA.  Canada  Er zijn in Canada wetten op zowel federaal als provinciaal niveau die zijn bestemd voor het beschermen van de persoonlijke informatie van de individuele persoon. De Personal Information Protection and Electronic Documents Act (PIPEDA) is bijvoorbeeld een federale wet die van toepassing is op organisaties in de private sector en wordt gehandhaafd door de Office of the Privacy Commissioner of Canada.  Op provinciaal niveau hebben Quebec, Alberta en British Columbia privacywetgeving uitgevaardigd die soortgelijk is aan de PIPEDA. Sommige andere provincies hebben ook regels geïmplementeerd die soortgelijke bescherming bieden voor persoonlijke informatie, waaronder de provincies Ontario, New Brunswick, Newfoundland en Labrador en Nova Scotia waar privacywetten zijn aangenomen op het gebied van gezondheidsinformatie.  Deze wetten zijn geïmplementeerd om ondersteuning te bieden bij het voorkomen van het verkeerd behandelen van informatie of het verzamelen van informatie zonder medeweten van de individuele persoon en geven mensen het recht op toegang tot hun eigen informatie en op correctie van eventuele fouten.  Schending van deze wetten kan leiden tot aanzienlijke boetes. Schending van de PIPEDA kan bijvoorbeeld leiden tot een boete van maximaal $ 100,000. In Alberta biedt de Personal Information Protection Act (PIPA) de mogelijkheid voor boetes van maximaal $ 10,000 voor individuele personen en $ 500,000 voor organisaties. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=12_C_11)  [12\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=12_C_11) | Asia Pacific  The privacy laws in the Asia Pacific region are constantly expanding and becoming more comprehensive. Some countries, such as China, have implemented data localization measures which require companies to store some personal data on servers within their borders. Additionally, China has privacy and security impact assessment requirements for the cross-border transfer of personal information.  Others, like Australia and Singapore, have adopted a more consumer-focused approach to privacy that gives individuals greater control over their information, including the right to know how companies are using it and the ability to access and correct it if necessary.  The penalties for companies who violate data privacy laws also differ widely across the region. In China, for example, companies can be fined up to 500,000 RMB (about $72,000 USD) for violating data privacy laws.  However, in Singapore, companies can be fined up to 1 million (Singapore) dollars (about $737,000 USD) for violating the country’s privacy law. | Azië Pacific  De privacywetgeving in de regio Azië Pacific wordt voortdurend uitgebreid en wordt steeds veelomvattender. Sommige landen, zoals China, hebben maatregelen genomen om gegevens te lokaliseren, waardoor bedrijven verplicht zijn sommige persoonsgegevens op servers binnen hun grenzen op te slaan. Bovendien heeft China voorschriften voor de beoordeling van de gevolgen voor de persoonlijke levenssfeer en de veiligheid bij de grensoverschrijdende overdracht van persoonsgegevens.  Andere landen, zoals Australië en Singapore, hebben een meer klantgerichte benadering van privacy aangenomen, die individuele personen meer controle geeft over hun informatie, waaronder het recht om te weten hoe bedrijven daarvan gebruikmaken en de mogelijkheid van toegang en correctie indien noodzakelijk.  Ook de straffen voor bedrijven die de wetgeving op de bescherming van de persoonlijke levenssfeer overtreden, lopen in de regio sterk uiteen. In China bijvoorbeeld kunnen bedrijven een boete krijgen van maximaal 500,000 RMB (ongeveer 72,000 USD) voor het overtreden van de privacywetgeving.  In Singapore kunnen bedrijven echter een boete krijgen van maximaal 1 miljoen (Singapore) dollar, (ongeveer 737,000 USD) voor het schenden van de privacywetgeving van het land. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11)  [13\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11) | Russia  Russia also has laws to protect its citizens' data, including a data localization law, which requires companies to store the personal data of Russian citizens on servers located in Russia.  The law applies to companies that process the data of Russia's citizens, regardless of whether those companies are based in Russia or not. So, for example, a U.S.-based company that processes the data of Russian citizens would need to comply with the law.  Like many countries, the law also requires companies to take steps to protect the personal data they process. For example, companies must ensure that the data is accurate and up-to-date and take steps to prevent it from being mishandled, lost, or stolen.  The fines for violating the law can range from $12,000 to $72,000 USD for the first offense and up to $216,000 USD for the second offense. | Rusland  Rusland heeft ook wetten om de gegevens van zijn burgers te beschermen, waaronder een wet op de lokalisatie van gegevens, die bedrijven verplicht de persoonsgegevens van Russische burgers op in Rusland gevestigde servers op te slaan.  De wet is van toepassing op bedrijven die de gegevens van Russische burgers verwerken, ongeacht of die bedrijven al dan niet in Rusland zijn gevestigd. Dus bijvoorbeeld een in de VS gevestigd bedrijf dat de gegevens van Russische burgers verwerkt moet zich aan die wet houden.  Net als in een groot aantal landen het geval is, vereist de wet ook dat bedrijven stappen ondernemen ter bescherming van de persoonsgegevens die zij verwerken. Bedrijven moeten bijvoorbeeld verzekeren dat de gegevens nauwkeurig en up-to-date zijn en stappen ondernemen om te voorkomen dat deze een verkeerde manier worden behandeld, verloren gaan of worden gestolen.  De boetes voor het schenden van de wet kunnen variëren van $ 12,000 tot $ 72,000 USD voor de eerste overtreding tot $ 216,000 USD voor de tweede overtreding. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=14_C_11)  [14\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=14_C_11) | Latin America  Most Latin American countries have laws in place that protect the privacy of individuals. However, many countries in the region, such as Ecuador, Argentina and Brazil, have recently revised their existing privacy regulations to stay current with international standards.  Ecuador, for example, recently passed the Organic Law on the Protection of Personal Data (LPPD), which will go into effect in 2023. This law applies to any company around the world that processes the personal data of individuals in Ecuador.  Like others in the region, the LPPD requires companies to provide notice and collect consent from individuals before using their data, destroy it when it is no longer needed, and meet certain restrictions before data is shared with other countries. These measures help protect the privacy of individuals across Latin America and ensure that companies are handling personal data responsibly.  Violations of the LPPD can result in significant fines, ranging from 3% to 17% of an organization’s annual revenue from the previous year, providing a strong incentive for companies to comply with the law. | Latijns-Amerika  De meeste Latijns-Amerikaanse landen hebben wetten geïmplementeerd die de privacy van individuele personen beschermen. Veel landen in de regio echter, zoals Ecuador, Argentinië en Brazilië hebben onlangs hun bestaande privacyregelgeving herzien om aan te sluiten bij internationale normen.  Ecuador bijvoorbeeld heeft onlangs de Organic Law on the Protection of Personal Data (LPPD) aangenomen, die in 2023 van kracht zal worden. Deze wet is van toepassing op elk bedrijf wereldwijd dat de persoonsgegevens van individuele personen in Ecuador verwerkt.  Net als anderen in de regio vereist de LPPD dat bedrijven kennis geven en toestemming vragen van individuele personen voordat zij hun gegevens gebruiken, deze vernietigen als ze deze niet langer nodig hebben en voldoen aan bepaalde beperkingen voordat gegevens met andere landen worden gedeeld. Deze maatregelen helpen bij het beschermen van de privacy van individuele personen overal in Latijns-Amerika en verzekeren dat bedrijven op een verantwoorde wijze omgaan met persoonsgegevens.  Schendingen van de LPPD kunnen leiden tot aanzienlijke boetes, variërend van 3% tot 17% van de jaaromzet van een organisatie in het voorafgaande jaar, wat een sterke aansporing is voor bedrijven om zich aan de wet te houden. |
| [Screen 9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=15_C_12)  [15\_C\_12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=15_C_12) | In addition to laws and regulations governing how Abbott conducts business, there may be additional obligations in specific contracts we have with customers.  For example, the U.S. government is a customer of Abbott. Under the terms of such an agreement, we are required to meet the obligations set out in the U.S. Privacy Act of 1974.  CLICK THE ‘PRIVACY ACT’ BUTTON TO LEARN MORE. | Naast wetten en voorschriften die bepalen hoe Abbott zaken doet, kunnen er aanvullende verplichtingen bestaan in specifieke contracten die we met klanten hebben.  De Amerikaanse overheid is bijvoorbeeld een klant van Abbott. Volgens de voorwaarden van een dergelijke overeenkomst zijn we verplicht om te voldoen aan de verplichtingen die zijn uiteengezet in de Amerikaanse Privacy Act van 1974.  KLIK OP DE KNOP 'PRIVACY ACT' VOOR MEER INFORMATIE. |
| [Screen 9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=16_C_12)  [16\_C\_12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=16_C_12) | Privacy Act  The Privacy Act of 1974 (5 U.S.C. 552a) is an important Federal regulation. It establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by federal agencies. For certain transactions, Abbott may be granted access to government agency records. In such cases, Abbott must meet several obligations, including the need to demonstrate that privacy training on protecting personally identifiable information has been conducted.  Employees should contact Legal before entering into any agreements with customers that have privacy obligations. | Privacy Act  De Privacy Act van 1974 (5 U.S.C. 552a) is een belangrijke federale regelgeving. Het stelt een code van eerlijke informatiepraktijken vast die het verzamelen, onderhouden, gebruiken en verspreiden van persoonlijk identificeerbare informatie over mensen regelt die door federale agentschappen wordt bijgehouden in documentatiesystemen. Voor bepaalde transacties kan Abbott toegang krijgen tot gegevens van overheidsinstanties. In dergelijke gevallen moet Abbott aan verschillende verplichtingen voldoen, waaronder de noodzaak om aan te tonen dat er privacytraining over het beschermen van persoonlijk identificeerbare informatie is gegeven.  Werknemers dienen contact op te nemen met de juridische afdeling voordat ze overeenkomsten aangaan met klanten die privacyverplichtingen hebben. |
| [Screen 10](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=17_C_13)  [17\_C\_13](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=17_C_13) | The laws, regulations, and contractual requirements we have just reviewed are often complex and can change rapidly.  Abbott has policies and procedures in place to ensure employees comply with these laws and regulations. If you have any questions or want to learn more, contact OEC or a member of the Global Privacy team.  For contacts and additional information, click the Resources icon. | De wetten, voorschriften en contractuele vereisten die we zojuist hebben bekeken, zijn vaak complex en kunnen snel veranderen.  Abbott heeft beleidsregels en procedures opgesteld om ervoor te zorgen dat medewerkers deze wetten en voorschriften naleven. Als u vragen hebt of meer wilt weten, neem dan contact op met OEC of een lid van het Global Privacy-team.  Klik voor contacten en aanvullende informatie op het pictogram Resources. |
