|  |  |  |
| --- | --- | --- |
| 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. | Protection des données sensibles  Cliquez sur la flèche « Suivant » pour commencer. |
| [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. | Abbott s’appuie sur des données, qui contiennent souvent des informations sensibles, pour prendre ses décisions.  Afin de remplir notre mission, qui consiste à aider les gens à vivre au mieux au travers d’une bonne santé, nous devons impérativement protéger ces données et nous conformer aux lois et aux normes éthiques en vigueur chez Abbott. Ce cours est conçu pour vous enseigner les compétences nécessaires pour le faire. |
| [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. | À l’issue de la formation, vous comprendrez mieux :   * ce que sont les données sensibles ; * comment Abbott protège ces données ; * votre rôle dans la protection des données sensibles ; et * que faire si vous pensez que des données sensibles ont été divulguées par erreur ou compromises. |
| [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 | Informations personnelles  Vous apprendrez comment les gouvernements, les consommateurs et le public sont devenus de plus en plus sensibles à la protection de la vie privée et la sécurité des informations personnelles.  12 minutes  Section 1 | Informations personnelles  Identifier les informations personnelles  Obligations légales, réglementaires et contractuelles  Principes d’Abbott sur Respect de la vie privée assuré dès la conception  Révision  2 | Informations commerciales confidentielles  Vous apprendrez pourquoi la plupart des informations commerciales que nous utilisons dans le cadre de nos activités courantes sont considérées comme confidentielles.  5 minutes  Section 2 | Informations commerciales confidentielles  Identifier les informations commerciales confidentielles  Ce que cela coûte de ne pas protéger les informations commerciales confidentielles  Information privilégiée  Révision  3 | Protection des données sensibles  Vous apprendrez ce que vous pouvez faire pour contribuer à la protection des données sensibles.  8 minutes  Section 3 | Votre rôle dans la protection des données sensibles  Accéder et utiliser des données sensibles  Partager des données sensibles  Conserver et éliminer des informations sensibles  Réagir aux divulgations inappropriées  Révision  4 | Contrôle des connaissances  Évaluez vos connaissances des principaux concepts et principes évoqués dans le cours.  5 minutes  Section 4 | Contrôle des connaissances  Évaluation  Cliquez sur le panneau pour commencer.  Cliquez sur le bouton jaune « Lecture » pour commencer.  Le contenu n’est pas encore disponible. Vous devez terminer la Section{a} {b}. |
| [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. | Chez Abbott, les informations personnelles sont un type courant de données sensibles que nous utilisons.  Depuis quelques années, les gouvernements, les consommateurs et le grand public sont de plus en plus sensibles à la question de la protection de la vie privée et de la sécurité des informations personnelles. |
| [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. | Les informations personnelles sont toutes les informations qui peuvent être utilisées pour identifier, contacter ou localiser une personne en particulier. |
| [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 | Responsable marketing  Pouvez-vous me donner des exemples d’informations personnelles ?  Les informations personnelles peuvent inclure des détails personnels comme le nom, la date de naissance, l’adresse e-mail et le numéro de téléphone.  Cela peut inclure des informations portant sur l’apparence physique d’une personne, comme la couleur de ses cheveux ou son poids.  Cela peut également inclure des informations sur la vie privée d’une personne comme des photos, les cookies d’un navigateur ou des informations de localisation. |
| [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 | Délégué commercial  Les informations personnelles incluent-elles aussi les informations de santé protégées ?  Oui.  Les Informations de santé protégées (PHI) correspondent à un type d’informations personnelles particulièrement sensibles qui sont utilisées dans le secteur de la santé. Cela comprend toutes les informations permettant d’identifier un individu dans un dossier médical, y compris lorsqu’elles sont utilisées dans le cadre de conversations entre des professionnels de santé portant sur les soins. |
| [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. | Dans la plupart des pays où Abbott exerce ses activités, des lois et des règlements sont en place pour protéger les informations personnelles, y compris les informations de santé protégées.  Les lois relatives à la protection de la vie privée et à la protection des informations personnelles diffèrent d’un pays à l’autre, mais présentent souvent les mêmes principes fondamentaux.  CLIQUEZ SUR CHACUNE DES ZONES SURLIGNÉES À L’ÉCRAN POUR EN SAVOIR PLUS SUR LES DIFFÉRENTS TYPES DE LOIS ET D’EXIGENCES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE À TRAVERS LE MONDE. |
| [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. | Europe  En Europe, le Règlement général sur la protection des données (RGPD) est l’une des lois les plus exhaustives au monde en matière de protection de la vie privée. Mis en œuvre en 2018, le RGPD a établi la norme de protection de la vie privée que d’autres pays tentent d’imiter. Le RGPD s’applique aux organisations situées en Europe, mais également aux organisations situées en dehors de l’Europe si elles offrent des biens et services ou encadrent les activités de toute personne résidant en Europe.  L’un des concepts clés du RGPD est le droit à l’effacement, également connu sous le nom de droit à l’oubli. Ce droit permet aux personnes de demander que leurs données personnelles soient effacées des dossiers de l’entreprise. L’entreprise qui reçoit une telle demande doit prendre des mesures pour effacer les données de ses systèmes et empêcher toute utilisation ou divulgation ultérieure. Il peut y avoir des exceptions aux demandes des personnes concernées. Néanmoins, Abbott informera chaque personne concernée de la suite donnée à chaque demande. Les violations du RGPD peuvent être sanctionnées par de lourdes amendes pour l’entreprise, représentant jusqu’à 4 % de son chiffre d’affaires mondial annuel ou 20 millions d’EUR (le montant le plus élevé étant retenu) pour les violations les plus graves. |
| [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. | États-Unis  Aux États-Unis, il n’existe pas de loi universelle pour protéger les informations personnelles. En revanche, des lois et règlements relatifs à la protection de la vie privée s’appliquent à des secteurs et types de données spécifiques. Par exemple, HIPAA, la loi sur la portabilité et la responsabilité des assurances maladie, protège la confidentialité des données relatives aux soins de santé, tandis que la Loi sur les rapports de solvabilité équitables (Fair Credit Reporting Act) protège les informations relatives au crédit.  Toutefois, certains États ont commencé à promulguer leurs propres lois exhaustives sur la confidentialité des données. Par exemple, la Californie a adopté la loi sur la protection de la vie privée des consommateurs (California Consumer Privacy Act ou CCPA) qui donne aux Californiens certains droits sur leurs données, dont le droit de savoir quelles informations personnelles sont recueillies à leur sujet et le droit de supprimer toute information personnelle recueillie. En 2023, la CCPA sera modifiée par la loi californienne sur les droits à la vie privée (California Privacy Rights Act ou CPRA) qui donnera aux particuliers encore plus de droits sur leurs données.  D’autres États dont la Virginie, le Colorado, l’Utah et le Connecticut ont également adopté leurs propres lois sur la confidentialité des données. Bien que la législation de chaque État diffère, elle confère généralement aux personnes des droits sur leurs données et oblige les entreprises à fournir certaines informations sur leurs activités de traitement des données.  