|  |  |  |
| --- | --- | --- |
| 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. | Ochrana citlivých údajů  Začněte kliknutím na šipku dopředu. |
| [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. | Ve společnosti Abbott se při rozhodování spoléháme na data, která často obsahují citlivé informace.  Abychom mohli plnit své poslání pomáhat lidem žít co nejlépe díky dobrému zdraví, je nezbytné, abychom tyto údaje uchovávali v bezpečí a dodržovali zákony a etické normy zastávané společností Abbott. Tento kurz je navržen tak, aby vám poskytl dovednosti potřebné k podpoře tohoto úkolu. |
| [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. | Po absolvování tohoto kurzu budete lépe rozumět následujícímu:   * co jsou citlivé údaje; * jak tyto údaje ve společnosti Abbott chráníme; * jaká je vaše úloha při ochraně citlivých údajů; * co dělat, pokud se domníváte, že citlivé údaje mohly být neoprávněně zveřejněny nebo ohroženy. |
| [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 | Osobní údaje  Dozvíte se, jak se vlády, spotřebitelé i široká veřejnost stále více zabývají otázkami souvisejícími s ochranou a zabezpečením osobních údajů.  12 minut  1. část | Osobní údaje  Rozpoznání osobních údajů  Právní, regulační a smluvní požadavky  Pravidla společnosti Abbott týkající se ochrany soukromí již od návrhu  Shrnutí  2 | Důvěrné obchodní údaje  Zde se dozvíte, že většina obchodních informací, které používáme při našich každodenních pracovních aktivitách, je považována za důvěrné.  5 minut  2. část | Důvěrné obchodní údaje  Rozpoznání důvěrných obchodních údajů  Následky nedostatečné ochrany důvěrných obchodních údajů  Důvěrné interní informace  Shrnutí  3 | Ochrana citlivých údajů  Zde se dozvíte, co můžete dělat, abyste pomohli ochránit citlivé údaje.  8 minut  3. část | Vaše úloha při ochraně citlivých údajů  Přístup k citlivým údajům a jejich používání  Sdílení citlivých údajů  Uchovávání a likvidace citlivých údajů  Reakce na nezákonné zveřejnění údajů  Shrnutí  4 | Prověření získaných znalostí  Zhodnoťte, jak jste pochopili klíčové pojmy a zásady tohoto kurzu.  5 minut  4. část | Prověření získaných znalostí  Hodnocení  Začněte kliknutím na panel.  Začněte kliknutím na žluté tlačítko pro přehrávání.  Tento obsah zatím není dostupný. Musíte vyplnit část {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. | Jedním z běžných typů citlivých údajů, které ve společnosti Abbott používáme, jsou osobní údaje.  V poslední době se vlády, spotřebitelé i široká veřejnost stále více zabývají otázkami souvisejícími s ochranou a zabezpečením osobních údajů. |
| [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. | Osobní údaje jsou jakékoliv informace, které lze přímo či nepřímo použít ke kontaktování, vyhledávání nebo jiné identifikaci osob. |
| [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 | Marketingová manažerka  Můžete mi uvést nějaké příklady osobních údajů?  K osobním údajům mohou patřit biografické informace jako jméno, datum narození, e-mailová adresa a telefonní číslo.  Mohou zahrnovat informace související se vzhledem osob, jako je například barva vlasů nebo hmotnost.  Mohou také zahrnovat informace související se soukromým životem osob, jako jsou fotky, soubory cookie prohlížeče nebo informace o sledování polohy. |
| [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 | Obchodní zástupce  Patří k osobním údajům také chráněné zdravotní informace?  Ano, patří.  Chráněné zdravotní informace (PHI – Protected health information) jsou zvlášť citlivým druhem osobních údajů, které se používají ve zdravotnictví. Patří sem jakékoliv osobně identifikovatelné údaje ve zdravotnických záznamech, včetně diskusí o léčbě mezi zdravotnickými odborníky. |
| [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. | Ve většině zemí, ve kterých společnost Abbott podniká, existují zákony a nařízení, které jsou koncipovány tak, aby chránily osobní údaje, včetně chráněných zdravotních informací.  Zákony týkající se ochrany soukromí a ochrany osobních údajů se liší v závislosti na zemi, ale často zahrnují stejné klíčové principy.  PO KLIKNUTÍ NA ZVÝRAZNĚNÉ OBLASTI NA OBRAZOVCE SE DOZVÍTE O RŮZNÝCH ZÁKONECH A POŽADAVCÍCH NA OCHRANU OSOBNÍCH ÚDAJŮ PLATNÝCH V RŮZNÝCH ČÁSTECH SVĚTA. |