| [Screen 11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=18_C_14)  [18\_C\_14](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=18_C_14) | Collection   * Notice * Consent   MANAGEMENT   * Data Integrity * Access and Correction   Usage   * Disclosure and Use   Disposition   * Retention and Disposal   Abbott’s data privacy and protection policies and procedures are organized around a simple set of principles. We call this Privacy by Design.  These principles are designed to help employees protect sensitive data at each stage of the data lifecycle. To illustrate, let’s look specifically at personal information.  The first stage of the data lifecycle is collection.  During this stage, Abbott uses a variety of methods to collect personal information. For example, we may request consumers to provide contact details at an Abbott website, or we may capture personal data generated from one of our devices.  In order to protect the privacy rights of the individuals during this stage, we maintain processes to ensure we adhere to the Privacy by Design principles of Notice and Consent.  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.  For example, when submitting an inquiry at abbott.com, the personal information we collect is used for the sole purpose of responding to the inquiry.  Consent is about providing individuals with the opportunity to agree to the collection and use of their personal information.  Generally, when we seek consent, we ensure it is:   * Freely given. The individual is never coerced or told that consent is a requirement. * Informed. The individual is given sufficient information to make a reasonable decision to which they are consenting. * Affirmative. The individual must affirmatively provide consent. We never assign consent, for example, through an individual’s silence, nor do we require the individual to take some action, such as unchecking a box, to opt out of something. * Revocable. The individual is provided with a clear explanation of how to revoke consent.   For example, a consumer registering with the Abbott Nutrition Similac© Strong Moms© Rewards program can consent to the collection and use of their Personal Information by opting in (e.g., checking a box) to receive additional promotional information.  The second stage of the data lifecycle is management.  During this stage, information is processed and stored.  In order to protect personal information during this stage, we maintain processes that ensure we adhere to the principles of:   * Data Integrity, and * Access and Correction.   Data Integrity is about taking reasonable measures to ensure that the personal information we retain is accurate, complete, and current.  One way we do this is by tracking and recording all activities that process personal information. This ensures we can identify the source of the data, the specific purposes for which the data has been processed, and where it is stored.  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.  This includes responding to an individual’s request to access, delete, transfer, or amend the stored records of personal information.  The third stage of the lifecycle is usage.  During this stage, personal information is used to support activities across the organization.  In order to protect personal information during this stage, we maintain processes that ensure we adhere to the principle of Disclosure and Use.  Disclosure and Use is about controlling who has access to personal information and limiting use to specific purposes.  We manage this through access controls and other processes. These controls and processes limit access to individuals in specific job functions as well as limiting use to the specific purposes set out in the notice for which consent was provided.  The final stage of the lifecycle is 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.  In order to protect personal information during this stage, we maintain policies and processes that ensure we adhere to the principle of Retention and Disposal.  Retention and Disposal of personal information is about retaining personal information for only the time necessary to achieve the purposes for which it was needed and processed.  Once personal information is no longer required in an active production environment, Abbott has put in place processes to either archive or dispose of it in a manner consistent with Abbott’s data management, retention, and disposal requirements. Our retention and disposal requirements are also subject to any legal hold requirements relating to legal matters.  For additional information related to retention or disposal requirements, see Abbott’s Global Records and Information Policy (l1-02) or contact Information Governance and Records. Details can be found in the Resources section of this training.  For contacts and additional information, click the Resources icon.  As we have just seen, our policies and procedures are designed to protect personal information throughout its lifecycle.  We do this by adhering to the principles of:   * Notice, * Consent, * Data Integrity, * Access and Correction, * Disclosure and Use, and * Retention and Disposal.   COLLECTION  Notice  Consent  MANAGEMENT  Data Integrity  Access and Correction  USAGE  Disclosure and Use  DISPOSITION  Retention and Disposal | Verzameling   * Kennisgeving * Toestemming   BEHEER   * Gegevensintegriteit * Toegang en correctie   Gebruik   * Openbaarmaking en gebruik   Dispositie   * Bewaren en verwijderen   Het beleid en de procedures voor gegevensprivacy en -bescherming van Abbott zijn georganiseerd rond een eenvoudige reeks principes. We noemen dit 'ingebouwde privacy'.  Deze principes zijn bedoeld om werknemers te helpen gevoelige gegevens in elke fase van de levenscyclus van gegevens te beschermen. Laten we ter illustratie specifiek naar persoonlijke informatie kijken.  De eerste fase van de levenscyclus van gegevens is het verzamelen.  Tijdens deze fase gebruikt Abbott verschillende methoden om persoonlijke informatie te verzamelen. We kunnen consumenten bijvoorbeeld vragen om contactgegevens op een Abbott-website te verstrekken, of we kunnen persoonlijke gegevens vastleggen die zijn gegenereerd door een van onze apparaten.  Om de privacyrechten van de mensen tijdens deze fase te beschermen, onderhouden we processen om ervoor te zorgen dat we ons houden aan de ingebouwde privacyprincipes van kennisgeving en toestemming.  Kennisgeving gaat over mensen laten weten welke persoonlijke informatie er wordt verzameld en in duidelijke, nauwkeurige en ondubbelzinnige taal uitleggen hoe we van plan zijn die informatie te gebruiken.  Wanneer u bijvoorbeeld een aanvraag indient bij abbott.com, wordt de persoonlijke informatie die we verzamelen alleen gebruikt om op de aanvraag te reageren.  Toestemming gaat over mensen de mogelijkheid te bieden om in te stemmen met het verzamelen en gebruiken van hun persoonlijke gegevens.  Over het algemeen zorgen we ervoor dat wanneer we toestemming vragen:   * Vrijelijk gegeven worden. Een persoon wordt nooit gedwongen of verteld dat toestemming een vereiste is. * Geïnformeerd zijn. De persoon krijgt voldoende informatie om een redelijke beslissing te nemen waarmee hij/zij instemt. * Bevestigend zijn. Het individu moet bevestigend toestemming geven. We kennen nooit toestemming toe, bijvoorbeeld via het zwijgen van een persoon, noch vereisen we dat de persoon een actie onderneemt, zoals het uitschakelen van een vakje, om zich voor iets af te melden. * Herroepbaar zijn. De persoon krijgt een duidelijke uitleg over hoe de toestemming kan worden ingetrokken.   Een consument die zich bijvoorbeeld registreert bij het Abbott Nutrition Similac© Strong Moms©-beloningsprogramma kan toestemming geven voor het verzamelen en gebruiken van zijn/haar persoonlijke gegevens door zich in te schrijven (bijv. door een vakje aan te vinken) om aanvullende promotionele informatie te ontvangen.  De tweede fase van de levenscyclus van gegevens is beheer.  Tijdens deze fase wordt informatie verwerkt en opgeslagen.  Om persoonlijke informatie tijdens deze fase te beschermen, onderhouden we processen die ervoor zorgen dat we ons houden aan de principes van:   * gegevensintegriteit, en * toegang en correctie.   Gegevensintegriteit gaat over het nemen van redelijke maatregelen om ervoor te zorgen dat de persoonlijke informatie die we bewaren nauwkeurig, volledig en actueel is.  Een manier waarop we dit doen, is door alle activiteiten die persoonlijke informatie verwerken bij te houden en vast te leggen. Dit zorgt ervoor dat we de bron van de gegevens kunnen identificeren, evenals de specifieke doeleinden waarvoor de gegevens zijn verwerkt en waar deze zijn opgeslagen.  Toegang en correctie gaat over mensen redelijke toegang tot hun gegevens te bieden en de mogelijkheid om hun rechten in verband met deze gegevens uit te oefenen.  Dit omvat het reageren op het verzoek van een persoon om de opgeslagen persoonlijke gegevens te openen, te verwijderen, over te dragen of te wijzigen.  De derde fase van de levenscyclus van gegevens is het gebruik.  Tijdens deze fase wordt persoonlijke informatie gebruikt om activiteiten in de hele organisatie te ondersteunen.  Om persoonlijke informatie tijdens deze fase te beschermen, onderhouden we processen die ervoor zorgen dat we ons houden aan het principe van openbaarmaking en gebruik.  Openbaarmaking en gebruik gaat over het beheersen wie er toegang heeft tot persoonlijke informatie en het beperken van het gebruik tot specifieke doeleinden.  We beheren dit via toegangscontroles en andere processen. Deze controles en processen beperken de toegang tot personen in specifieke functies en beperken het gebruik tot de specifieke doeleinden die zijn uiteengezet in de kennisgeving waarvoor toestemming is verleend.  De laatste fase van de levenscyclus van gegevens is dispositie.  Dispositie verwijst naar wat er met gegevens gebeurt als deze niet langer actief worden gebruikt. Activiteiten kunnen bestaan uit verwijderen, archiveren of bewaren vanwege juridische bewaarplicht.  Om persoonlijke informatie tijdens deze fase te beschermen, handhaven we beleid en processen die ervoor zorgen dat we ons houden aan het principe van bewaring en verwijdering.  Bewaring en verwijdering van persoonlijke informatie gaat over het alleen bewaren van persoonlijke informatie gedurende de tijd die nodig is om de doeleinden te bereiken waarvoor deze informatie nodig was en waarvoor deze werd verwerkt.  Abbott heeft processen ingevoerd op basis waarvan persoonlijke informatie die niet langer nodig is in een actieve productieomgeving wordt gearchiveerd of verwijderd op een manier die consistent is met de vereisten voor gegevensbeheer, -bewaring en -verwijdering die bij Abbott gelden. Onze vereisten voor bewaring of verwijdering zijn ook onderworpen aan eventuele wettelijke bewaarplichten met betrekking tot wettelijke zaken.  Raadpleeg voor aanvullende informatie met betrekking tot vereisten voor bewaring of verwijdering, Abbott's Global Records and Information Policy (l1-02) of neem contact op met de afdeling Information Governance and Records. Details zijn te vinden in het Hoofdstuk Resources van deze training.  Klik voor contacten en aanvullende informatie op het pictogram Resources.  Zoals we zojuist hebben gezien, zijn ons beleid en onze procedures ontworpen om persoonlijke informatie gedurende de gehele levenscyclus te beschermen.  We doen dit door ons te houden aan de principes van:   * kennisgeving, * toestemming, * gegevensintegriteit, * toegang en correctie, * openbaarmaking en gebruik, en * bewaren en verwijderen.   VERZAMELING  Kennisgeving  Toestemming  BEHEER  Gegevensintegriteit  Toegang en correctie  GEBRUIK  Openbaarmaking en gebruik  DISPOSITIE  Bewaren en verwijderen |