Les amendes infligées en cas de violation des lois sur la protection de la vie privée peuvent être importantes. Par exemple, la Californie peut infliger aux entreprises des amendes allant jusqu’à 7 500 USD par violation de la CCPA.  Canada  Au Canada, des lois, tant au niveau fédéral que provincial, sont conçues pour protéger les informations personnelles des personnes. Par exemple, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE ou PIPEDA en anglais) est une loi fédérale qui s’applique aux entreprises du secteur privé et dont l’application est assurée par le Commissariat à la protection de la vie privée du Canada.  Au niveau provincial, le Québec, l’Alberta et la Colombie-Britannique ont adopté des lois sur la protection de la vie privée similaires à la LPRPDE. D’autres provinces ont également mis en place des règles qui offrent des protections similaires des informations personnelles, notamment les provinces de l’Ontario, du Nouveau-Brunswick, de Terre-Neuve-et-Labrador et de la Nouvelle-Écosse, qui ont adopté des lois sur la confidentialité des données de santé.  Ces lois visent à empêcher que les informations personnelles soient mal gérées ou collectées à l’insu des personnes concernées et à leur permettre d’accéder à leurs propres informations et de corriger toute erreur.  Enfreindre ces lois peut entraîner de lourdes amendes. Par exemple, enfreindre la LPRPDE peut entraîner une amende pouvant atteindre 100 000 USD. En Alberta, la loi sur la protection des informations personnelles (Personal Information Protection Act ou PIPA) prévoit des amendes pouvant atteindre 10 000 USD pour les particuliers et 500 000 USD pour les entreprises. |
| [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. | Asie Pacifique  Les lois sur la protection de la vie privée dans la région Asie-Pacifique ne cessent de se développer et de se préciser. Certains pays, comme la Chine, ont mis en œuvre des mesures de localisation des données qui obligent les entreprises à stocker certaines données personnelles sur des serveurs situés sur leur territoire. En outre, la Chine a des exigences en matière d’évaluation de l’impact sur la vie privée et la sécurité concernant le transfert transfrontalier d’informations personnelles.  D’autres, comme l’Australie et Singapour, ont adopté une approche de la vie privée davantage axée sur le consommateur, qui lui permet de mieux contrôler ses informations, notamment le droit de savoir comment les entreprises les utilisent et la possibilité d’y accéder et de les corriger si besoin.  Les peines encourues par les entreprises qui enfreignent les lois sur la confidentialité des données varient également considérablement à travers la région. En Chine, par exemple, les entreprises peuvent se voir infliger une amende allant jusqu’à 500 000 RMB (environ 72 000 USD) en cas de violation des lois sur la confidentialité des données.  Par contre, à Singapour, les entreprises peuvent se voir infliger une amende allant jusqu’à 1 million SGD (environ 737 000 USD) pour avoir enfreint la loi sur la protection de la vie privée du pays. |
| [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. | Russie  La Russie dispose également de lois visant à protéger les données de ses citoyens, notamment une loi sur la localisation des données qui oblige les entreprises à stocker les données personnelles des citoyens russes sur des serveurs situés en Russie.  La loi s’applique aux entreprises qui traitent les données des citoyens russes, qu’elles soient basées ou non en Russie. Ainsi, par exemple, une entreprise basée aux États-Unis qui traite les données de citoyens russes devra se conformer à cette loi.  Comme de nombreux autres pays, la loi impose également aux entreprises de prendre des mesures pour protéger les données personnelles qu’elles traitent. Par exemple, les entreprises doivent s’assurer de l’exactitude et de la pertinence des données et prendre des mesures pour éviter qu’elles ne soient mal gérées, perdues ou volées.  En cas d’infraction, les amendes peuvent aller de 12 000 à 72 000 USD pour la première infraction et jusqu’à 216 000 USD pour la deuxième infraction. |
| [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. | Amérique Latine  La plupart des pays d’Amérique Latine ont promulgué des lois de protection de la vie privée. Toutefois, de nombreux pays de la région, notamment l’Équateur, l’Argentine et le Brésil, ont récemment révisé leur réglementation en matière de protection de la vie privée afin de s’aligner sur les normes internationales.  L’Équateur, par exemple, a récemment adopté la loi organique sur la protection des données personnelles (LPPD), qui entrera en vigueur en 2023. Cette loi concerne toute entreprise dans le monde qui traite des données personnelles en Équateur.  Comme dans d’autres pays de la région, la LPPD exige que les entreprises informent les personnes concernées et obtiennent leur consentement avant d’utiliser leurs données, qu’elles les détruisent lorsqu’elles ne sont plus nécessaires et qu’elles respectent certaines restrictions avant de partager des données avec d’autres pays. Ces mesures permettent de protéger la vie privée des personnes en Amérique Latine et de s’assurer que les entreprises traitent les données personnelles de manière responsable.  Toute violation de la LPPD peut entraîner de lourdes amendes, allant de 3 % à 17 % du chiffre d’affaires annuel de l’année précédente de l’entreprise, ce qui incite fortement ces dernières à respecter la loi. |
| [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. | En plus des lois et réglementations régissant la façon dont Abbott exerce ses activités, les contrats que nous passons avec certains clients incluent parfois des obligations supplémentaires.  Par exemple, le gouvernement des États-Unis est un client d’Abbott. En vertu des conditions d’un tel accord, nous devons respecter les obligations stipulées dans la Loi sur la protection des renseignements personnels des États-Unis de 1974 (U.S. Privacy Act of 1974).  CLIQUEZ SUR LE BOUTON « PRIVACY ACT » POUR EN SAVOIR PLUS. |
| [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  Le Privacy Act of 1974 (5 U.S.C. 552a) est une importante réglementation fédérale. Elle établit un Code de déontologie de l’information régissant la collecte, l’entretien, l’utilisation et la diffusion d’informations permettant d’identifier un individu qui sont conservées dans les systèmes de dossiers par les agences fédérales. Dans le cadre de certaines transactions, Abbott peut avoir accès à des dossiers d’agences gouvernementales. Le cas échéant, Abbott doit respecter plusieurs obligations, y compris l’obligation de prouver que la formation sur la protection de la vie privée concernant la protection des informations permettant d’identifier un individu a été suivie.  Les employés doivent contacter le service juridique avant de conclure des accords avec des clients ayant eux-mêmes des obligations en matière de protection de la vie privée. |
| [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. | Les lois, les réglementations et les obligations contractuelles que nous venons de présenter sont souvent complexes et peuvent rapidement changer.  Abbott a mis en place des politiques et des procédures pour s’assurer que ses employés respectent ces lois et réglementations. Si vous avez des questions ou souhaitez en savoir plus, contactez le BEC ou un membre de l’équipe mondiale de la protection de la vie privée.  Cliquez sur l’icône « Ressources » pour en savoir plus et pour consulter les coordonnées. |