| [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. | Evropa  Obecné nařízení o ochraně osobních údajů (GDPR) je v Evropě jedním z nejkomplexnějších zákonů o ochraně osobních údajů na světě a od svého zavedení v roce 2018 zavedlo standard ochrany osobních údajů, který se snaží napodobit i další země. GDPR se vztahuje na společnosti se sídlem v Evropě, ale i na společnosti nacházející se mimo Evropu, které nabízejí své zboží a služby obyvatelům Evropy nebo sledují chování jakékoliv osoby sídlící v Evropě.  Jedním z klíčových pojmů GDPR je právo na výmaz, známé také jako právo být zapomenut. Toto právo dává jednotlivcům možnost požádat o vymazání svých osobních údajů ze záznamů organizace. Pokud fyzická osoba podá takovou žádost, musí organizace podniknout kroky k vymazání údajů ze svých systémů a zabránit jejich dalšímu použití nebo zpřístupnění. V případě žádostí subjektů údajů mohou existovat výjimky. Společnost Abbott však bude každý potvrzený subjekt údajů informovat o tom, jaká opatření budou přijata v případě každé žádosti. Porušení GDPR může vést k vysokým pokutám pro společnosti, a to až do výše 4 % jejich ročního celosvětového obratu nebo 20 milionů eur (podle toho, která částka je vyšší) v případě nejzávažnějších přestupků. |
| [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. | USA  Ve Spojených státech neexistuje jediný zákon, který by chránil všechny osobní údaje. Místo toho existují zákony a předpisy o ochraně osobních údajů, které se vztahují na konkrétní odvětví a typy údajů. Například zákon o přenositelnosti zdravotního pojištění a o související odpovědnosti chrání soukromí zdravotnických údajů, zatímco zákon Fair Credit Reporting Act chrání úvěrové informace.  Některé státy však začaly přijímat vlastní komplexní zákony o ochraně osobních údajů. Například v Kalifornii platí kalifornský zákon o ochraně soukromí spotřebitelů (California Consumer Privacy Act, CCPA), který Kaliforňanům poskytuje určitá práva na jejich údaje, například právo vědět, jaké osobní údaje jsou o nich shromažďovány, a právo na vymazání všech shromážděných osobních údajů. Zákon CCPA bude v roce 2023 novelizován kalifornským zákonem o právech na soukromí (CPRA), který lidem poskytne ještě větší práva na jejich údaje.  Mezi další státy, které přijaly vlastní zákony o ochraně osobních údajů, patří Virginie, Colorado, Utah a Connecticut. I když se zákony jednotlivých států liší, všechny obecně poskytují lidem práva na jejich údaje a vyžadují, aby společnosti poskytovaly určité informace o svých činnostech zpracování údajů.  Pokuty za porušení státních zákonů o ochraně osobních údajů mohou být značné. Například v Kalifornii může být společnostem uložena pokuta až 7 500 USD za porušení zákona CCPA.  Kanada  V Kanadě existují zákony na federální úrovni i úrovni provincií, jejichž cílem je chránit osobní údaje jednotlivců. Například zákon o ochraně osobních údajů a elektronických dokumentech (Personal Information Protection and Electronic Documents Act, PIPEDA) je federální zákon, který se vztahuje na organizace soukromého sektoru a jehož dodržování prosazuje Úřad kanadského komisaře pro ochranu soukromí.  Na úrovni provincií přijaly Québec, Alberta a Britská Kolumbie zákony o ochraně osobních údajů, které jsou podobné zákonu PIPEDA. Také některé další provincie zavedly pravidla, která poskytují podobnou ochranu osobních údajů, včetně provincií Ontario, Nový Brunšvik, Newfoundland a Labrador a Nové Skotsko, které přijaly zákony o ochraně osobních údajů v oblasti zdravotnictví.  Tyto zákony mají zabránit nesprávnému zacházení s osobními údaji nebo jejich shromažďování bez vědomí jednotlivce a dávají lidem právo na přístup k jejich vlastním informacím a na opravu případných chyb.  Porušení těchto zákonů může vést ke značným pokutám. Například porušení zákona PIPEDA může mít za následek pokutu až 100 000 USD. Zákon o ochraně osobních údajů (Personal Information Protection Act, PIPA) v Albertě umožňuje udělit pokutu až 10 000 dolarů pro jednotlivce a 500 000 dolarů pro organizace. |