| [Screen 12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=19_C_15)  [19\_C\_15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=19_C_15) | Click the arrow to begin your review.  Review  Take a moment to review some of the key concepts covered in this section.  Personal Information (PI)  PI is any information that can be used to   * Contact * Locate, or * Identify an individual.   Protected Health Information (PHI)  PHI is a particularly sensitive type of personal information used in the healthcare industry.  Privacy Laws  Privacy laws 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 a set of principles, called Privacy by Design.  Notice and Consent  Notice and Consent is about letting people know what PI is being collected and providing them the opportunity to agree to that collection.  Data Integrity  Data Integrity is about taking reasonable measures to ensure that PI is accurate, complete, and current.  Access and Correction  Access and Correction is about providing individuals the right to access and correct their data.  Disclosure and Use  Disclosure and Use is about controlling who has access to PI.  Retention and Disposal  Retention and Disposal of PI is about retaining personal information for only the time necessary to achieve the purposes for which it was needed and processed.  To check your progress, click the Menu button  Great job!  You have completed section 1 of 4  Click the forward arrow to continue learning | Klik op het pijltje om met uw beoordeling te beginnen.  Opnieuw bekijken  Neem even de tijd voor het bestuderen van een aantal van de belangrijkste concepten waarover het in dit hoofdstuk gaat.  Persoonlijke informatie (PI)  Onder PI wordt elke informatie verstaan die kan worden gebruikt voor   * contact opnemen * lokaliseren of * identificeren van een individueel persoon.   Beschermde gezondheidsinformatie (Protected Health Information, PHI)  Beschermde gezondheidsinformatie is een bijzonder gevoelige soort persoonlijke informatie die in de gezondheidszorg wordt gebruikt.  Privacywetten  Privacywetten verschillen van land tot land, maar omarmen vaak dezelfde kernprincipes.  Abbott's principes van ingebouwde privacy (Privacy by Design)  Het beleid en de procedures van Abbott op het gebied van gegevensprivacy en -bescherming is georganiseerd rond een aantal principes met de naam Privacy by Design (ingebouwde privacy).  Keuze en toestemming  Bij Keuze en toestemming gaat het over mensen laten weten welke persoonlijke informatie wordt verzameld en hen de gelegenheid te geven om in te stemmen met die verzameling.  Gegevensintegriteit  Bij Gegevensintegriteit gaat het over het nemen van redelijke maatregelen om ervoor te zorgen dat de persoonlijke informatie nauwkeurig, volledig en actueel is.  Toegang en correctie  Bij Toegang en correctie gaat het over individuele personen het recht geven op toegang tot en correctie van hun gegevens.  Openbaarmaking en gebruik  Bij Openbaarmaking en gebruik gaat het over onder controle houden wie toegang heeft tot persoonlijke informatie.  Bewaren en verwijderen  Bij Bewaren en verwijderen gaat over het alleen bewaren van persoonlijke informatie gedurende de tijd die nodig is om de doeleinden te bereiken waarvoor deze informatie nodig was en waarvoor deze werd verwerkt.  Om uw voortgang te controleren, klikt u op de knop Menu  Prima gedaan!  Hoofdstuk 1 van 4 afgerond  Klik op het vooruitpijltje om verder te gaan |
| [Screen 13](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=20_C_17)  [20\_C\_17](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=20_C_17) | Another type of sensitive data that we may frequently use is confidential business information.  Confidential business information is a broad category. It includes much of the business information we use and come in contact with on a daily basis. Confidential Information is information that is not publicly available that might be of use to Abbott’s competitors or harmful to Abbott if disclosed. | Een ander type gevoelige gegevens die we vaak gebruiken, is vertrouwelijke bedrijfsinformatie.  Vertrouwelijke bedrijfsinformatie is een brede categorie. Het bevat veel van de zakelijke informatie die we gebruiken en waarmee we dagelijks in contact komen. Vertrouwelijke informatie is informatie die niet openbaar beschikbaar is die van nut kan zijn voor concurrenten van Abbott of schadelijk voor Abbott indien bekendgemaakt. |
| [Screen 14](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=21_C_18)  [21\_C\_18](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=21_C_18) | Kandice | Marketing Manager  Can you give me some examples of confidential business information?  Confidential business information can include, but is not limited to: product designs and processes, compositions, organisms, computer software, research and development data, clinical and pharmacological data, patient data, technical data, customer and prospective customer lists, business practices, marketing plans and strategies, financial and operational data, and personnel data.  It can also include purchasing information, such as bids for contracts, supplier lists, and costing information. | Kandice | Marketing Manager  Kunt u mij enkele voorbeelden geven van vertrouwelijke bedrijfsinformatie?  Vertrouwelijke bedrijfsinformatie kan zijn, maar is niet beperkt tot: productontwerpen en processen, samenstellingen, organismen, computersoftware, onderzoeks- en ontwikkelingsgegevens, klinische en farmacologische gegevens, patiëntgegevens, technische gegevens, lijsten met klanten en potentiële klanten, zakelijke praktijken, marketingplannen en -strategieën, financiële en operationele gegevens en personeelsgegevens.  Dit geldt ook voor inkoopinformatie, zoals offertes voor contracten, leverancierslijsten en kosteninformatie. |
| [Screen 15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19)  [22\_C\_19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19) | Jerry | Sales Representative  Are there certain types of confidential business information that are more sensitive than others?  Yes. 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, manufacturing formulas and processes; * Clinical and regulatory data, regulatory submissions, or pre-approval information; and * Financial data that has not been released to the public. | Jerry | Sales Representative  Zijn er bepaalde soorten vertrouwelijke bedrijfsinformatie die gevoeliger zijn dan andere?  Ja. Bepaalde soorten vertrouwelijke bedrijfsinformatie vereisen meer zorgvuldigheid dan normaal, omdat ongepaste openbaarmaking of ongeoorloofd gebruik van deze informatie het bedrijf ernstig kan schaden.  Voorbeelden zijn:   * bedrijfsgeheimen, productieformules en -processen; * klinische en regelgevende gegevens, indieningen bij regelgevende instanties, of informatie voorafgaand aan een goedkeuring; en * financiële gegevens die niet zijn vrijgegeven voor het publiek. |
| [Screen 16](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=23_C_20)  [23\_C\_20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=23_C_20) | As you can see, most of the business information we use in our day-to-day work activities is considered confidential.  A good way to confirm whether the business information you are using is confidential is to ask yourself a simple question:  Is this information publicly available?  If the answer is no, then the information should be considered confidential and appropriate steps must be taken to protect it. | Zoals u kunt zien, wordt de meeste zakelijke informatie die we gebruiken bij onze dagelijkse werkzaamheden als vertrouwelijk beschouwd.  Een goede manier om te bevestigen of de bedrijfsinformatie die u gebruikt vertrouwelijk is, is door uzelf een eenvoudige vraag te stellen:  Is deze informatie openbaar beschikbaar?  Als het antwoord nee is, moet de informatie als vertrouwelijk worden beschouwd en moeten er passende maatregelen worden genomen om deze te beschermen. |
| [Screen 17](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=24_C_20b)  [24\_C\_20b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=24_C_20b) | It is also important to remember that any confidential business information created as part of your job function at Abbott is Abbott’s property.  As a result, you must protect this information and cannot keep it if your Abbott employment ends. | Het is belangrijk om te weten dat alle vertrouwelijke bedrijfsinformatie die wordt opgesteld als onderdeel van uw werkzaamheden bij Abbott geldt als eigendom van Abbott.  Daarom moet u deze informatie beschermen en mag u deze niet behouden als uw werkzaamheden bij Abbott eindigen. |
| [Screen 18](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=25_C_20c)  [25\_C\_20c](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=25_C_20c) | Protecting confidential business information is crucial.  Not surprisingly, the improper use or disclosure of this information can result in significant harm to Abbott. | Het beschermen van vertrouwelijke bedrijfsinformatie is van cruciaal belang.  Het is dus niet verrassend dat ongepast gebruik of openbaarmaking van deze informatie aanzienlijke schade voor Abbott kan opleveren. |
| [Screen 19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=26_C_20d)  [26\_C\_20d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=26_C_20d) | The improper use or disclosure of confidential information can significantly harm Abbott’s relationship with its customers and clients, lead to embarrassing press and media coverage, and result in the loss of competitive advantages for Abbott. It can also result in civil lawsuits and criminal penalties, including against current and former employees.  CLICK THE ‘RECENT CASES’ BUTTON FOR MORE INFORMATION. | Ongepast gebruik of openbaarmaking van vertrouwelijke informatie kan aanzienlijke schade aan de relatie van Abbott met haar klanten en cliënten opleveren, leiden tot gênante berichten in de pers en media, en resulteren in het verlies van concurrentievoordelen voor Abbott. Het kan ook leiden tot civiele gerechtelijke procedures en strafrechtelijke boetes, waaronder tegen huidige en vroegere medewerkers.  KLIK OP DE KNOP “RECENTE GEVALLEN” VOOR MEER INFORMATIE. |
| [Screen 19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=27_C_20d)  [27\_C\_20d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=27_C_20d) | RECENT CASES  In recent years, companies have received large jury verdicts and awards against former employees for improperly taking company information. For example, one company received $240 million award against a former employee who improperly disclosed the company’s confidential information to a competitor. Another company received an $854 million jury award against a former employee and his new employer when the former employee misappropriated the company’s confidential information and then used the company’s confidential information on behalf of the new employer.  Studies indicate that the theft of confidential information causes losses between $209 and $625 billion to publicly traded companies. | RECENTE GEVALLEN  De afgelopen jaren hebben bedrijven belangrijke juryvonnissen gekregen en zijn toekenningen uitgesproken tegen vroegere medewerkers die op ongepaste wijze bedrijfsinformatie meenamen. Eén bedrijf kreeg bijvoorbeeld een toekenning van $ 240 miljoen tegen een voormalig werknemer die op ongepaste wijze de vertrouwelijke informatie van het bedrijf openbaar had gemaakt aan een concurrent. Een ander bedrijf kreeg een toekenning van een jury van $ 854 miljoen tegen een voormalig werknemer en zijn nieuwe werkgever nadat de voormalig werknemer de vertrouwelijke informatie van het bedrijf ontvreemdde en de vertrouwelijke informatie van het bedrijf vervolgens namens zijn nieuwe werkgever gebruikte.  Uit studies blijkt dat de diefstal van vertrouwelijke informatie verliezen van tussen $ 209 en $ 625 miljard dollar opleveren voor beursgenoteerde bedrijven. |