| [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 | Collecte   * Avis * Consentement   GESTION   * Intégrité des données * Accès et correction   Utilisation   * Divulgation et utilisation   Élimination   * Conservation et élimination   Les politiques et procédures d’Abbott en matière de protection des données et de la vie privée sont articulées autour d’un ensemble de principes. C’est ce que l’on appelle le Respect de la vie privée assuré dès la conception.  Ces principes ont pour but d’aider les employés à protéger les données sensibles à chaque étape du cycle de vie des données. Mais revenons aux informations personnelles pour que cela soit plus concret.  La collecte est la première étape du cycle de vie des données.  Au cours de cette étape, Abbott utilise différentes méthodes pour collecter des informations personnelles. Par exemple, nous pouvons demander aux consommateurs de fournir leurs coordonnées sur un site Web Abbott ou nous pouvons capturer les données personnelles générées à partir de l’un de nos appareils.  Afin de protéger les droits des personnes en matière de protection de la vie privée lors de cette étape, nous suivons des procédures qui garantissent notre respect des principes d’Avis et de Consentement du Respect de la vie privée assuré dès la conception.  L’avis a pour but d’indiquer le type d’informations personnelles collectées et d’expliquer dans des termes clairs, précis et univoques la façon dont nous prévoyons d’utiliser ces informations.  Par exemple, lorsque vous envoyez une demande sur abbott.com, les informations personnelles que nous collectons sont utilisées à la seule fin de répondre à la demande.  Le consentement a pour but de fournir aux personnes la possibilité d’accepter la collecte et l’utilisation de leurs informations personnelles.  De manière générale, lorsque nous recherchons un consentement, nous nous assurons qu’il est donné de façon :   * Libre. L’individu n’est jamais obligé ou contraint de donner son consentement. * Éclairée. L’individu a reçu suffisamment d’informations pour prendre une décision raisonnable à laquelle il consent. * Positive. L’individu doit donner son consentement par un acte positif clair. Nous n’obtenons jamais le consentement via le silence d’un individu, ni n’exigeons de l’individu qu’il réalise une action, comme désactiver une case, pour refuser quelque chose. * Révocable. L’individu a reçu des explications claires sur la façon dont il peut révoquer son consentement.   Par exemple, un consommateur qui s’inscrit au programme de fidélité Nutrition Similac© Strong Moms© d’Abbott peut consentir à la collecte et à l’utilisation de ses informations personnelles en acceptant (c.-à-d., en cochant une case) de recevoir des informations promotionnelles supplémentaires.  La gestion est la deuxième étape du cycle de vie des données.  Au cours de cette étape, les informations sont traitées et conservées.  Afin de protéger les informations personnelles lors de cette étape, nous suivons des procédures qui garantissent notre respect des principes suivants :   * intégrité des données, et * accès et correction.   Le principe d’intégrité des données consiste à prendre des mesures raisonnables pour nous assurer que les informations personnelles que nous conservons sont exactes, complètes et à jour.  Nous pouvons par exemple le faire en suivant et en enregistrant toutes les activités qui traitent des informations personnelles. Cela nous permet de nous assurer que nous pouvons identifier la source des données, les finalités spécifiques pour lesquelles les données ont été traitées et où elles sont conservées.  Le principe d’Accès et de correction consiste à accorder aux individus un accès raisonnable à leurs données ainsi que la possibilité de faire valoir leurs droits concernant ces données.  Cela comprend le fait de répondre à la demande d’un individu qui souhaite accéder, supprimer, transférer ou modifier les enregistrements d’informations personnelles que nous conservons.  L’utilisation est la troisième étape du cycle de vie des données.  Au cours de cette étape, les informations personnelles sont utilisées dans le cadre des activités menées dans toute l’organisation.  Afin de protéger les informations personnelles lors de cette étape, nous suivons des procédures qui garantissent notre respect du principe de Divulgation et d’utilisation.  Le principe de Divulgation et d’utilisation consiste à contrôler les personnes qui ont accès aux informations personnelles et à limiter leur utilisation aux finalités spécifiques.  Nous gérons cela via des contrôles d’accès et d’autres procédures. Ces contrôles et procédures limitent l’accès de personnes occupant certains postes et limitent l’utilisation aux finalités spécifiques décrites dans l’avis pour lequel le consentement a été donné.  L’élimination est la dernière étape du cycle de vie des données.  Cela concerne tout ce qui arrive aux données lorsqu’elles ne sont plus activement utilisées. Les activités peuvent inclure la suppression, l’archivage ou la conservation à des fins de conservation légales.  Afin de protéger les informations personnelles lors de cette étape, nous suivons des politiques et des procédures qui garantissent notre respect du principe de Conservation et élimination.  Le principe de Conservation et d’élimination des informations personnelles concerne la conservation des informations personnelles uniquement pour la durée nécessaire à la réalisation des finalités pour lesquelles elles sont nécessaires et traitées.  Lorsque les informations personnelles ne sont plus nécessaires dans un environnement de production active, Abbott a mis en place des procédures pour les archiver ou les éliminer d’une manière conforme aux obligations d’Abbott en matière de gestion, de conservation et d’élimination des données. Nos obligations en matière de conservation et d’élimination sont également soumises aux exigences juridiques des ordonnances de conservation.  Pour en savoir plus sur les obligations en matière de conservation et d’élimination, consultez la Politique mondiale de conservation des dossiers et des informations d’Abbott (I1-02) ou contactez le service Gouvernance des informations et archives. Des détails supplémentaires sont disponibles dans la section Ressources de cette formation.  Cliquez sur l’icône « Ressources » pour en savoir plus et pour consulter les coordonnées.  Comme nous venons de le voir, nos politiques et procédures ont pour objectif de protéger les informations personnelles tout au long de leur cycle de vie.  Nous le garantissons en respectant les principes suivants :   * avis, * consentement, * intégrité des données, * accès et correction, * divulgation et utilisation, et * conservation et élimination.   COLLECTE  Avis  Consentement  GESTION  Intégrité des données  Accès et correction  UTILISATION  Divulgation et utilisation  ÉLIMINATION  Conservation et élimination |
| [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 | Cliquez sur la flèche pour commencer votre examen.  Révision  Prenez le temps d’examiner certains des principaux concepts couverts dans cette section.  Informations personnelles (PI)  Les PI (Personal Information ou Informations personnelles) sont toute information pouvant être utilisée pour   * contacter * localiser ou * identifier une personne.   Informations de santé protégées (PHI)  Les PHI (Protected Health Information ou Informations de santé protégées) correspondent à un type d’informations personnelles particulièrement sensibles utilisées dans le secteur de la santé.  Lois sur la protection de la vie privée  Les lois sur la protection de la vie privée diffèrent d’un pays à l’autre mais regroupent souvent les mêmes principes fondamentaux.  Principes du Respect de la vie privée assuré dès la conception d’Abbott  Les politiques et procédures d’Abbott en matière de protection des données et de la vie privée sont articulées autour d’un ensemble de principes appelé Respect de la vie privée assuré dès la conception.  Avis et consentement  L’avis et le consentement consistent à informer les personnes de la nature des PI collectées et à leur donner la possibilité d’accepter cette collecte.  Intégrité des données  Le principe d’intégrité des données consiste à prendre des mesures raisonnables pour nous assurer que les PI que nous conservons sont exactes, complètes et à jour.  Accès et correction  L’accès et la correction consistent à donner aux personnes le droit d’accéder à leurs données et de les corriger.  Divulgation et utilisation  La divulgation et l’utilisation visent à contrôler qui a accès aux PI.  Conservation et élimination  Le principe de Conservation et d’élimination des PI concerne la conservation des informations personnelles uniquement pour la durée nécessaire à la réalisation des finalités pour lesquelles elles sont nécessaires et traitées.  Pour savoir où vous en êtes, cliquez sur le bouton « Menu »  Bravo !  Vous avez terminé la section 1 sur 4  Cliquez sur la flèche « Suivant » pour continuer la formation |