| [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. | Asijsko-pacifická oblast  Zákony o ochraně osobních údajů v asijsko-pacifické oblasti se neustále rozšiřují a jsou čím dál komplexnější. Některé země, například Čína, zavedly opatření pro lokalizaci dat, která vyžadují, aby společnosti uchovávaly určité osobní údaje na serverech v rámci svých hranic. Kromě toho má Čína požadavky na posouzení dopadů na soukromí a bezpečnost při přeshraničním předávání osobních údajů.  Jiné země, například Austrálie a Singapur, přijaly přístup k ochraně soukromí více zaměřený na spotřebitele, který dává jednotlivcům větší kontrolu nad jejich údaji, včetně práva vědět, jak je společnosti používají, a možnosti přístupu k nim a jejich případných oprav.  Sankce pro společnosti, které porušují zákony o ochraně osobních údajů, se v jednotlivých regionech také značně liší. Například v Číně mohou být společnosti za porušení zákonů o ochraně osobních údajů pokutovány až do výše 500 000 RMB (přibližně 72 000 USD).  V Singapuru však mohou být společnosti za porušení zákona o ochraně osobních údajů pokutovány až do výše 1 milionu singapurských dolarů (přibližně 737 000 USD). |
| [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. | Rusko  Rusko má také zákony na ochranu údajů svých občanů, včetně zákona o lokalizaci údajů, který vyžaduje, aby společnosti ukládaly osobní údaje ruských občanů na serverech umístěných v Rusku.  Zákon se vztahuje na společnosti, které zpracovávají údaje ruských občanů, bez ohledu na to, zda tyto společnosti sídlí v Rusku, či nikoliv. Zákon by tedy musela dodržovat například společnost se sídlem v USA, která zpracovává údaje ruských občanů.  Stejně jako v mnoha jiných zemích i zde platí, že společnosti musí přijmout opatření na ochranu osobních údajů, které zpracovávají. Společnosti například musí zajistit, aby údaje byly přesné a aktuální, a přijmout opatření, která zabrání nesprávné manipulaci s nimi, ztrátě nebo krádeži.  Pokuty za porušení zákona se mohou pohybovat od 12 000 USD do 72 000 USD za první přestupek a až do 216 000 USD za druhý přestupek. |
| [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. | Latinská Amerika  Ve většině latinskoamerických zemí platí zákony na ochranu soukromí osob. Řada zemí v regionu, například Ekvádor, Argentina a Brazílie, však v nedávné době revidovala své stávající předpisy o ochraně osobních údajů tak, aby odpovídaly mezinárodním standardům.  Ekvádor například nedávno přijal organický zákon o ochraně osobních údajů (LPPD), který vstoupí v platnost v roce 2023. Tento zákon se vztahuje na všechny společnosti na celém světě, které zpracovávají osobní údaje osob v Ekvádoru.  Stejně jako ostatní země v regionu i LPPD vyžaduje, aby společnosti před použitím údajů informovaly jednotlivce a získaly od nich souhlas, aby údaje zničily, pokud již nejsou potřeba, a aby před sdílením údajů s jinými zeměmi splnily určité restrikce. Tato opatření pomáhají chránit soukromí osob v celé Latinské Americe a zajišťují, že společnosti nakládají s osobními údaji zodpovědně.  Porušení LPPD může mít za následek značné pokuty v rozmezí od 3 % do 17 % ročních příjmů organizace za předchozí rok, což pro společnosti znamená silnou motivaci tento zákon dodržovat. |
| [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. | Kromě zákonů a nařízení, kterými se společnost Abbott při podnikání řídí, mohou existovat další povinnosti vyplývající z konkrétních smluv, jež máme se zákazníky.  Zákazníkem společnosti Abbott je například i vláda USA. V rámci smluvních podmínek musíme plnit povinnosti stanovené americkým Zákonem o ochraně soukromí z roku 1974.  ZJISTĚTE VÍCE KLIKNUTÍM NA TLAČÍTKO ZÁKON O OCHRANĚ SOUKROMÍ. |
| [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. | Zákon o ochraně soukromí  Zákon o ochraně soukromí z roku 1974 (5 U.S.C. 552a) je důležitým federálním nařízením. Zřizuje Kodex čestného nakládání s informacemi, který řídí shromažďování, správu, používání a šíření osobně identifikovatelných údajů o osobách, kdy tyto údaje vedou federální agentury v evidenčních systémech. U některých transakcí může být společnosti Abbott udělen přístup k záznamům vládní agentury. V takových případech musí společnost Abbott splnit několik povinností, včetně nutnosti prokázat, že se uskutečnilo školení o ochraně osobně identifikovatelných informací.  Zaměstnanci by se měli před uzavřením jakékoli smlouvy se zákazníky, vůči nimž mají povinnosti ohledně ochrany soukromí, obrátit na právní oddělení. |