| [Screen 20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=28_C_20e)  [28\_C\_20e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=28_C_20e) | It should come as no surprise that authorities take the theft of confidential information very seriously.  For example, under federal criminal statutes, an individual can face up to ten years in prison and a $5 million fine for stealing confidential information. In addition, if a company is found guilty of stealing confidential information, it can be fined $10 million or three times the value of the confidential information.  CLICK THE ‘FINES AND PENALTIES’ BUTTON FOR MORE INFORMATION. | Het zal geen verrassing zijn dat de autoriteiten de diefstal van vertrouwelijke informatie zeer serieus nemen.  In overeenstemming met federale strafwetten kan een persoon bijvoorbeeld tot 10 jaar gevangenisstraf krijgen en een boete van $ 5 miljoen voor het stelen van vertrouwelijke informatie. Bovendien geldt dat als een bedrijf schuldig wordt bevonden aan het stelen van vertrouwelijke informatie het een boete van $ 10 miljoen of 3 keer de waarde van de vertrouwelijke informatie kan krijgen.  KLIK OP DE KNOP “BOETES EN SANCTIES” VOOR MEER INFORMATIE. |
| [Screen 20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=29_C_20e)  [29\_C\_20e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=29_C_20e) | FINES AND PENALTIES  In recent years, several people and companies have been fined or sentenced to prison for stealing confidential information. For example:   * A competitor was fined $60 Million for stealing another company’s confidential information; * A former IT employee was sentenced to 97 months in prison for stealing confidential information; * A former salesman was sentenced to 12 months in prison for stealing confidential information; * A senior executive was sentenced to 24 months in prison for stealing confidential information; and * A research scientist was sentenced to 18 months in prison for stealing confidential information. | BOETES EN SANCTIES  De afgelopen jaren hebben verscheidene mensen en bedrijven een boete gekregen of een gevangenisstraf voor het stelen van vertrouwelijke informatie. Bijvoorbeeld:   * een concurrent heeft een boete van $ 60 miljoen gekregen voor het stelen van vertrouwelijke informatie van een ander bedrijf; * een voormalige IT-medewerker is veroordeeld tot 97 maanden gevangenisstraf voor het stelen van vertrouwelijke informatie; * een voormalig verkoper is veroordeeld tot 12 maanden gevangenisstraf voor het stelen van vertrouwelijke informatie; * een hogere leidinggevende is veroordeeld tot 24 maanden gevangenisstraf voor het stelen van vertrouwelijke informatie; en * Een onderzoekswetenschapper is veroordeeld tot 18 maanden gevangenisstraf voor het stelen van vertrouwelijke informatie. |
| [Screen 21](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=30_C_21)  [30\_C\_21](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=30_C_21) | Another type of confidential business information that is important to recognize and protect is 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. | Een ander soort vertrouwelijke bedrijfsinformatie die belangrijk is om te herkennen en die speciaal moet worden beschermd, is *voorkennis.*  Voorkennis is alle niet-openbare, belangrijke informatie waarvan redelijkerwijs mag worden verwacht dat deze, indien openbaar gemaakt, de marktwaarde van de aandelen van een bedrijf zou beïnvloeden, of die van invloed is op de beslissingen van beleggers over het al dan niet kopen of verkopen van aandelen. |
| [Screen 22](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=31_C_22)  [31\_C\_22](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=31_C_22) | Examples of insider information include:   * News of a potential acquisition, * A delay in a product launch, * News of a breach of internal IT systems, * Unanticipated changes in earnings or dividend rates, * Proposed tender offers or stock splits, * Information about major new products, * Contract awards, * Expansion plans, * Significant litigation or regulatory proceedings, etc. | Voorbeelden van voorkennis zijn:   * nieuws van een mogelijke overname, * een vertraging in een productlancering, * nieuws over een inbreuk op interne IT-systemen, * onverwachte veranderingen in winst of dividendpercentages, * voorgestelde offertevoorstellen of aandelensplitsingen, * informatie over belangrijke nieuwe producten, * toekenning van contracten, * uitbreidingsplannen, * belangrijke procesvoering of regelgevingsprocedures, enz. |
| [Screen 23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23)  [32\_C\_23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23) | If you are aware or in possession of insider information, it is illegal to trade in, or recommend others to trade in, Abbott securities.  This also applies to the buying and selling of securities of other companies, including those currently doing or expected to do business with Abbott.  To learn more about Abbott’s expectations with regard to the use and protection of unpublicized information, review Abbott’s policy on Insider Trading. Details can be found in the Resources section of this training. | Als u op de hoogte bent van of in het bezit bent van voorkennis, is het illegaal om te handelen in de aandelen van Abbott, of anderen aan te bevelen om te handelen in de aandelen van Abbott.  Dit geldt ook voor het kopen en verkopen van aandelen van andere bedrijven, inclusief bedrijven die momenteel zaken doen of waarvan wordt verwacht dat ze zaken zullen doen met Abbott.  Raadpleeg voor meer informatie over de verwachtingen van Abbott met betrekking tot het gebruik en de bescherming van niet-gepubliceerde informatie het Abbott-beleid inzake handelen met voorkennis. Details zijn te vinden in het Hoofdstuk Resources van deze training. |
| [Screen 24](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=33_C_24)  [33\_C\_24](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=33_C_24) | Click the arrow to begin your review.  Review  Take a moment to review some of the key concepts covered in this section.  Confidential Business Information  Any business information that is not publicly available should be considered confidential. This includes much of the business information we use in our day-to-day work activities.  Improper Use of Confidential Business Information  The improper use or disclosure of confidential business information can result in significant harm to the Company, our customers and employees.  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.  To check your progress, click the Menu button  Great job!  You have completed section 2 of 4  Click the forward arrow to continue learning | Klik op het pijltje om met uw beoordeling te beginnen.  Opnieuw bekijken  Neem even de tijd voor het bestuderen van een aantal van de belangrijkste concepten waarover het in dit hoofdstuk gaat.  Vertrouwelijke bedrijfsinformatie  Alle bedrijfsinformatie die niet openbaar beschikbaar is, moet als vertrouwelijk worden beschouwd. Hieronder valt een groot deel van de bedrijfsinformatie die we bij onze dagelijkse werkactiviteiten gebruiken.  Ongepast gebruik van vertrouwelijke bedrijfsinformatie  Onjuist gebruik of openbaarmaking van vertrouwelijke bedrijfsinformatie kan leiden tot aanzienlijke schade voor het bedrijf, onze klanten en onze medewerkers.  Voorkennis  Voorkennis is alle niet-openbare, belangrijke informatie waarvan redelijkerwijs mag worden verwacht dat deze, indien openbaar gemaakt, de marktwaarde van de aandelen van een bedrijf zou beïnvloeden, of die van invloed is op de beslissingen van beleggers over het al dan niet kopen of verkopen van aandelen.  Om uw voortgang te controleren, klikt u op de knop Menu  Prima gedaan!  U hebt Hoofdstuk 2 van 4 afgerond  Klik op het vooruitpijltje om verder te gaan met leren. |
| [Screen 25](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=34_C_25)  [34\_C\_25](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=34_C_25) | Now that you have a good understanding of the different kinds of data you are likely to encounter during your workday, here is what you can do to help protect it. | Nu u een goed begrip heeft van de verschillende soorten gegevens die u tijdens uw werkdag kunt tegenkomen, kunt u het volgende doen om deze gegevens te helpen beschermen. |
| [Screen 26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=35_C_26)  [35\_C\_26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=35_C_26) | Before accessing any sensitive data, make sure your role and responsibilities require you to access the data.  If you have a question about whether you should access the data, especially with respect to personal information, contact your manager, the OEC or a member of the Global Privacy team.  CLICK THE ‘DID YOU KNOW’ BUTTON FOR MORE INFORMATION. | Voordat u toegang krijgt tot gevoelige gegevens, moet u zich ervan overtuigen dat uw functie en verantwoordelijkheden het noodzakelijk maken dat u toegang heeft tot die gegevens.  Als u zich afvraagt of u toegang moet krijgen tot de gegevens (vooral met betrekking tot persoonlijke informatie) neem dan contact op met uw manager, OEC of een lid van het Global Privacy-team.  KLIK OP DE KNOP ‘WIST U DAT’ VOOR MEER INFORMATIE. |
| [Screen 26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=36_C_26)  [36\_C\_26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=36_C_26) | DID YOU KNOW  Abbott engages in various forms of lawful monitoring to reduce the risk of improper data usage.  This include monitoring the downloading of data or the sending of data to non-Abbott email addresses. | WIST U DAT?  Abbott zich bezighoudt met verschillende vormen van wettelijke monitoring om het risico op ongepast gegevensgebruik te verminderen?  Hieronder valt ook het controleren van het downloaden van gegevens of het verzenden van gegevens naar e-mailadressen die niet van Abbott zijn. |
| [Screen 27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27)  [37\_C\_27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27) | If you have permission to access sensitive data, only use it for the specific purpose for which you have been granted access.  In the case of personal information, only use the data according to the consent given or notice provided. | Als u toestemming hebt om toegang te krijgen tot gevoelige gegevens, gebruik deze dan alleen voor het specifieke doel waarvoor u toegang hebt gekregen.  Gebruik in het geval van persoonlijke informatie de gegevens alleen in overeenstemming met de gegeven toestemming of kennisgeving. |
| [Screen 28](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=38_C_30)  [38\_C\_30](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=38_C_30) | Before sharing sensitive data, make sure the person you plan to share with has proper authorization.  If you have a question about whether you should access the data, especially with respect to personal information, talk to your manager or a member of Abbott’s Privacy team. | Voordat u gevoelige gegevens deelt, moet u ervoor zorgen dat de persoon met wie u van plan bent te delen, de juiste toestemming heeft.  Als u zich afvraagt of u toegang mag hebben tot de gegevens, vooral met betrekking tot persoonlijke informatie, neem dan contact op met uw manager of een lid van het Privacy-team van Abbott. |