| [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. | Un autre type de données sensibles que nous pouvons régulièrement utiliser sont les informations commerciales confidentielles.  Les informations commerciales confidentielles désignent une vaste catégorie d’informations. Cela comprend la plupart des informations commerciales que nous utilisons et avec lesquelles nous sommes en contact au quotidien. Les informations confidentielles sont des informations qui ne sont pas accessibles au public et qui pourraient être utiles aux concurrents d’Abbott ou causer du tort à Abbott si elles étaient divulguées. |
| [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 | Responsable marketing  Pouvez-vous me donner des exemples d’informations commerciales confidentielles ?  Les informations commerciales confidentielles peuvent inclure, sans s’y limiter : les designs et processus du produit, les compositions, les organismes, les logiciels, les données de recherche et développement, les données cliniques et pharmacologiques, les données des patients, les données techniques, les listes de clients et de prospection, les pratiques commerciales, les stratégies et plans marketing, les données financières et opérationnelles et les données personnelles.  Elles peuvent également comprendre les informations relatives aux achats, telles que les offres de contrats, les listes de fournisseurs et les informations sur les coûts. |
| [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 | Délégué commercial  Certains types d’informations commerciales confidentielles sont-ils plus sensibles que d’autres ?  Oui. Certains types d’informations commerciales confidentielles nécessitent une plus grande attention, car une divulgation ou une utilisation inappropriées de ces informations peuvent sérieusement nuire à la société.  Parmi les exemples :   * secrets commerciaux, formules de fabrication et processus ; * données cliniques et réglementaires, présentations réglementaires ou informations préalables à l’approbation ; et * données financières qui n’ont pas été communiquées au public. |
| [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. | Comme vous pouvez le voir, la plupart des informations commerciales que nous utilisons dans le cadre de nos activités quotidiennes sont considérées comme confidentielles.  Pour savoir si l’information commerciale que vous utilisez est confidentielle, posez-vous simplement la question suivante :  Cette information est-elle disponible publiquement ?  Si la réponse est non, alors l’information doit être considérée comme confidentielle et des mesures appropriées doivent être prises pour la protéger. |
| [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. | Il est également important de ne pas oublier que toute information commerciale confidentielle créée dans le cadre de vos fonctions chez Abbott appartient à Abbott.  Pour cette raison, vous devez protéger ces informations et ne pas les conserver si votre contrat avec Abbott prend fin. |
| [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. | Il est essentiel de protéger les informations commerciales confidentielles.  Il n’est pas surprenant que l’utilisation ou la divulgation inappropriée de ces informations puisse causer beaucoup de tort à Abbott. |
| [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. | Une utilisation ou divulgation inappropriée d’informations confidentielles peut porter un grave préjudice aux relations d’Abbott avec ses clients et entraîner une couverture médiatique embarrassante ainsi que la perte d’avantages concurrentiels pour Abbott. Elle peut aussi conduire à des poursuites civiles et des sanctions pénales, notamment à l’encontre des employés en poste et des anciens employés.  CLIQUEZ SUR LE BOUTON « DERNIERS CAS » POUR EN SAVOIR PLUS. |
| [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. | DERNIERS CAS  Ces dernières années, plusieurs entreprises se sont vu octroyer d’importants verdicts et indemnités par les jurys à l’encontre de leurs anciens employés qui s’étaient emparés indûment d’informations sur l’entreprise. Par exemple, un employé s’est vu condamné à payer environ 240 millions USD à son ancienne entreprise pour avoir divulgué de façon inappropriée des informations confidentielles de l’entreprise à un concurrent. Un autre ex-employé d’une entreprise et sa nouvelle entreprise ont été contraints de payer une amende de 854 millions USD quand il a été déterminé que l’employé en question s’était approprié des informations confidentielles et les a utilisées au nom du nouvel employeur.  Les études indiquent que le vol d’informations confidentielles a causé des pertes allant de 209 milliards à 625 milliards USD aux entreprises cotées en Bourse. |
| [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. | Il n’est donc pas surprenant que les autorités prennent très au sérieux le vol d’informations confidentielles.  Par exemple, d’après les lois pénales fédérales, un individu encourt jusqu’à 10 ans de prison et une amende de 5 millions USD pour le vol d’informations confidentielles. En outre, toute entreprise reconnue coupable de voler des informations confidentielles encourt jusqu’à 10 millions USD d’amende ou trois fois la valeur des informations confidentielles.  CLIQUEZ SUR LE BOUTON « AMENDES ET SANCTIONS » POUR EN SAVOIR PLUS. |
| [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. | AMENDES ET SANCTIONS  Ces dernières années, plusieurs personnes et entreprises se sont vu imposer des amendes ou des peines de prison pour avoir volé des informations confidentielles. Exemple :   * un concurrent a été condamné à une amende de 60 millions USD pour avoir volé les informations confidentielles d’une autre entreprise ; * un ex-informaticien s’est vu condamné à 97 mois de prison pour avoir volé des informations confidentielles ; * un ex-vendeur a été condamné à 12 mois de prison pour avoir volé des informations confidentielles ; * un cadre supérieur a été condamné à 24 mois de prison pour avoir volé des informations confidentielles ; et * un scientifique a été condamné à 18 mois de prison pour avoir volé des informations confidentielles. |
| [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. | Les *informations privilégiées* sont un autre type d’informations commerciales confidentielles qu’il est important d’identifier et de protéger.  Les informations privilégiées sont des informations importantes privées qui, si elles sont divulguées publiquement, pourraient vraisemblablement avoir une incidence sur la valeur marchande des actions d’une société ou influencer les décisions des investisseurs quant à l’achat ou la vente d’actions. |
| [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. | D’autres exemples d’informations privilégiées comprennent :   * des nouvelles sur une potentielle acquisition, * un retard dans le lancement d’un produit, * des nouvelles sur une violation des systèmes informatiques internes, * des changements imprévus dans les résultats ou les dividendes, * des propositions d’offres ou de fractionnement d’actions, * des informations sur les principaux nouveaux produits, * des attributions de contrat, * des plans d’expansion, * un litige ou une procédure règlementaire importants, etc. |
| [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. | Si vous avez connaissance ou êtes en possession d’informations privilégiées, il est illégal de négocier ou de recommander à d’autres d’effectuer des opérations sur les titres d’Abbott.  Cela concerne également l’achat et la vente de titres d’autres sociétés, y compris les sociétés qui travaillent actuellement avec Abbott ou qui vont le faire.  Pour en savoir plus sur les attentes d’Abbott en ce qui concerne l’utilisation et la protection des informations non publiées, consultez la politique d’Abbott sur le délit d’initié. Des détails supplémentaires sont disponibles dans la section Ressources de cette formation. |