| [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. | Zákony, nařízení a smluvní požadavky, které jsme si právě prošli, jsou často složité a mohou se rychle měnit.  Společnost Abbott má zavedené zásady a postupy zajišťující, aby se zaměstnanci těmito zákony a nařízeními řídili. Pokud máte jakékoliv dotazy nebo se chcete dozvědět více, kontaktujte Oddělení pro etiku a dodržování předpisů (OEC) nebo Globální tým pro ochranu soukromí.  Kontakty a další informace získáte kliknutím na ikonu Zdroje. |
| [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 | Shromažďování   * Oznámení * Souhlas   SPRÁVA   * Integrita údajů * Přístup k údajům a možnost jejich opravy   Použití   * Zpřístupnění a používání   Likvidace   * Uchovávání a likvidace   Zásady a postupy společnosti Abbott v oblasti ochrany soukromí a osobních údajů se týkají jednoduché sady pravidel. Říkáme jí Ochrana soukromí již od návrhu.  Tato pravidla slouží jako pomoc zaměstnancům při ochraně citlivých údajů v každé fázi jejich životního cyklu. Pro ilustraci se zaměříme konkrétně na osobní údaje.  První fází životního cyklu údajů je jejich shromáždění.  Během této fáze společnost Abbott využívá řadu metod ke shromáždění osobních údajů. Můžeme například požadovat, aby spotřebitelé uvedli své kontaktní údaje na webových stránkách společnosti Abbott, nebo můžeme zaznamenat osobní údaje generované z některého z našich zařízení.  Abychom dodrželi práva na ochranu soukromí jednotlivců během této fáze, využíváme procesy, které zajišťují, že dodržujeme principy Ochrany soukromí již od návrhu, jako je oznámení a souhlas.  Oznámení znamená, že osoby informujeme o tom, jaké osobní údaje shromažďujeme, a jasně, detailně a jednoznačně vysvětlujeme, jakým způsobem zamýšlíme tyto informace používat.  Když například odesíláte dotaz prostřednictvím stránek abbott.com, využíváme získané osobní údaje výhradně pro účely zodpovězení tohoto dotazu.  Souhlas je pro každého možností, jak vyjádřit svolení se shromažďováním a používáním svých osobních údajů.  Když požadujeme souhlas, obecně ručíme za to, že:   * Musí být poskytnutý dobrovolně. Danou osobu nikdo nepřesvědčuje ani jí neříká, že je souhlas nutností. * Musí být informovaný. Daná osoba má dostatek informací, aby mohla učinit opodstatněné rozhodnutí, k čemu dává souhlas. * Musí být vědomý. Daná osoba musí souhlas poskytnout s plným vědomím. Nikdy za souhlas nepokládáme například mlčení dané osoby ani nevyžadujeme provedení jakékoli akce, jako je například zrušení zaškrtnutí políčka k vyjádření nesouhlasu. * Musí být odvolatelný. Dané osobě je jednoznačně vysvětleno, jak souhlas odvolat.   Například spotřebitel, který se zaregistruje do programu odměn Abbott Nutrition Similac© Strong Moms© Rewards, může schválit shromažďování a používání svých osobních údajů díky souhlasu (například zaškrtnutím políčka) se zasíláním dalších informací o promoakcích.  Druhou fází životního cyklu údajů je jejich správa.  V této fázi jsou informace zpracovávány a uchovávány.  Pro zajištění ochrany osobních údajů během této fáze využíváme procesy, které zajišťují, abychom se řídili následujícími pravidly:   * Integrita údajů. * Přístup k údajům a možnost jejich opravy.   Integrita údajů s sebou nese přijetí odpovídajících opatření, která zajistí, aby byly osobní údaje, které uchováváme, přesné, úplné a aktuální.  Jedním ze způsobů, jak toho dosáhnout, je sledování a zaznamenávání veškerých činností při zpracování osobních údajů. Tím se zajistí, že dokážeme určit zdroj údajů, konkrétní účely, proč jsou údaje zpracovávány, a kde jsou údaje uchovávány.  Přístup k údajům a možnost jejich opravy poskytuje osobám přiměřený přístup ke svým údajům a možnost uplatnit svoje práva, která s nimi souvisejí.  Patří sem odpovídání na žádosti osob o přístup a odstranění, přenos nebo změnu uložených záznamů s osobními údaji.  Třetí fází životního cyklu údajů je jejich využívání.  Během této fáze se osobní údaje používají na podporu aktivit v rámci organizace.  Pro zajištění ochrany osobních údajů během této fáze využíváme procesy, které zajišťují, abychom se řídili pravidly pro zveřejňování a používání osobních údajů.  Zveřejňování a používání je o řízení, kdo má přístup k osobním údajům, a o omezení použití na konkrétní účely.  To zvládáme prostřednictvím kontrol přístupu a dalších procesů. Tyto kontroly a procesy omezují přístup na jednotlivce v konkrétních pracovních funkcích a také omezují použití na konkrétní účely uvedené v oznámení, pro které byl udělen souhlas.  