| [Screen 29](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=39_C_31)  [39\_C\_31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=39_C_31) | Requests from Your Own Country  If an Abbott employee located in your same country requests sensitive data, always:   * Confirm the identity of the person making the request; * Confirm the person’s need to access the information; * Check to make sure the person is authorized to receive the information; * Verify that the information can be used for the requested purpose; and * Share only the amount of information required to meet the need, not more.   If in doubt, contact OEC or Global Privacy prior to sharing sensitive data. | Verzoeken uit uw eigen land  Als een medewerker van Abbott in hetzelfde land om gevoelige gegevens vraagt, moet u altijd:   * de identiteit bevestigen van de persoon die het verzoek indient; * de noodzaak van de persoon om toegang te krijgen tot de informatie bevestigen; * controleren of de persoon bevoegd is om de informatie te ontvangen; * controleren of de informatie kan worden gebruikt voor het gevraagde doel; en * alleen de hoeveelheid informatie delen die nodig is om aan de behoefte te voldoen, niet meer.   Neem bij twijfel contact op met OEC of Global Privacy voordat u gevoelige gegevens deelt. |
| [Screen 30](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=40_C_32)  [40\_C\_32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=40_C_32) | Requests from Other Countries  Many countries and regions have laws designed to protect the rights of their citizens, and place restrictions on the transference of personal information across national borders.  If you receive a request for information containing sensitive data from a colleague in a different country than your own, check your division or function’s data privacy policies, or consult OEC or Global Privacy before proceeding. Then, follow the same steps you would if responding to a request from a colleague in your own country. | Verzoeken uit andere landen  Veel landen en regio's hebben wetten die zijn ontworpen om de rechten van hun burgers te beschermen en die beperkingen opleggen aan de overdracht van persoonlijke informatie buiten de nationale grenzen.  Als u een verzoek om informatie ontvangt dat gevoelige informatie over een collega in een ander land dan het uwe behelst, controleer dan het gegevensprivacybeleid van uw afdeling of functie of raadpleeg OEC of Global Privacy voordat u het verzoek inwilligt. Daarna moet u dezelfde stappen volgen als wanneer u zou reageren op een verzoek van een collega in eigen land. |
| [Screen 31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33)  [41\_C\_33](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33) | Requests from Third Parties  If the request for sensitive data is from a third party, ensure there is a valid and appropriate contractual agreement in place. If you are unsure, contact OEC, Global Privacy, or Legal prior to sharing. | Verzoeken van derden  Als het verzoek om gevoelige gegevens van een derde partij is, zorg er dan voor dat er een geldige en passende contractuele overeenkomst is. Neem bij twijfel contact op met OEC, Global Privacy of Legal voordat u iets deelt. |
| [Screen 32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35)  [42\_C\_35](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35) | Always archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements. | Archiveer of verwijder gevoelige gegevens altijd op een manier die in overeenstemming is met de vereisten voor gegevensbeheer, bewaring en verwijdering van Abbott. |
| [Screen 33](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=43_C_36)  [43\_C\_36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=43_C_36) | If you receive a legal hold order, you are prohibited from discarding, destroying, or deleting any information covered by the hold.  If you have questions related to legal hold orders or retention and disposal, contact the attorney/paralegal listed in the Legal Hold notification, or call the Litigation Department at (224) 667-5701. | Als u een juridische bewaarorder ontvangt, mag u de informatie die onder de bewaarorder valt nooit weggooien, vernietigen of verwijderen.  Als u vragen hebt met betrekking tot juridische bewaarorders of bewaren en weggooien, neemt u dan contact op met de jurist/juridisch medewerker die wordt genoemd in de kennisgeving van de juridische bewaarorder of neem telefonisch contact op met het Litigation Department op (224) 667-5701. |
| [Screen 34](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37)  [44\_C\_37](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37) | Always take special care with sensitive data when someone leaves Abbott.  Managers must ensure the departing employee is terminated in the appropriate system (e.g., Workday for Employees or Fieldglass for Contingent Workers) as soon as they are notified the employee is leaving. This will ensure access to Abbott data, physical access to buildings, and final pay will be properly managed. | Wees altijd extra voorzichtig met gevoelige gegevens wanneer iemand Abbott verlaat.  Managers moeten ervoor zorgen dat de vertrekkend werknemer uit de toepasselijke systemen wordt verwijderd (bijv. Workday voor werknemers of Fieldglass voor tijdelijke werknemers) zodra hij/zij berichtgeving ontvangt dat de werknemer vertrekt. Dit zorgt ervoor dat de toegang tot gegevens van Abbott, fysieke toegang tot bedrijfspanden en de laatste uitbetaling op de juiste wijze worden beheerd. |
| [Screen 35](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=45_C_37b)  [45\_C\_37b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=45_C_37b) | Ensure no sensitive data leaves with the departing employee. Transition all files to the Abbott employee who will be assuming the departing person’s role or responsibilities.  Remind the departing employee of the obligation not to keep or disclose sensitive information. Employees may not take their work product or any other Abbott property (e.g. mobile devices) with them when they leave Abbott. If you have questions about your local termination process, contact Human Resources. | Zorg dat er geen gevoelige gegevens meegaan met de vertrekkende werknemer. Draag alle bestanden over aan de werknemer van Abbott die de rol of verantwoordelijkheden van de vertrekkende persoon op zich neemt.  Herinner de vertrekkende werknemer aan de verplichting om geen gevoelige informatie te behouden of openbaar te maken. Werknemers mogen hun werkproduct of ander eigendom van Abbott (bijv. mobiele apparatuur) niet meenemen als zij Abbott verlaten. Heeft u vragen over uw plaatselijke ontslagproces, neem dan contact op met Human Resources. |
| [Screen 36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38)  [46\_C\_38](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38) | Inadvertent disclosures of PHI can happen at any time.  For example, you may overhear a nurse discussing details of a patient’s health status or you may accidentally be copied on an email containing details of a patient’s record. | Onbedoelde bekendmakingen van beschermde gezondheidsinformatie kunnen op elk moment plaatsvinden.  U kunt bijvoorbeeld opvangen dat een verpleegkundige details over de gezondheidstoestand van een patiënt bespreekt of dat uw e-mailadres per ongeluk worden gekopieerd in een e-mail met details over het dossier van een patiënt. |
| [Screen 37](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=47_C_38a)  [47\_C\_38a](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=47_C_38a) | In response to any inadvertent or improper disclosure of a patient’s protected health information (PHI), you should immediately report the incident to OEC or a member of the Global Privacy team. | Na elke onbedoelde of ongepaste openbaarmaking van de beschermde gezondheidsinformatie van een patiënt moet u het incident onmiddellijk melden aan OEC of aan een lid van het Global Privacy team. |
| [Screen 38](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=48_C_38b)  [48\_C\_38b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=48_C_38b) | If you become aware of the improper or inadvertent disclosure of Confidential Business Information, you should immediately report the disclosure to both:   * Your direct supervisor, and * OEC or a member of the Global Privacy team.   Your immediate reporting of the disclosure will help Abbott immediately retrieve the information, prevent additional improper or misuse of the information and if appropriate, assist the company with pursuing civil or criminal action. | Als u ongepaste of onbedoelde openbaarmaking van vertrouwelijke bedrijfsinformatie opmerkt, moet u de openbaarmaking melden aan:   * uw directe leidinggevende en * OEC of een lid van het Global Privacy-team.   Als u onmiddellijk de openbaarmaking meldt, helpt dit Abbott bij het direct terughalen van de informatie, het voorkomen van extra ongepast gebruik of misbruik van de informatie en indien gepast, het bedrijf helpen bij het ondernemen van civiele of juridische actie. |
| [Screen 39](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c)  [49\_C\_38c](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c) | You should never disclose Abbott sensitive data to anyone not authorized to receive the sensitive data.  Similarly, you should only use Abbott sensitive data on behalf of Abbott and while performing your Abbott business function.  If you improperly disclose sensitive data, you may face disciplinary action, up to and including termination of employment. | U mag nooit gevoelige gegevens van Abbott openbaar maken aan iemand die de gevoelige gegevens niet zou mogen ontvangen.  Daarnaast zou u gevoelige gegevens van Abbott alleen voor Abbott en bij het uitvoeren van uw zakelijke functie bij Abbott moeten gebruiken.  Als u op ongepaste wijze gevoelige gegevens bekendmaakt, kunt u te maken krijgen met disciplinaire maatregelen tot en met beëindiging van het dienstverband. |
| [Screen 40](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=50_C_38d)  [50\_C\_38d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=50_C_38d) | You are not permitted, both during and after your Abbott employment, to share Abbott data with any Abbott competitor. | U hebt geen toestemming om, zowel tijdens als na uw tewerkstelling bij Abbott, gegevens van Abbott met concurrenten van Abbott te delen. |
| [Screen 41](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=51_C_38e)  [51\_C\_38e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=51_C_38e) | Failure to return sensitive data to Abbott, transmitting sensitive data to an unapproved device, storage, account or server, or providing sensitive data to any person or entity not authorized to possess the information can lead to Abbott pursuing legal action against you.  CLICK THE ‘LEGAL ACTION’ BUTTON FOR MORE INFORMATION. | Als u gevoelige gegevens niet teruggeeft aan Abbott, gevoelige gegevens naar een niet-goedgekeurd apparaat, opslag, account of server stuurt of gevoelige gegevens aan een persoon of entiteit geeft die geen toestemming heeft om deze informatie te hebben, kan dit leiden tot een rechtszaak van Abbott tegen u.  KLIK OP DE KNOP ‘JURIDISCHE ACTIE’ VOOR MEER INFORMATIE. |