| [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 | Cliquez sur la flèche pour commencer votre examen.  Révision  Prenez le temps d’examiner certains des principaux concepts couverts dans cette section.  Informations commerciales confidentielles  Toute information commerciale qui n’est pas mise à disposition du public doit être traitée comme étant confidentielle. C’est-à-dire presque toutes les informations que nous utilisons dans nos activités courantes.  Mauvaise utilisation des informations commerciales confidentielles  L’utilisation ou la divulgation inappropriée d’informations commerciales confidentielles peut entraîner un grave préjudice pour l’entreprise, ses clients et ses employés.  Information privilégiée  Les informations privilégiées sont des informations importantes privées qui, si elles sont divulguées publiquement, pourraient vraisemblablement avoir une incidence sur la valeur marchande des actions d’une société ou influencer les décisions des investisseurs quant à l’achat ou la vente d’actions.  Pour savoir où vous en êtes, cliquez sur le bouton « Menu »  Bravo !  Vous avez terminé la section 2 sur 4  Cliquez sur la flèche « Suivant » pour continuer la formation |
| [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. | Maintenant que vous comprenez mieux les différents types de données que vous êtes susceptible de rencontrer pendant votre journée de travail, voici ce que vous pouvez faire pour nous aider à les protéger. |
| [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. | Avant d’accéder aux données sensibles, assurez-vous que votre poste et vos responsabilités professionnelles vous obligent à accéder aux données.  Si vous avez des questions relatives à l’accès aux données (en particulier s’il s’agit d’informations personnelles), contactez votre responsable, le Bureau d’éthique et de conformité ou un membre de l’équipe mondiale de protection de la vie privée.  CLIQUEZ SUR LE BOUTON « LE SAVIEZ-VOUS ? » POUR EN SAVOIR PLUS. |
| [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. | LE SAVIEZ-VOUS ?  Abbott effectue différents types de contrôles légitimes afin de réduire le risque d’utilisation inappropriée des données.  Il s’agit notamment de surveiller le téléchargement de données ou l’envoi de données à des adresses électroniques extérieures à Abbott. |
| [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. | Si vous avez l’autorisation d’accéder à des données sensibles, vous devez uniquement les utiliser dans le cadre de la finalité pour laquelle vous avez obtenu un accès.  S’il s’agit d’informations personnelles, utilisez les données uniquement dans le cadre du consentement accordé ou de l’avis fourni. |
| [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. | Avant de partager des données sensibles, assurez-vous que le destinataire possède les autorisations appropriées.  Si vous avez des questions relatives à l’accès aux données, en particulier s’il s’agit d’informations personnelles, contactez votre responsable ou un membre de l’équipe chargée de la confidentialité chez 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. | Demandes venant de votre pays  Si un employé Abbott situé dans le même pays que vous demande des données sensibles, vous devez toujours :   * confirmer l’identité de la personne qui fait la demande ; * confirmer le besoin de la personne d’accéder aux informations ; * vérifier que la personne est autorisée à recevoir les informations ; * vérifier que les informations demandées peuvent être utilisées aux fins pour lesquelles la demande est faite ; et * partager uniquement les quantités d’informations nécessaires pour satisfaire le besoin.   En cas de doute, contactez le Bureau d’éthique et de conformité avant de partager des données sensibles. |
| [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. | Demandes venant d’autres pays  De nombreux pays et régions ont des lois conçues pour protéger les droits de leurs citoyens et imposent des restrictions sur le transfert des informations personnelles au-delà des frontières nationales.  Si vous recevez une demande d’informations contenant des données sensibles de la part d’un collègue d’un autre pays, vérifiez les politiques de confidentialité des données de votre division ou fonction ou contactez le Bureau d’éthique et de conformité avant de poursuivre. Ensuite, suivez les mêmes étapes que pour une demande d’un collègue de votre pays. |
| [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. | Demandes de tiers  Si la demande contenant des données sensibles émane d’un tiers, vérifiez qu’un accord contractuel valable et approprié est en place. En cas de doute, contactez le Bureau d’éthique et de conformité, un membre de l’équipe mondiale de la protection de la vie privée ou le service juridique avant tout partage de données. |
| [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. | Archivez ou éliminez toujours les données sensibles d’une façon conforme aux obligations de gestion, conservation et élimination des données d’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. | Si vous recevez une ordonnance de conservation, il vous est interdit de jeter, supprimer ou détruire toute information couverte par l’ordonnance.  Si vous avez des questions concernant les ordonnances de conservation ou encore la conservation et l’élimination, contactez l’avocat/le juriste dont le nom figure sur l’ordonnance de conservation ou appelez le service des litiges au (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. | Soyez très vigilant(e) concernant les données sensibles lorsqu’un employé quitte Abbott.  Le responsable doit veiller à ce que l’employé qui quitte l’entreprise n’a plus accès aux systèmes (par ex., Workday pour les employés ou Fieldglass pour les travailleurs occasionnels) dès qu’il est informé du départ de l’employé. Cela permet de s’assurer de la bonne gestion des données d’Abbott, de l’accès physique aux bâtiments et du paiement final. |
| [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. | Assurez-vous que l’employé ne part avec aucune donnée sensible. Transférez tous les fichiers à l’employé d’Abbott qui va prendre le poste ou les responsabilités de la personne quittant la société.  Rappelez à l’employé qui quitte la société de ses obligations de ne pas conserver ni divulguer d’informations sensibles. Les employés n’ont pas le droit d’emporter le fruit de leur travail ou tout autre bien d’Abbott (par ex., des appareils mobiles) lorsqu’ils quittent Abbott. Si vous avez des questions sur les procédures locales de départ, contactez les ressources humaines. |
| [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. | Une divulgation accidentelle d’informations de santé protégées est toujours possible.  Par exemple, vous pouvez surprendre la conversation d’un infirmier discutant de l’état de santé d’un patient ou être accidentellement mis(e) en copie d’un e-mail contenant des détails sur le dossier d’un patient. |
| [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. | Afin de gérer correctement toute divulgation accidentelle ou inappropriée d’informations de santé protégées (PHI) d’un patient, signalez immédiatement l’incident au Bureau d’éthique et de conformité ou à un membre de l’équipe mondiale de protection de la vie privée. |
| [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. | Si vous apprenez l’existence d’une divulgation inappropriée ou par inadvertance d’informations commerciales confidentielles, vous devez immédiatement la reporter à la fois :   * à votre supérieur hiérarchique et * au BEC ou un membre de l’équipe mondiale de la protection de la vie privée.   En signalant immédiatement la divulgation, vous aiderez Abbott à récupérer immédiatement les informations et à empêcher un usage inapproprié ou erroné des informations. Si nécessaire, cela permettra à la société d’engager des poursuites civiles ou pénales. |