Poslední fází životního cyklu je uspořádání údajů.  Uspořádání údajů uvádí, co se s nimi děje, jakmile se přestanou aktivně používat. Sem může patřit odstranění, archivace nebo uchování údajů za účelem jejich zadržení ze zákona.  Pro zajištění ochrany osobních údajů během této fáze využíváme procesy a zásady, které zajišťují, abychom se řídili pravidly pro uchovávání a likvidaci osobních údajů.  Uchovávání a likvidace osobních údajů se vztahují k uchovávání osobních údajů pouze po dobu nezbytnou pro dosažení účelů, pro které byly tyto údaje nezbytné a zpracovávané.  Jakmile osobní údaje přestanou být zapotřebí v aktivním provozním prostředí, má společnost Abbott funkční procesy pro jejich archivaci nebo likvidaci způsobem, který je v souladu s požadavky na správu, uchovávání a likvidaci. Naše požadavky na uchovávání a likvidaci osobních údajů se také řídí veškerými požadavky na zadržování údajů týkajících se právních záležitostí.  Další informace týkající se požadavků na uchovávání nebo likvidaci naleznete v globálních zásadách společnosti Abbott pro záznamy a informace (l1-02) nebo vám je poskytne oddělení správy informací a záznamů. Podrobnosti lze nalézt v části Zdroje tohoto školení.  Kontakty a další informace získáte kliknutím na ikonu Zdroje.  Jak jsme si právě ukázali, naše zásady a postupy slouží k ochraně osobních údajů během jejich životního cyklu.  Dosahujeme toho dodržováním následujících pravidel pro:   * oznámení, * souhlas, * integritu údajů, * přístup k údajům a možnost jejich opravy, * zveřejnění a používání a * uchovávání a likvidaci.   SHROMAŽĎOVÁNÍ  Oznámení  Souhlas  SPRÁVA  Integrita údajů  Přístup k údajům a možnost jejich opravy  POUŽITÍ  Zveřejnění a používání  LIKVIDACE  Uchovávání a likvidace |
| [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 | Kliknutím na šipku spustíte shrnutí.  Shrnutí  Podívejte se na shrnutí některých klíčových pojmů uvedených v této části.  Osobní údaje (PI)  Osobní údaje jsou jakékoli informace, které lze použít ke   * Kontaktování * Vyhledání * Identifikaci jednotlivce   Chráněné zdravotní informace (PHI)  PHI jsou zvlášť citlivým druhem osobních údajů, které se používají ve zdravotnictví.  Zákony na ochranu soukromí  Zákony na ochranu soukromí se liší v závislosti na zemi, ale často zahrnují stejné klíčové principy.  Pravidla společnosti Abbott týkající se ochrany soukromí již od návrhu  Zásady a postupy společnosti Abbott v oblasti ochrany soukromí a osobních údajů se týkají jednoduché sady pravidel označované jako Ochrana soukromí již od návrhu.  Možnost volby a souhlas  Možnost volby a souhlas je informování jednotlivců o tom, jaké osobní údaje jsou shromažďovány, a poskytnutí možnosti se shromažďováním souhlasit.  Integrita údajů  Integrita údajů spočívá v přijetí přiměřených opatření k zajištění přesnosti, úplnosti a aktuálnosti osobních údajů.  Přístup k údajům a možnost jejich opravy  Přístup k údajům a možnost jejich opravy se týká poskytnutí práva jednotlivcům na přístup k jejich údajům a na jejich opravu.  Zpřístupnění a používání  Zpřístupnění a používání se týká kontroly toho, kdo má přístup k osobním údajům.  Uchovávání a likvidace  Uchovávání a likvidace osobních údajů se vztahují k uchovávání osobních údajů pouze po dobu nezbytnou pro dosažení účelů, pro které byly tyto údaje nezbytné a zpracovávané.  Pokud chcete zkontrolovat svůj pokrok, klikněte na tlačítko Nabídka  Skvělá práce!  Absolvoval/a jste část 1 ze 4  Pokračujte ve studiu kliknutím na šipku vpřed. |
| [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. | Dalším typem citlivých údajů, které můžeme často používat, jsou důvěrné obchodní údaje.  Důvěrné obchodní údaje jsou širokým pojmem. Zahrnují většinu obchodních informací, které používáme a s nimiž denně přicházíme do styku. Důvěrné informace jsou informace, které nejsou veřejně dostupné a které by mohly být užitečné pro konkurenty společnosti Abbott nebo by mohly být v případě vyzrazení pro společnost Abbott škodlivé. |