| [Screen 41](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=52_C_38e)  [52\_C\_38e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=52_C_38e) | LEGAL ACTION  Legal action could include Abbott filing a civil lawsuit against you that would:   * Prevent you from working for a new employer until Abbott sensitive data has been returned and protected; * Require you to turn over all electronic devices to Abbott for review and inspection; * Cause you to pay monetary damages for illegally retaining and/or using Abbott sensitive data, and violating the duties and obligations you owe Abbott under your Abbott Employment Agreement; and * Obligate you to pay the legal fees Abbott incurs as a result of filing a lawsuit to protect its sensitive data.   If necessary, Abbott will also work with local, state and federal authorities to protect and retain Abbott sensitive data. In this scenario, you could also face criminal penalties. | JURIDISCHE ACTIE  Juridische actie kan bestaan uit een civielrechtelijke procedure van Abbott die moet:   * voorkomen dat u gaat werken voor een nieuwe werkgever voordat de gevoelige gegevens van Abbott zijn teruggegeven en beschermd; * zorgen dat u al uw elektronische apparaten ter evaluatie en inspectie aan Abbott geeft; * zorgen dat u de financiële schade betaalt voor het illegaal behouden en/of gebruiken van gevoelige gegevens van Abbott en het overtreden van de plichten en verplichtingen jegens Abbott op basis van uw arbeidsovereenkomst met Abbott; en * verplichten dat u betaalt voor de juridische kosten van Abbott voor het aanspannen van een rechtszaak voor het beschermen van haar gevoelige gegevens.   Indien noodzakelijk werkt Abbott ook samen met lokale, staats- en federale autoriteiten om de gevoelige gegevens van Abbott te beschermen en behouden. U zou in dit scenario ook strafrechtelijke straffen kunnen krijgen opgelegd. |
| [Screen 42](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=53_C_43)  [53\_C\_43](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=53_C_43) | 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 Global Privacy. | Elk voorval dat een mogelijk gevaar voor de informatiebeveiliging inhoudt, met inbegrip van een verloren of gestolen mobiel apparaat, moet onmiddellijk worden gemeld aan uw plaatselijke Global Service Desk.  Als u zich zorgen maakt over een mogelijke schending of een mogelijk privacyincident wilt melden, neem dan contact op met Global Privacy. |
| [Screen 43](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=54_C_44)  [54\_C\_44](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=54_C_44) | Click the arrow to begin your review.  Review  Take a moment to review some of the key concepts covered in this section.  Accessing and Using Sensitive Data  Only access and use sensitive data for the specific purpose for which you have been granted access.  Sharing Sensitive Data  Before sharing sensitive data:   * Confirm the identity of the requestor; * Confirm their need to access the information; * Verify the information can be used for the purpose(s) requested; and * Share only the amount required to meet the need.   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.  Responding to Inadvertent Disclosure of PHI  In response to any inadvertent or improper disclosure of a patient’s PHI, immediately report the disclosure to OEC or a member of the Global Privacy team.  Reporting a Privacy Incident  Contact the Global Privacy team to report a potential privacy incident.  To check your progress, click the Menu button  Great job!  You have completed section 3 of 4  Click the forward arrow to continue learning | Klik op het pijltje om met uw beoordeling te beginnen.  Opnieuw bekijken  Neem even de tijd voor het bestuderen van een aantal van de belangrijkste concepten waarover het in dit Hoofdstuk gaat.  Toegang tot en gebruik van gevoelige gegevens  Als u toestemming hebt om toegang te krijgen tot gevoelige gegevens, gebruik deze dan alleen voor het specifieke doel waarvoor u toegang hebt gekregen.  Gevoelige gegevens delen  Voorafgaand aan het delen van gevoelige gegevens:   * bescherm de identiteit van de aanvrager; * bevestig dat het voor hem/haar noodzakelijk is om toegang te krijgen tot de informatie; * controleer of de informatie kan worden gebruikt voor het/de gevraagde doel(en); en * deel alleen de hoeveelheid informatie die nodig is om aan de behoefte te voldoen.   Gevoelige gegevens bewaren en verwijderen  Archiveer of verwijder gevoelige gegevens altijd op een manier die in overeenstemming is met de vereisten voor gegevensbeheer, bewaring en verwijdering van Abbott.  Reageren op onbedoelde openbaarmakingen van beschermde gezondheidsinformatie  Na elke onbedoelde of ongepaste openbaarmaking van de beschermde gezondheidsinformatie van een patiënt moet u het incident onmiddellijk melden aan OEC of aan een lid van het Global Privacy team.  Melden van een privacyincident  Neem contact op met het team van Global Privacy om een mogelijk privacyincident te melden.  Om uw voortgang te controleren, klikt u op de knop Menu  Prima gedaan!  U hebt Hoofdstuk 3 van 4 afgerond  Klik op het vooruitpijltje om verder te gaan met leren |
| [Screen 44](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=55_C_45)  [55\_C\_45](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=55_C_45) | Where to Get Help  Office of Ethics and Compliance (OEC)  Global Privacy – Contact Global Privacy via email at [privacy@abbott.com](mailto:privacy@abbott.com). You can find additional contact details and important information about privacy on the Global Privacy Portal [here](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) on Abbott World.  OEC Contacts – You are encouraged to contact the OEC at any time with any ethics and compliance questions, or to discuss concerns about possible violations of our written standards, laws, or regulations.   * Visit the [Contact OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) page on the [OEC website](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) on Abbott World or [OEC@abbott.com](mailto:OEC@abbott.com).   ENTERPRISE CYBERSECURITY  Visit the Enterprise Cybersecurity site [here](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) on Abbott World.  Visit the [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) site to learn about secure ways to share information.  Legal Division  Contact the [Legal Division](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) with questions or concerns about third-party contractual obligations regarding privacy and data protection.  Contact the Information Governance team at [information.governance@abbott.com](mailto:information.governance@abbott.com) with questions or concerns regarding retention requirements or for guidance on acceptable use of technology solutions.  REFERENCE POLICIES:   * Click [here](http://abbottmfiles.oneabbott.com/#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?limit=499&00_p100=107&01_p1170*=GLB-CONF-INFO&06_p39=138_p2C131&resultsFromEachRepository=true&includeUnmanaged=true) to review the Confidential Information Policy * Click [here](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) to review Abbott’s policy on Insider Trading * Click [here](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0) to review the Acceptable Technology Use Policy. * Click [here](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0) to review the Records and Information Policy on M-Files.   OEC Policies and Procedures  For our company’s global and country-specific OEC policies and procedures:   * Abbott employees should visit [iComply](https://icomply.abbott.com/Default.aspx).   Human Resources Service Center   * Click [here](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) for a list of HR support contact numbers.   Course Resources  Transcript  Click [here](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) for a full transcript of the course. | Waar u terecht kunt voor hulp  Het Bureau voor ethiek en naleving (OEC)  Wereldwijde privacy - Neem contact op met Global Privacy via e-mail op [privacy@abbott.com](mailto:privacy@abbott.com). U kunt [hier](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) op Abbott World aanvullende contactgegevens en belangrijke informatie vinden over privacy op de Global Privacy Portal.  OEC Contacten – U kunt op elk gewenst moment contact opnemen met de OEC voor vragen over ethische kwesties en naleving, of om de bezorgdheid over mogelijke schendingen van onze schriftelijke normen, wetten of voorschriften te bespreken.   * Bezoek de pagina [Contact OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) op de [OEC-website](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) op Abbott World of gebruik [OEC@abbott.com](mailto:OEC@abbott.com).   CYBERBEVEILIGING VAN ONDERNEMINGEN  Bezoek de Enterprise Cybersecurity website [hier](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) op Abbott World.  Bezoek de site [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) voor informatie over veilige manieren om informatie te delen.  De juridische afdeling  Neem contact op met de [juridische afdeling](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) bij vragen of opmerkingen over contractuele verplichtingen van derden met betrekking tot privacy en gegevensbescherming.  Neem contact op met het Information Governance-team via [information.governance@abbott.com](mailto:information.governance@abbott.com) met vragen of opmerkingen over bewaarvoorschriften of voor advies over het aanvaardbaar gebruik van technologische oplossingen.  REFERENTIEBELEID:   * Klik [hier](http://abbottmfiles.oneabbott.com/#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?limit=499&00_p100=107&01_p1170*=GLB-CONF-INFO&06_p39=138_p2C131&resultsFromEachRepository=true&includeUnmanaged=true) om het beleid voor vertrouwelijke informatie te bekijken * Klik [hier](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) om het beleid van Abbott inzake handel met voorkennis te bekijken * Klik [hier](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0) om het beleid voor acceptabel gebruik van technologie te bekijken. * Klik [hier](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0) om het beleid voor bestanden en informatie op M-Files te bekijken.   OEC-beleid en -procedures  Voor de wereldwijde en landspecifieke OEC-beleidslijnen en -procedures van ons bedrijf:   * moeten medewerkers van Abbott [iComply](https://icomply.abbott.com/Default.aspx) bezoeken.   Servicecentrum Personeelszaken (HR)   * Klik [hier](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) voor een lijst met contactnummers voor ondersteuning door HR.   Bij de cursus gebruikte middelen  Transcriptie  Klik [hier](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) voor een volledige transcriptie van de cursus. |
| [Screen 45](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=56_C_47)  [56\_C\_47](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=56_C_47) | The Knowledge Check consists of 10 questions. You must score 80% or higher to successfully complete this course.  When you are ready, click the Knowledge Check button. | De Kennischeck bestaat uit 10 vragen. U moet 80% of hoger scoren om deze cursus met succes af te ronden.  Wanneer u er klaar voor bent, klikt u op de knop **Kennischeck**. |
| Screen 46  Question 1: Scenario  57\_C\_48 | Assuming you have worked for Abbott for several years and have recently accepted an offer to work for another company, which of the following would you be legally allowed to take with you when you leave? | Ervan uitgaande dat u al een aantal jaren voor Abbott werkt en ondanks een aanbod heeft aanvaard om voor een ander bedrijf te gaan werken, welke van de volgende zult u dan wettelijk zijn toegestaan om mee te nemen als u vertrekt? |
| Screen 46  Question 1: Options  58\_C\_48 | [1] Personal Patient Information from clinical studies  [2] Abbott customers lists and presentation information that you created while working for Abbott  [3] Sales projections and financial data for your Abbott Division or Business Unit  [4] Personal photos and mementos | [1] Persoonlijke patiëntgegevens van klinische studies  [2] Lijsten van klanten van Abbott en presentatiegegevens die u tijdens uw werk voor Abbott hebt gemaakt  [3] Verkoopprognoses en financiële gegevens voor uw Divisie of Business Unit van Abbott  [4] Persoonlijke foto’s en herinneringen |