| [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. | Vous ne devez jamais révéler les données sensibles d’Abbott aux personnes qui n’ont pas l’autorisation de recevoir des données sensibles.  De la même façon, vous devez utiliser les données sensibles d’Abbott au nom d’Abbott et pendant l’exercice de vos fonctions professionnelles au sein d’Abbott.  Toute divulgation accidentelle de données sensibles pourra faire l’objet de mesures disciplinaires pouvant aller jusqu’au licenciement. |
| [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. | Il ne vous est pas permis de partager des données d’Abbott avec un concurrent, pendant et après votre contrat avec Abbott. |
| [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. | Si vous ne restituez pas les données sensibles d’Abbott à Abbott, si vous transmettez des données sensibles vers un appareil, un dispositif de stockage, un compte ou un serveur non approuvé, ou si vous transmettez des données sensibles à une personne ou entité non autorisée à les détenir, Abbott pourra intenter une action en justice à votre encontre.  CLIQUEZ SUR LE BOUTON « ACTION EN JUSTICE » POUR EN SAVOIR PLUS. |
| [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. | ACTION EN JUSTICE  Une action en justice pourrait prendre la forme d’une poursuite au civil envers vous pour :   * vous empêcher de travailler avec un nouvel employeur jusqu’à ce que les données sensibles d’Abbott aient été rendues et protégées ; * vous forcer à rendre tous les appareils électroniques à Abbott qui les examinera et les inspectera ; * vous imposer de payer des dommages et intérêts pour avoir gardé et/ou utilisé de façon inappropriée des données sensibles d’Abbott et pour avoir enfreint les devoirs et obligations que vous devez respecter aux termes de votre contrat de travail avec Abbott ; et * vous obliger à payer les frais de justice d’Abbott pour avoir engagé des poursuites légales pour protéger ses données sensibles.   Si nécessaire, Abbott collaborera avec les autorités locales, nationales et fédérales pour protéger et conserver ses données sensibles. Dans ce cas, vous encourrez aussi des sanctions pénales. |
| [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. | Tout événement susceptible de compromettre la sécurité des informations, notamment la perte ou le vol d’un appareil mobile, doit être immédiatement signalé à votre Service Desk mondial local.  Si vous avez des inquiétudes concernant une éventuelle violation ou si vous voulez signaler un éventuel incident en matière de protection de la vie privée, contactez le service mondial de protection de la vie privée. |
| [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 | Cliquez sur la flèche pour commencer votre examen.  Révision  Prenez le temps d’examiner certains des principaux concepts couverts dans cette section.  Accéder à et utiliser des données sensibles  Vous devez uniquement accéder aux données sensibles et les utiliser dans le cadre de la finalité pour laquelle vous avez obtenu l’accès.  Partager des données sensibles  Avant de partager des données sensibles :   * confirmez l’identité de la personne qui les demande ; * confirmez son besoin d’accéder aux informations ; * vérifiez que les informations peuvent être utilisées aux fins auxquelles elles sont demandées ; et * partagez uniquement les quantités d’informations nécessaires pour satisfaire le besoin.   Conserver et éliminer des informations sensibles  Archivez ou éliminez toujours les données sensibles d’une façon conforme aux obligations de gestion, conservation et élimination des données d’Abbott.  Réagir aux divulgations inappropriées d’informations de santé protégées  Afin de gérer correctement toute divulgation accidentelle ou inappropriée d’informations de santé protégées d’un patient, signalez immédiatement l’incident au Bureau d’éthique et de conformité ou à un membre de l’équipe mondiale de protection de la vie privée.  Signaler un incident de confidentialité  Contactez l’équipe mondiale de protection de la vie privée pour signaler tout éventuel incident de confidentialité.  Pour savoir où vous en êtes, cliquez sur le bouton « Menu »  Bravo !  Vous avez terminé la section 3 sur 4  Cliquez sur la flèche « Suivant » pour continuer la formation |
| [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. | Où obtenir de l’aide  Bureau d’éthique et de conformité (BEC)  Équipe mondiale de la protection de la vie privée – Contactez l’équipe mondiale de la protection de la vie privée par e-mail à l’adresse [privacy@abbott.com](mailto:privacy@abbott.com). Vous trouverez des coordonnées supplémentaires et des informations importantes sur le portail mondial de la confidentialité [ici](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) sur Abbott World.  Personnes du BEC à contacter – N’hésitez pas à contacter le BEC à tout moment pour des questions portant sur l’éthique et la conformité ou pour discuter de préoccupations relatives à de possibles infractions à nos normes, lois ou règlements écrits.   * Rendez-vous sur la page [Contacter le Bureau d’éthique et de conformité](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) sur le [site web du Bureau d’éthique et de conformité](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) sur Abbott World ou écrivez à [OEC@abbott.com](mailto:OEC@abbott.com).   SÉCURITÉ INFORMATIQUE AU SEIN DE L’ENTREPRISE  Consultez le site Sécurité informatique au sein de l’entreprise [ici](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) sur Abbott World.  Consultez le site [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) pour en savoir plus sur les façons sûres de partager des informations.  Division des Affaires juridiques  Contactez [la division des Affaires juridiques](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) en cas de questions ou de préoccupations concernant les obligations contractuelles d’un tiers en matière de protection de la vie privée et des données.  Contactez l’équipe de Gouvernance des informations à l’adresse [information.governance@abbott.com](mailto:information.governance@abbott.com) si vous avez des questions ou des préoccupations concernant les obligations de conservation ou pour obtenir des instructions sur l’utilisation acceptable de solutions technologiques.  POLITIQUES DE RÉFÉRENCE :   * Cliquez [ici](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) pour consulter la Politique relative aux informations confidentielles * Cliquez [ici](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) pour consulter la politique d’Abbott sur le délit d’initié * Cliquez [ici](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) pour consulter la Politique d’utilisation acceptable de la technologie. * Cliquez [ici](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) pour consulter la Politique en matière d’archives et d’informations sur M-Files.   Politiques et procédures du BEC  Pour les politiques et les procédures mondiales et nationales du BEC de notre entreprise en matière d’éthique et de conformité :   * Les employés d’Abbott doivent visiter [iComply](https://icomply.abbott.com/Default.aspx).   Centre de services des ressources humaines   * Cliquez [ici](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) pour consulter la liste des numéros d’assistance des RH.   Ressources sur le cours  Transcription  Cliquez [ici](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) pour afficher la transcription complète de la formation. |
| [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. | Le contrôle des connaissances comprend 10 questions. Vous devez obtenir une note d’au moins 80 % pour réussir ce cours.  Lorsque vous êtes prêt(e), cliquez sur le bouton **«** **Contrôle des connaissances »**. |
| 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? | En supposant que vous travailliez pour Abbott depuis plusieurs années et que vous ayez récemment accepté une offre d’emploi dans une autre entreprise, que seriez-vous légalement autorisé à emporter avec vous au moment du départ ? |