| [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 | Marketingová manažerka  Můžete mi uvést nějaké příklady důvěrných obchodních údajů?  Důvěrné obchodní údaje mohou mimo jiné zahrnovat: návrhy produktů a postupy týkající se produktů, složení, organismy, počítačový software, údaje týkající se výzkumu a vývoje, klinické a farmakologické údaje, údaje pacientů, technické údaje, seznamy zákazníků a potenciálních zákazníků, obchodní praktiky, marketingové plány a strategie, finanční a provozní data a údaje o personálu.  Mohou sem patřit také údaje o nákupech, jako jsou například výběrová řízení, seznamy zákazníků a informace o cenách. |
| [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 | Obchodní zástupce  Existují nějaké druhy důvěrných obchodních údajů, které jsou citlivější než jiné?  Ano. Některé druhy důvěrných obchodních údajů vyžadují větší pozornost, než je běžné, protože nezákonné zpřístupnění nebo používání těchto údajů může společnosti způsobit vážné škody.  Patří sem například:   * obchodní tajemství, jako jsou výrobní vzorce a postupy; * klinické a regulační údaje, údaje předložené regulačním orgánům nebo údaje předložené před schválením; a * finanční údaje, které zatím nebyly zveřejněny. |
| [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. | Jak vidíte, většina obchodních informací, které používáme při našich každodenních pracovních aktivitách, je považována za důvěrné.  Dobrým způsobem, jak ověřit, zda jsou obchodní informace, které používáte, důvěrné, je položit si jednoduchou otázku:  Jsou tyto informace veřejně dostupné?  Pokud je odpověď záporná, informace by měly být považovány za důvěrné a je nutné podniknout příslušné kroky k zajištění jejich ochrany. |
| [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. | Je také důležité pamatovat na to, že jakékoliv důvěrné obchodní údaje vzniklé či připravené v rámci výkonu vaší pracovní funkce ve společnosti Abbott jsou majetkem společnosti Abbott.  Proto musíte tyto informace chránit a nemůžete si je ponechat, pokud váš pracovní poměr ve společnosti Abbott skončí. |
| [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. | Ochrana důvěrných obchodních údajů je zásadně důležitá.  Proto není překvapením, že nezákonné používání nebo zpřístupnění takových informací může vést ke značné újmě pro společnost 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. | Nezákonné používání nebo zpřístupnění důvěrných údajů může mít značný negativní dopad na vztahy společnosti Abbott se zákazníky a klienty, vést k nepříznivé reakci tisku a médií a může mít za následek ztrátu konkurenčních výhod společnosti Abbott. Může také vést k občanskoprávním žalobám a trestním postihům, a to i proti současným a bývalým zaměstnancům.  DALŠÍ INFORMACE ZÍSKÁTE KLIKNUTÍM NA TLAČÍTKO „NEDÁVNÉ PŘÍPADY“. |
| [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. | NEDÁVNÉ PŘÍPADY  V posledních letech obdržely společnosti vysoké rozsudky a odměny od poroty proti bývalým zaměstnancům za neoprávněné využívání firemních informací. Jedna společnost například obdržela odškodnění v hodnotě 240 milionů USD, protože její bývalý zaměstnanec nepatřičným způsobem zveřejnil důvěrné údaje společnosti ve prospěch konkurence. Jiná společnost obdržela odškodnění ve výši 854 milionů dolarů od bývalého zaměstnance a jeho nového zaměstnavatele. Bývalý zaměstnanec si totiž přisvojil důvěrné údaje společnosti a posléze je použil ve prospěch nového zaměstnavatele.  Studie dokazují, že odcizení důvěrných údajů má pro veřejně obchodovatelné společnosti za následek škody ve výši 209 až 625 miliard USD. |
| [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. | Není žádným překvapením, že úřady berou krádeže důvěrných informací velmi vážně.  Například podle federálního trestního zákona může jednotlivcům za odcizení důvěrných údajů hrozit až deset let odnětí svobody a sankce ve výši až 5 milionů dolarů. Kromě toho společnosti, která je shledána vinnou za odcizení důvěrných údajů, může být uložena pokuta 10 milionů dolarů nebo ve výši odpovídající trojnásobné hodnotě příslušných důvěrných údajů.  DALŠÍ INFORMACE SE DOZVÍTE KLIKNUTÍM NA TLAČÍTKO „POKUTY A POSTIHY“. |
| [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. | POKUTY A POSTIHY  V posledních letech bylo několik osob a společností pokutováno nebo odsouzeno k odnětí svobody za krádež důvěrných informací. Příklad:   * Jednomu konkurentovi byla za odcizení důvěrných údajů jiné společnosti udělena pokuta v hodnotě 60 milionů dolarů; * Bývalý zaměstnanec IT oddělení byl za odcizení důvěrných údajů odsouzen k 97 měsícům odnětí svobody; * Bývalý obchodní zástupce byl za odcizení důvěrných údajů odsouzen k 12 měsícům odnětí svobody; * Člen vedení společnosti byl za odcizení důvěrných údajů odsouzen ke 24 měsícům odnětí svobody; * Výzkumný pracovník byl za odcizení důvěrných údajů odsouzen k 18 měsícům odnětí svobody. |