| Screen 46  Question 1: Feedback  59\_C\_48 | The correct answer is 4. Personal information, confidential business information, and Protected Health Information are all considered sensitive data that you cannot take with you or use after leaving Abbott. Additionally, all Abbott electronic devices and other Abbott property must be returned prior to leaving.  For more information, see  Section 3.4, Responding to Improper Disclosures. | Het juiste antwoord is 4. Persoonlijke informatie, vertrouwelijke bedrijfsinformatie en beschermde gezondheidsinformatie worden alle beschouwd als gevoelige gegevens die u niet mee kunt nemen of gebruiken nadat u Abbott verlaten hebt. Bovendien moeten alle elektronische apparaten en andere eigendommen van Abbott vóór het vertrek worden teruggegeven.  Raadpleeg voor meer informatie  Hoofdstuk 3.4, Reageren op onbedoelde openbaarmakingen. |
| Screen 46  Question 2: Scenario  60\_C\_48 | A Marketing Manager is working on a new product launch and must create a consent form for potential customers. The form will allow for the collection and use of personal information. To align with Abbott’s practices for consent, which of the following must be true for the consent form?  Check all that apply. | Een marketingmanager werkt aan een nieuwe productlancering en moet een toestemmingsformulier opstellen voor mogelijke klanten. Het formulier zal de verzameling en het gebruik van persoonlijke informatie mogelijk maken. Welke van de volgende moet waar zijn wil het toestemmingsformulier aansluiten bij de bij Abbott geldende praktijken voor toestemming?  Vink alles aan wat van toepassing is. |
| Screen 46  Question 2: Options  61\_C\_48 | [1] The form must not pressure customers into giving their consent.  [2] The form must provide customers with all the information about how their personal information will be used.  [3] The form must require customers to actively agree to the collection and use of their personal information.  [4] The form must not allow customers to withdraw their consent once they have given it. | [1] Het formulier mag klanten niet onder druk zetten om hun toestemming te geven.  [2] Het formulier moet klanten voorzien van alle informatie over de manier waarop hun persoonlijke informatie zal worden gebruikt.  [3] Het formulier moet van klanten eisen dat ze actief instemmen met de verzameling en het gebruik van hun persoonlijke informatie.  [4] Het formulier mag klanten niet toestaan om hun toestemming weer in te trekken nadat zij deze hebben gegeven. |
| Screen 46  Question 2: Feedback  62\_C\_48 | Abbott's practices for consent require that the form:   * Be clear and concise. * Not pressure people into giving their consent. * Provide all information about how personal information will be used. * Require people to actively agree to the collection and use of their personal information. * Allow withdrawal of consent if desired.   For more information, see  Section 1.3, Abbott’s Privacy by Design Principles. | De praktijken bij Abbott voor toestemming vereisen dat het formulier:   * duidelijk en beknopt is. * mensen niet onder druk zet om hun toestemming te geven. * alle informatie geeft over de manier waarop persoonlijke informatie zal worden gebruikt. * van mensen eist dat ze actief instemmen met de verzameling en het gebruik van hun persoonlijke informatie. * desgewenst intrekking van de toestemming toestaan.   Zie voor meer informatie  Hoofdstuk 1.3, De ingebouwde privacy- principes van Abbott. |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Openbaarmaking en gebruik van gevoelige gegevens zoals persoonlijke informatie wordt bij Abbott beheerd door middel van: |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] De-identificatie van alle gegevens.  [2] Toegangscontroles.  [3] Zowel 1 als 2. |
| Screen 46  Question 3: Feedback  65\_C\_48 | Disclosure and Use of personal information are managed through access controls and other processes that limit access and use to individuals in specific job functions and for the specific purposes set out in the notice for which consent was given.  For more information, see  Section 1.3, Abbott’s Privacy by Design Principles. | De openbaarmaking en het gebruik van persoonlijke informatie worden beheerd via toegangscontroles en andere processen die de toegang en het gebruik beperken tot personen in specifieke functies en voor de specifieke doeleinden die zijn uiteengezet in de kennisgeving waarvoor de toestemming is gegeven.  Zie voor meer informatie  Hoofdstuk 1.3, De ingebouwde privacy- principes van Abbott. |
| Screen 46  Question 4: Scenario  66\_C\_48 | Which of the following is true in relation to the retention and disposal of personal information?  Check all that apply. | Welke van de volgende is juist met betrekking tot het bewaren van en beschikken over persoonlijke informatie?  Vink alles aan wat van toepassing is. |
| Screen 46  Question 4: Options  67\_C\_48 | [1] Personal information is only retained for the time necessary to achieve the purposes for which it was collected and processed.  [2] Once data is no longer required in an active production environment, it should always be disposed of.  [3] Retention and disposal of personal information is subject to any holds relating to legal matters. | [1] Persoonlijke gegevens worden alleen bewaard voor de tijd die nodig is om de doeleinden te bereiken waarvoor ze zijn verzameld en verwerkt.  [2] Zodra gegevens niet langer nodig zijn in een actieve productieomgeving, moeten ze altijd worden verwijderd.  [3] Het bewaren en verwijderen van persoonlijke informatie is onderhevig aan de bewaarplicht met betrekking tot juridische zaken. |
| Screen 46  Question 4: Feedback  68\_C\_48 | Generally, Abbott should only retain personal information for the time necessary to achieve the purposes for which it was collected and processed. Once data is no longer required in an active production environment, it should be either archived or disposed of, in a manner consistent with Abbott’s data management, retention, and disposal requirements. Retention and disposal requirements are also subject to any holds relating to legal matters.  For more information about the correct answer, Section 1.3, Abbott’s Privacy by Design Principles. | Over het algemeen mag Abbott persoonlijke informatie alleen bewaren voor de tijd die nodig is om de doeleinden te bereiken waarvoor deze is verzameld en verwerkt. Zodra gegevens niet langer nodig zijn in een actieve productieomgeving, moeten ze worden gearchiveerd of verwijderd op een manier die consistent is met de vereisten voor gegevensbeheer, bewaring en verwijdering van Abbott. Vereisten inzake bewaren en verwijderen zijn ook onderworpen aan eventuele bewaarplichten met betrekking tot juridische zaken.  Zie voor meer informatie over het juiste antwoord Hoofdstuk 1.3, Abbott's ingebouwde privacy- principes. |
| Screen 46  Question 5: Scenario  69\_C\_48 | An Engineer is working on developing a new product. Which of the following would be considered confidential business information that must be kept secure?  Check all that apply. | Een technicus werkt aan de ontwikkeling van een nieuw product. Welke van de volgende zal worden beschouwd als vertrouwelijke bedrijfsinformatie die veilig moet worden gehouden?  Vink alles aan wat van toepassing is. |
| Screen 46  Question 5: Options  70\_C\_48 | [1] Sales projections and forecasts for the new product.  [2] Financial reporting data from Abbott’s Annual Report.  [3] Purchasing information, such as bids for contracts for the new product.  [4] Competitive information about similar products.  [5] Proposals from third-party suppliers related to the new product. | [1] Verkoopprojecties en -voorspellingen voor het nieuwe product.  [2] Financiële rapportagegegevens uit het jaarverslag van Abbott.  [3] Inkoopinformatie, zoals offertes voor contracten voor het nieuwe product.  [4] Concurrentie-informatie over soortgelijke producten.  [5] Voorstellen van externe leveranciers met betrekking tot het nieuwe product. |
| Screen 46  Question 5: Feedback  71\_C\_48 | Confidential Business Information is a broad category. It includes much of the business information we use and come in contact with on a daily basis. A good way to confirm whether something is confidential is to ask yourself a simple question:  Is this information publicly available?  If the answer is no, then the information is most certainly confidential, and you should take appropriate steps to protect it.  For more information, see Section 2.1, Recognizing Confidential Business Information. | Vertrouwelijke bedrijfsinformatie is een brede categorie. Het bevat veel van de zakelijke informatie die we gebruiken en waarmee we dagelijks in contact komen. Een goede manier om te controleren of iets vertrouwelijk is, is door uzelf een eenvoudige vraag te stellen:  Is deze informatie openbaar beschikbaar?  Als het antwoord nee is, is de informatie zeer zeker vertrouwelijk en moet u passende maatregelen nemen om deze te beschermen.  Voor meer informatie, zie Hoofdstuk 2.1, Vertrouwelijke bedrijfsinformatie herkennen. |
| Screen 46  Question 6: Scenario  72\_C\_48 | The Global Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws in the world. Implemented in 2018, it is the standard for privacy protection. This regulation was designed in: | De Algemene Verordening Gegevensbescherming (AVG) behoort tot de meest uitgebreide privacywetten ter wereld. De verordening is geïmplementeerd in 2018 en is de norm voor privacybescherming. Deze verordening werd opgesteld in: |
| Screen 46  Question 6: Options  73\_C\_48 | [1] Canada  [2] Asia  [3] Europe  [4] Russia  [5] United States  [6] Latin America | [1] Canada  [2] Azië  [3] Europa  [4] Rusland  [5] Verenigde Staten  [6] Latijns-Amerika |
| Screen 46  Question 6: Feedback  74\_C\_48 | The correct answer is Europe. In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate.  For more information, see Section 1.2, Legal, Regulatory and Contractual Agreements. | Het juiste antwoord is Europa. In Europa behoort de Algemene Verordening Gegevensbescherming (AVG) tot de meest uitgebreide privacywetten en sinds de implementatie ervan in 2018 bepaalt deze verordening de norm voor privacybescherming die andere landen proberen te evenaren.  Zie voor meer informatie Hoofdstuk 1.2 Wet- en regelgeving, contractuele overeenkomsten. |
| Screen 46  Question 7: Scenario  75\_C\_48 | Your colleague just completed a project that involved collecting and using personal data. He's since received a request from another department to access that data. You advise your colleague to: | Uw collega heeft net een project afgerond waarbij de verzameling en het gebruik van persoonsgegevens aan de orde was. Hij heeft sindsdien een verzoek ontvangen van een andere afdeling om toegang tot de gegevens. U adviseert uw collega om: |
| Screen 46  Question 7: Options  76\_C\_48 | [1] Confirm the requester's identity and their need to access the information.  [2] Verify that the requester is authorized to have a copy of the information.  [3] Make sure that the data can be used for the requested purposes.  [4] All of the above. | [1] De identiteit van de aanvrager en zijn/haar noodzaak om toegang te krijgen tot de informatie te bevestigen.  [2] Te verifiëren dat de aanvrager is geautoriseerd om een kopie van de informatie te hebben.  [3] Zich ervan te overtuigen dat de gegevens kunnen worden gebruikt voor het doel waarvoor deze zijn aangevraagd.  [4] Alle bovengenoemde opties. |