| 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] Les données personnelles de patients provenant d’études cliniques  [2] Les listes des clients d’Abbott et les présentations que vous avez créées quand vous travailliez pour Abbott  [3] Les projections de vente et les données financières de votre Division ou entité commerciale Abbott  [4] Des photos et des souvenirs personnels |
| 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. | La réponse 4 est la bonne. Les informations personnelles, les informations commerciales confidentielles et les Informations de santé protégées sont considérées comme des données sensibles que vous ne pouvez pas emporter lorsque vous quitterez Abbott. En outre, vous devrez restituer les appareils électroniques d’Abbott et autres biens d’Abbott à votre départ.  Pour en savoir plus, consultez la Section 3.4., Réagir aux divulgations inappropriées. |
| 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. | Une responsable marketing travaille au lancement d’un nouveau produit et doit développer un formulaire de consentement pour les clients potentiels. Le formulaire permettra de recueillir et d’utiliser des informations personnelles. Pour être conforme aux pratiques d’Abbott en matière de consentement, lequel des éléments suivants doit être vrai concernant le formulaire de consentement ?  Cochez toutes les réponses qui s’appliquent. |
| 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] Le formulaire ne doit pas inciter les clients à donner leur consentement.  [2] Le formulaire doit expliquer en détail aux clients la manière dont leurs informations personnelles seront utilisées.  [3] Le formulaire doit demander aux clients d’accepter explicitement la collecte et l’utilisation de leurs informations personnelles.  [4] Le formulaire ne doit pas permettre aux clients de retirer leur consentement après l’avoir donné. |
| 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. | Conformément aux pratiques d’Abbott en matière de consentement, le formulaire :   * doit être clair et précis. * ne doit pas inciter les clients à donner leur consentement. * doit expliquer en détail la manière dont les informations personnelles seront utilisées. * doit demander un consentement explicite pour la collecte et l’utilisation des informations personnelles. * doit permettre de retirer son consentement si besoin.   Pour en savoir plus, consultez la Section 1.3, Les principes du Respect de la vie privée assuré dès la conception d’Abbott. |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Abbott gère la divulgation et l’utilisation de données sensibles (par ex., les informations personnelles) de la manière suivante : |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] L’anonymisation de toutes les données.  [2] Les contrôles d’accès.  [3] Réponses 1 et 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. | La divulgation et l’utilisation des données personnelles sont gérées via des contrôles d’accès et autres procédures qui limitent l’accès et l’utilisation aux personnes occupant des fonctions spécifiques et pour les finalités spécifiques décrites dans l’avis faisant l’objet du consentement.  Pour en savoir plus, consultez la Section 1.3, Les principes du Respect de la vie privée assuré dès la conception d’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. | Laquelle des affirmations est vraie concernant la conservation et l’élimination des informations personnelles ?  Cochez toutes les réponses qui s’appliquent. |
| 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] Les informations personnelles sont uniquement conservées pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées et traitées.  [2] Une fois que les données ne sont plus nécessaires dans un environnement de production active, elles doivent toujours être supprimées.  [3] La conservation et l’élimination des informations personnelles sont également soumises aux ordonnances de conservation. |
| 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. | En règle générale, Abbott doit uniquement conserver les informations personnelles pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées et traitées. Lorsque les données ne sont plus nécessaires dans un environnement de production active, elles doivent être archivées ou éliminées d’une manière conforme aux obligations d’Abbott en matière de gestion, de conservation et d’élimination des données. Les obligations en matière de conservation et d’élimination sont également soumises aux conservations à des fins légales.  Pour en savoir plus sur la bonne réponse, consultez la Section 1.3, Principes du Respect de la vie privée assuré dès la conception d’Abbott. |
| 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. | Un ingénieur travaille au développement d’un nouveau produit. Lesquelles des informations suivantes sont considérées comme des informations commerciales confidentielles qui doivent être protégées ?  Cochez toutes les réponses qui s’appliquent. |
| 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] Les projections et prévisions de vente du nouveau produit.  [2] Des données d’informations financières extraites du rapport annuel d’Abbott.  [3] Les informations relatives aux achats, telles que les offres de contrats pour le nouveau produit.  [4] Les informations concurrentielles sur des produits similaires.  [5] Les propositions de fournisseurs tiers liées au nouveau produit. |
| 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. | Les informations commerciales confidentielles désignent une vaste catégorie d’informations. Cela comprend la plupart des informations commerciales que nous utilisons et avec lesquelles nous sommes en contact au quotidien. Pour savoir si une information est confidentielle, posez-vous simplement la question suivante :  Cette information est-elle disponible publiquement ?  Si la réponse est non, l’information est alors très probablement confidentielle et vous devez prendre les mesures appropriées pour la protéger.  Pour en savoir plus, consultez la Section 2.1, Identifier les informations commerciales confidentielles. |
| 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: | Le règlement général sur la protection des données (RGPD) est l’une des lois les plus exhaustives au monde en matière de protection de la vie privée. Mis en œuvre en 2018, le RGPD a établi la norme de protection de la vie privée. Le règlement a été conçu en/au/aux : |
| 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] Asie  [3] Europe  [4] Russie  [5] États-Unis  [6] Amérique Latine |
| 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. | La bonne réponse est en Europe. En Europe, le Règlement général sur la protection des données (RGPD) est l’une des lois les plus exhaustives au monde en matière de protection de la vie privée. Mis en œuvre en 2018, le RGPD a établi la norme de protection de la vie privée que d’autres pays tentent d’imiter.  Pour en savoir plus, consultez la Section 1.2, Obligations légales, réglementaires et contractuelles. |
| 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: | Votre collègue vient de terminer un projet qui impliquait la collecte et l’utilisation de données personnelles. Entre temps, un autre service lui a demandé l’accès à ces données. Vous conseillez à votre collègue de : |
| 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] Confirmer l’identité de la personne qui les demande ainsi que son besoin d’accéder aux informations.  [2] Vérifier que la personne qui les demande est autorisée à recevoir une copie des informations.  [3] S’assurer que les données peuvent être utilisées pour la finalité demandée.  [4] Toutes les réponses ci-dessus. |
| 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. | Le partage inapproprié de données avec des personnes non autorisées est l’une des causes les plus répandues d’incidents concernant les données au sein d’une organisation. Avant de partager un document ou un fichier contenant des données sensibles, vous devez toujours :   * confirmer l’identité de la personne effectuant la demande ainsi que le besoin de la personne d’accéder aux informations ; * vérifier que la personne est autorisée à détenir une copie des informations ; * vérifier que les informations peuvent être utilisées aux fins pour lesquelles la demande est faite ; et * partager uniquement les quantités d’informations nécessaires pour satisfaire le besoin.   Pour en savoir plus, consultez la Section 3.2, Partage des données sensibles. |