| [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. | Dalším druhem důvěrných obchodních údajů, které je důležité rozpoznat a chránit, jsou *důvěrné interní informace*.  Důvěrné interní informace jsou jakékoliv neveřejné zásadní údaje, u kterých lze v případě zveřejnění důvodně očekávat, že ovlivní tržní hodnotu akcií společnosti nebo rozhodnutí investorů, zda koupit nebo prodat akcie. |
| [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. | Mezi příklady důvěrných interních informací patří:   * zprávy o případné akvizici, * prodleva při uvedení produktu na trh, * zprávy o narušení vnitřních IT systémů, * neočekávané změny ve výdělcích nebo výši dividend, * předložené nabídky ve výběrových řízeních nebo štěpení akcií, * informace o významných nových produktech, * přidělení kontraktů, * plány na rozšíření, * významné soudní spory nebo řízení vedená ze strany úřadů atd. |
| [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. | Pokud znáte nebo vlastníte důvěrné interní informace, je nezákonné obchodovat s cennými papíry společnosti Abbott nebo doporučovat takové obchodování ostatním.  To platí také pro nákup a prodej cenných papírů jiných firem, včetně těch, které v současné době obchodují nebo u nichž se očekává obchodování se společností Abbott.  Pokud chcete zjistit více o očekáváních společnosti Abbott týkajících se používání a ochrany nezveřejněných informací, podívejte se na její Zásady o zneužívání důvěrných interních informací v obchodním styku. Podrobnosti lze nalézt v části Zdroje tohoto školení. |
| [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 | Kliknutím na šipku spustíte shrnutí.  Shrnutí  Podívejte se na shrnutí některých klíčových pojmů uvedených v této části.  Důvěrné obchodní údaje  Veškeré obchodní informace, které nejsou veřejně dostupné, by měly být považovány za důvěrné. Patří sem většina obchodních informací, které používáme při každodenních pracovních činnostech.  Nesprávné použití důvěrných obchodních údajů  Nesprávné použití nebo vyzrazení důvěrných obchodních údajů může mít za následek značné škody pro společnost, naše zákazníky a zaměstnance.  Důvěrné interní informace  Důvěrné interní informace jsou jakékoliv neveřejné zásadní údaje, u kterých lze v případě zveřejnění důvodně očekávat, že ovlivní tržní hodnotu akcií společnosti nebo rozhodnutí investorů, zda koupit nebo prodat akcie.  Pokud chcete zkontrolovat svůj pokrok, klikněte na tlačítko Nabídka  Skvělá práce!  Absolvoval/a jste část 2 ze 4  Pokračujte ve studiu kliknutím na šipku vpřed. |
| [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. | Teď, když rozumíte různým druhům údajů, s nimiž se pravděpodobně setkáte při své práci, se můžete podívat, jak pomoci chránit citlivé údaje. |
| [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. | Před získáním přístupu k jakýmkoli citlivým údajům se vždy ujistěte, že vám vaše pracovní pozice a odpovědnosti povolují přístup k těmto údajům.  Pokud máte dotaz, zda můžete mít k údajům, zejména pak k osobním údajům, přístup, měli byste se obrátit na Oddělení pro etiku a dodržování předpisů (OEC) nebo na člena globálního týmu pro ochranu soukromí.  DALŠÍ INFORMACE ZÍSKÁTE KLIKNUTÍM NA TLAČÍTKO „VĚDĚLI JSTE, ŽE“. |
| [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. | VĚDĚLI JSTE, ŽE...  Společnost Abbott provádí různé formy zákonného monitorování, aby snížila riziko nezákonného používání údajů.  To zahrnuje sledování stahování dat nebo odesílání údajů na e-mailové adresy, které nejsou od společnosti 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. | Pokud máte oprávnění pro přístup k citlivým údajům, používejte je pouze pro konkrétní účel, pro který vám byl přístup udělen.  Osobní údaje používejte pouze v souladu s uděleným souhlasem nebo poskytnutým oznámením. |