| Screen 46  Question 7: Feedback  77\_C\_48 | One of the most common causes of data incidents within an organization is the improper sharing of data with unauthorized personnel. Before sharing any document or file containing sensitive data, always:   * Confirm the identity of the person making the request and the person’s need to access the information. * Check to make sure the person is authorized to have a copy of the information. * Verify that the information can be used for the purposes they are requesting to use it for. * Share only the amount of information required to meet the need, not more.   For more information, see Section 3.2, Sharing Sensitive Data. | Een van de meest voorkomende oorzaken van gegevensincidenten binnen een organisatie is het onjuist delen van gegevens met ongeautoriseerd personeel. Voordat u een document of bestand met gevoelige gegevens deelt, moet u altijd:   * de identiteit van de persoon die het verzoek indient controleren, evenals de behoefte van de persoon om toegang te krijgen tot de informatie; * controleren of de persoon bevoegd is om een ​​kopie van de informatie te hebben; * controleren of de informatie kan worden gebruikt voor de doeleinden waarvoor het is aangevraagd; * alleen de hoeveelheid informatie delen die nodig is om aan de behoefte te voldoen, niet meer.   Voor meer informatie, zie Hoofdstuk 3.2, Delen van gevoelige gegevens. |
| Screen 46  Question 8: Scenario  78\_C\_48 | You are a Sales Representative visiting a clinic in your area. While waiting in the reception area, you accidentally misplace sensitive documents containing a patient's protected health information. What do you do? | U bent verkoopvertegenwoordiger en bezoekt een ziekenhuis in uw regio. Terwijl u bij de receptie wacht, legt u onbedoeld gevoelige documenten met beschermde gezondheidsinformatie op een verkeerde plaats. Wat doet u? |
| Screen 46  Question 8: Options  79\_C\_48 | [1] Notify the clinic's privacy officer.  [2] Contact your supervisor.  [3] Report the incident to OEC or a member of the Global Privacy team. | [1] De privacyfunctionaris van het ziekenhuis informeren.  [2] Contact opnemen met uw leidinggevende.  [3] Het incident melden aan OEC of een lid van het Global Privacy-team. |
| Screen 46  Question 8: Feedback  80\_C\_48 | In response to any inadvertent disclosure of a patient’s protected health information, you should immediately report the incident to:   * OEC or a member of the Global Privacy team.   For more information, see Section 3.4, Responding to Improper Disclosures. | Als reactie op elke onbedoelde openbaarmaking van de beschermde gezondheidsinformatie van een patiënt, moet u het incident onmiddellijk melden aan:   * OEC of een lid van het Global Privacy-team.   Raadpleeg voor meer informatie  Hoofdstuk 3.4, Reageren op ongepaste openbaarmakingen. |
| Screen 46  Question 9: Scenario  81\_C\_48 | While traveling to work on the train, you accidentally leave your laptop containing sensitive work documents at your seat and exit the train. You realize your mistake when you reach your office and frantically search for your laptop, but it is nowhere to be found. What should you do first? | Terwijl u per trein naar uw werk reist laat u onbedoeld uw laptop met daarop gevoelige werkdocumenten op uw zitplaats in de trein liggen en verlaat u de trein. U realiseert zich uw fout als u op kantoor bent en naar uw laptop zoekt, maar deze nergens kunt vinden. Wat zijn de eerste stappen die u moet zetten? |
| Screen 46  Question 9: Options  82\_C\_48 | [1] Call the train company and ask if someone turned in your laptop.  [2] Go back to the train station and search for your laptop.  [3] Contact your local Global Service Desk. | [1] De spoorwegmaatschappij bellen en vragen of iemand uw laptop daar heeft afgegeven.  [2] Teruggaan naar het treinstation en uw laptop zoeken.  [3] Contact opnemen met uw lokale Global Service Desk. |
| Screen 46  Question 9: Feedback  83\_C\_48 | If you believe that sensitive information may have been compromised, such as through a lost or stolen laptop, please contact your local Global Service Desk immediately.  For more information, see Section 3.4, Reporting a Data Incident. | Als u van mening bent dat mogelijk gevoelige informatie is gecompromitteerd, zoals door een verloren of gestolen laptop, moet u onmiddellijk contact opnemen met uw lokale Global Service Desk.  Zie voor meer informatie Hoofdstuk 3.4, Het melden van een gegevensincident. |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | U mag persoonlijke informatie uitsluitend gebruiken:  Vink alles aan wat van toepassing is. |
| Screen 46  Question 10: Options  85\_C\_48 | [1] For the specific purpose for which you have been granted access.  [2] According to the notice provided to the data subject.  [3] According to the consent granted by the data subject. | [1] Voor het specifieke doel waarvoor u er toegang toe is verleend.  [2] In overeenstemming met de kennisgeving verstrekt aan de betrokkene.  [3] In overeenstemming met de toestemming verleend door de betrokkene. |
| Screen 46  Question 10: Feedback  86\_C\_48 | If you have permission to access personal information, only use it:   * For the specific purpose for which you have been granted access. * According to the notice provided to the data subject. * According to the consent granted by the data subject.   For more information, see Section 3.1 Accessing and Using Sensitive Data. | Als u toestemming heeft om toegang te verkrijgen tot persoonlijke informatie, mag u deze uitsluitend gebruiken:   * Voor het specifieke doel waarvoor u er toegang toe is verleend. * In overeenstemming met de kennisgeving verstrekt aan de betrokkene. * In overeenstemming met de toestemming verleend door de betrokkene.   Zie voor meer informatie over het juiste antwoord Hoofdstuk 3.1, Toegang tot en gebruik van gevoelige gegevens. |
| [Screen 46](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48)  [87\_C\_48](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48) | All questions remain unanswered | Alle vragen blijven onbeantwoord |
| [Screen 47](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49)  [88\_C\_49](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49) | No results are available, as you have not completed the Knowledge Check.  Congratulations! You have successfully passed the Knowledge Check and completed the course.  Please review your results below by clicking on each question.  Once you are done, you must click the EXIT [X] icon in the course title bar before closing your browser window or browser tab.  Sorry, you did not pass the Knowledge Check. Take a few minutes to review your results below by clicking on each question.  When you are done, click the Retake Knowledge Check button. | Er zijn geen resultaten beschikbaar, omdat u de Kennischeck niet hebt voltooid.  Gefeliciteerd! U hebt de Kennischeck succesvol afgerond en de cursus voltooid.  Bekijk uw resultaten hieronder door op elke vraag te klikken.  Nadat u klaar bent, moet u klikken op het pictogram **AFSLUITEN [X]** in de titelbalk van de cursus voordat u uw browservenster of -tabblad sluit.  Helaas, u bent niet geslaagd voor de Kennischeck. Neem even de tijd om uw resultaten hieronder te bekijken door op elke vraag te klikken.  Wanneer u klaar bent, klikt u op de knop **Kennischeck opnieuw doen**. |
| 89\_toc\_1 | Introduction | Inleiding |
| 90\_toc\_2 | Welcome | Welkom |
| 91\_toc\_3 | Objectives | Doelstellingen |
| 92\_toc\_4 | Menu | Menu |
| 93\_toc\_5 | Personal Information | Persoonlijke informatie |
| 94\_toc\_6 | Recognizing Personal Information | Persoonlijke informatie herkennen |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Wet- en regelgeving en contractuele vereisten |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Abbott's principes van ingebouwde privacy (Privacy by Design) |
| 97\_toc\_9 | Review | Opnieuw bekijken |
| 98\_toc\_10 | Confidential Business Information | Vertrouwelijke bedrijfsinformatie |
| 99\_toc\_11 | Recognizing Confidential Business Information | Vertrouwelijke bedrijfsinformatie herkennen |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | De kosten voor het niet beschermen van vertrouwelijke bedrijfsinformatie |
| 101\_toc\_13 | Insider Information | Voorkennis |
| 102\_toc\_14 | Review | Opnieuw bekijken |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Uw rol bij het beschermen van gevoelige gegevens |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Toegang tot en gebruik van gevoelige gegevens |
| 105\_toc\_17 | Sharing Sensitive Data | Gevoelige gegevens delen |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Gevoelige gegevens bewaren en verwijderen |
| 107\_toc\_19 | Responding to Improper Disclosures | Reageren op ongepaste openbaarmakingen |
| 108\_toc\_20 | Review | Opnieuw bekijken |
| 109\_toc\_21 | Knowledge Check | Kennischeck |
| 110\_toc\_22 | Introduction | Inleiding |
| 111\_toc\_23 | Assessment | Toets |
| 112\_toc\_24 | Question 1 | Vraag 1 |
| 113\_toc\_25 | Question 2 | Vraag 2 |
| 114\_toc\_26 | Question 3 | Vraag 3 |
| 115\_toc\_27 | Question 4 | Vraag 4 |
| 116\_toc\_28 | Question 5 | Vraag 5 |
| 117\_toc\_29 | Question 6 | Vraag 6 |
| 118\_toc\_30 | Question 7 | Vraag 7 |
| 119\_toc\_31 | Question 8 | Vraag 8 |
| 120\_toc\_32 | Question 9 | Vraag 9 |
| 121\_toc\_33 | Question 10 | Vraag 10 |
| 122\_toc\_34 | Feedback | Feedback |
| 123\_string\_1 | The Course cannot contact the LMS. Click 'OK' to continue and review the course. Note, Course Certification may not be available. Click 'Cancel' to exit | De cursus kan geen verbinding maken met het LMS. Klik op 'OK' om verder te gaan en de cursus opnieuw door te nemen. Let op, het cursuscertificaat is mogelijk niet beschikbaar. Klik op 'Annuleren' om af te sluiten |
| 124\_string\_2 | All questions remain unanswered | Alle vragen blijven onbeantwoord |
| 125\_string\_3 | Questions | Vragen |
| 126\_string\_4 | Question | Vraag |
| 127\_string\_5 | not answered | niet beantwoord |
| 128\_string\_6 | That's correct! | Dat is juist! |
| 129\_string\_7 | That's not correct! | Dat is niet juist! |
| 130\_string\_8 | Feedback: | Feedback: |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | BESCHERMEN VAN GEVOELIGE GEGEVENS |
| 132\_string\_10 | Knowledge Check | Kennischeck |
| 133\_string\_11 | Submit | Indienen |
| 134\_string\_12 | Retake Knowledge Check | Kennischeck opnieuw doen |
| 135\_string\_13 | Course Description: At Abbott, we frequently use sensitive data to make important business decisions. Because many of our stakeholders have concerns about how this data is collected and used, Abbott has policies and procedures in place to ensure this data is protected. This course explains what sensitive data is, why it is vital to our business, and what steps we can take to ensure we process and handle this information safely and securely. This course will take approximately 30 minutes to complete. | Cursusbeschrijving: Bij Abbott gebruiken we vaak gevoelige gegevens om belangrijke zakelijke beslissingen te nemen. Omdat veel van onze belanghebbenden zich zorgen maken over hoe deze gegevens worden verzameld en gebruikt, heeft Abbott beleidsregels en procedures ingevoerd om ervoor te zorgen dat deze gegevens worden beschermd. In deze cursus wordt uitgelegd wat gevoelige gegevens zijn, waarom ze van vitaal belang zijn voor ons bedrijf en welke stappen we kunnen nemen om ervoor te zorgen dat we deze informatie veilig en beveiligd verwerken en behandelen. Het voltooien van deze cursus duurt ongeveer 30 minuten. |
| 136\_string\_14 | Menu | Menu |
| 137\_string\_15 | Resources | Hulpbronnen |
| 138\_string\_16 | Reference Material | Referentiemateriaal |
| 139\_string\_17 | Audio | Audio |
| 140\_string\_18 | Exit | Afsluiten |
| 141\_string\_19 | Record My Results | Mijn resultaten vastleggen |