| 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? | Vous êtes délégué(e) commercial(e) et rendez visite à une clinique de votre territoire. Alors que vous attendez dans le hall d’accueil, vous oubliez accidentellement des documents sensibles contenant les informations de santé protégées d’un patient. Que faites-vous ? |
| 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] Vous prévenez le délégué à la protection des données de la clinique.  [2] Vous contactez votre supérieur hiérarchique.  [3] Vous signalez l’incident au Bureau d’éthique et de conformité ou à un membre de l’équipe mondiale de la protection de la vie privée. |
| 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. | En réponse à la divulgation par inadvertance des informations de santé protégées d’un patient, vous devez immédiatement signaler l’incident :   * au BEC ou un membre de l’équipe mondiale de la protection de la vie privée.   Pour en savoir plus, consultez la Section 3.4., Réagir aux divulgations inappropriées. |
| 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? | Vous vous rendez au travail en train. Vous oubliez accidentellement votre ordinateur portable contenant des documents de travail sensibles sur votre siège alors que vous descendez du train. Vous vous apercevez de votre erreur en arrivant au bureau. Vous cherchez votre ordinateur portable partout, sans résultat. Que devez-vous faire en premier ? |
| 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] Vous appelez la compagnie de train pour demander si quelqu’un a rapporté votre ordinateur portable.  [2] Vous retournez à la gare pour chercher votre ordinateur portable.  [3] Vous contactez votre Service Desk mondial local. |
| 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. | Si vous pensez que des informations sensibles ont pu être compromises, par exemple en cas de perte ou de vol d’un ordinateur portable, contactez immédiatement votre Service Desk mondial local.  Pour en savoir plus, consultez la Section 3.4, Signaler un incident concernant des données. |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | Vous ne devez utiliser des informations personnelles que dans les cas suivants :  Cochez toutes les réponses qui s’appliquent. |
| 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] Pour la finalité spécifique pour laquelle l’accès vous a été accordé.  [2] Selon l’avis fourni à la personne concernée.  [3] Selon le consentement accordé par la personne concernée. |
| 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. | Si vous avez l’autorisation d’accéder à des informations personnelles, vous ne pouvez les utiliser que dans les cas suivants :   * pour la finalité spécifique pour laquelle l’accès vous a été accordé. * selon l’avis fourni à la personne concernée. * selon le consentement accordé par la personne concernée.   Pour en savoir plus, consultez la Section 3.1, Accès et utilisation de données sensibles. |
| [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 | Toutes les questions restent sans réponse |
| [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. | Aucun résultat n’est disponible, car vous n’avez pas terminé le Contrôle des connaissances.  Félicitations ! Vous avez réussi le contrôle des connaissances et avez terminé le cours.  Veuillez examiner vos résultats présentés ci-dessous en cliquant sur chaque question.  Une fois que vous aurez terminé, vous devrez cliquer sur l’icône **«** **QUITTER [X] »** dans la barre de titre du cours avant de fermer la fenêtre ou l’onglet de votre navigateur.  Désolé, vous n’avez pas réussi le contrôle des connaissances. Prenez quelques minutes pour examiner vos résultats présentés ci-dessous en cliquant sur chaque question.  Lorsque vous aurez terminé, cliquez sur le bouton **« Repasser le contrôle des connaissances »**. |
| 89\_toc\_1 | Introduction | Introduction |
| 90\_toc\_2 | Welcome | Bienvenue |
| 91\_toc\_3 | Objectives | Objectifs |
| 92\_toc\_4 | Menu | Menu |
| 93\_toc\_5 | Personal Information | Informations personnelles |
| 94\_toc\_6 | Recognizing Personal Information | Identifier les informations personnelles |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Obligations légales, réglementaires et contractuelles |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Principes du Respect de la vie privée assuré dès la conception d’Abbott |
| 97\_toc\_9 | Review | Révision |
| 98\_toc\_10 | Confidential Business Information | Informations commerciales confidentielles |
| 99\_toc\_11 | Recognizing Confidential Business Information | Identifier les informations commerciales confidentielles |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Ce que cela coûte de ne pas protéger les informations commerciales confidentielles |
| 101\_toc\_13 | Insider Information | Information privilégiée |
| 102\_toc\_14 | Review | Révision |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Votre rôle dans la protection des données sensibles |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Accéder à et utiliser des données sensibles |
| 105\_toc\_17 | Sharing Sensitive Data | Partager des données sensibles |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Conserver et éliminer des informations sensibles |
| 107\_toc\_19 | Responding to Improper Disclosures | Réagir aux divulgations inappropriées |
| 108\_toc\_20 | Review | Révision |
| 109\_toc\_21 | Knowledge Check | Contrôle des connaissances |
| 110\_toc\_22 | Introduction | Introduction |
| 111\_toc\_23 | Assessment | Évaluation |
| 112\_toc\_24 | Question 1 | Question 1 |
| 113\_toc\_25 | Question 2 | Question 2 |
| 114\_toc\_26 | Question 3 | Question 3 |
| 115\_toc\_27 | Question 4 | Question 4 |
| 116\_toc\_28 | Question 5 | Question 5 |
| 117\_toc\_29 | Question 6 | Question 6 |
| 118\_toc\_30 | Question 7 | Question 7 |
| 119\_toc\_31 | Question 8 | Question 8 |
| 120\_toc\_32 | Question 9 | Question 9 |
| 121\_toc\_33 | Question 10 | Question 10 |
| 122\_toc\_34 | Feedback | Commentaire |
| 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 | Le cours ne peut pas contacter le LMS. Cliquez sur « OK » pour continuer et revoir le cours. Note : une certification pour ce cours n’est peut-être pas disponible. Cliquez sur « Annuler » pour quitter |
| 124\_string\_2 | All questions remain unanswered | Toutes les questions restent sans réponse |
| 125\_string\_3 | Questions | Questions |
| 126\_string\_4 | Question | Question |
| 127\_string\_5 | not answered | pas de réponse |
| 128\_string\_6 | That's correct! | Bonne réponse ! |
| 129\_string\_7 | That's not correct! | Réponse incorrecte. |
| 130\_string\_8 | Feedback: | Commentaire : |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | PROTECTION DES DONNÉES SENSIBLES |
| 132\_string\_10 | Knowledge Check | Contrôle des connaissances |
| 133\_string\_11 | Submit | Envoyer |
| 134\_string\_12 | Retake Knowledge Check | Repasser le Contrôle des connaissances |
| 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. | Description du cours : Chez Abbott, nous utilisons régulièrement des données sensibles pour prendre d’importantes décisions commerciales. Un grand nombre de nos partenaires étant préoccupés par la collecte et l’utilisation de ces données, Abbott a mis en place des politiques et des procédures pour veiller à la protection de ces données. Ce cours explique à quoi correspondent les données sensibles, pourquoi elles sont essentielles pour notre activité et quelles sont les mesures que nous pouvons prendre afin de garantir que nous traitons et gérons ces informations en toute sécurité. Le cours vous prendra environ 30 minutes. |
| 136\_string\_14 | Menu | Menu |
| 137\_string\_15 | Resources | Ressources |
| 138\_string\_16 | Reference Material | Documents de référence |
| 139\_string\_17 | Audio | Audio |
| 140\_string\_18 | Exit | Quitter |
| 141\_string\_19 | Record My Results | Enregistrer mes résultats |