| [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. | Před sdílením citlivých údajů se ujistěte, že osoba, s níž se je chystáte sdílet, má řádné oprávnění.  Pokud máte dotazy, zda můžete s údaji pracovat, zejména pak s osobními údaji, poraďte se se svým manažerem nebo členem týmu pro ochranu soukromí společnosti 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. | Žádosti z vaší vlastní země  Pokud vás zaměstnanec společnosti Abbott, sídlící ve stejné zemi jako vy, požádá o citlivé údaje, vždy postupujte následovně:   * ověřte si totožnost osoby, která zaslala žádost; * ověřte si potřebu přístupu dané osoby k těmto informacím; * ujistěte se, že má daná osoba oprávnění údaje obdržet; * ověřte, že tyto informace lze použít pro účely, pro které jsou požadovány; * sdílejte pouze takové množství informací, které jsou potřeba ke splnění dané potřeby, ne více.   Pokud máte nějaké pochybnosti, kontaktujte před sdílením citlivých dat Oddělení pro etiku a dodržování předpisů (OEC) nebo člena globálního týmu pro ochranu soukromí. |
| [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. | Žádosti z jiných zemí  Mnoho zemí a správních oblastí má zákony navržené tak, aby chránily práva svých občanů, a má zavedená omezení ohledně přenosu osobních údajů přes státní hranice.  Pokud od kolegy z jiné země dostanete žádost o informace obsahující citlivé údaje, než ji začnete vyřizovat, podívejte se do zásad ochrany osobních údajů pro vaši divizi či funkci nebo se poraďte s OEC nebo se členem globálního týmu pro ochranu soukromí. Potom se řiďte stejnými kroky, jako když reagujete na žádost od kolegy z vaší země. |
| [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. | Žádosti od třetích stran  Pokud žádost o citlivé údaje pochází od třetí strany, ujistěte se, že existuje platná a příslušná smluvní dohoda. Pokud máte nějaké pochybnosti, než se rozhodnete cokoliv sdílet, kontaktujte OEC nebo člena právního oddělení. |
| [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. | Citlivé údaje vždy archivujte nebo likvidujte způsobem, který odpovídá požadavkům na správu, uchovávání a likvidaci údajů společnosti 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. | Pokud dostanete příkaz k zadržení údajů ze zákona, nikdy nevyhazujte, neničte ani nemažte žádné informace, na které se vztahuje povinnost zadržení.  Máte-li dotazy týkající se příkazů k zadržení nebo zadržení a likvidace, obraťte se na právníka uvedeného v oznámení o zadržení nebo zavolejte na oddělení soudních sporů na číslo (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. | Vždy věnujte speciální pozornost citlivým údajům, když někdo ze společnosti Abbott odchází.  Manažeři musí ověřit, že každý odcházející zaměstnanec má ukončený pracovní poměr v příslušném systému (např. Workday pro zaměstnance nebo Fieldglass pro pomocné pracovníky) ihned poté, co jsou upozorněni, že zaměstnanec společnost opouští. Tím bude ochráněn přístup k údajům společnosti Abbott, fyzický přístup do budov a bude správně provedena úhrada poslední výplaty. |
| [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. | Zajistěte, aby s odcházejícím zaměstnancem neunikly žádné citlivé údaje. Předejte všechny dokumenty zaměstnanci společnosti Abbott, který přebírá roli nebo odpovědnosti odcházející osoby.  Připomeňte odcházejícímu zaměstnanci povinnost neuchovávat a nezveřejňovat citlivé informace. Zaměstnanci si při odchodu ze společnosti Abbott nesmějí s sebou brát produkty ani žádný jiný majetek společnosti Abbott (např. mobilní zařízení). Máte-li dotazy k místním pravidlům ukončení pracovního poměru, obraťte se na personální oddělení. |
| [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. | K neúmyslnému zpřístupnění chráněných zdravotních informací může dojít kdykoli.  Můžete například zaslechnout zdravotní sestru, jak probírá detaily zdravotního stavu pacienta, nebo vám může být neúmyslně zaslána kopie e-mailu s podrobnostmi o pacientových záznamech. |
| [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. | V reakci na jakékoliv neúmyslné nebo nezákonné zveřejnění chráněných zdravotních informací pacienta (PHI) byste měli incident ihned nahlásit Oddělení pro etiku a dodržování předpisů nebo členovi globálního týmu pro ochranu soukromí. |
| [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. | Dozvíte-li se o nezákonném nebo neúmyslném zpřístupnění důvěrných obchodních údajů, měli byste to ihned nahlásit těmto dvěma subjektům:   * vašemu přímému nadřízenému, a * oddělení pro etiku a dodržování předpisů nebo členovi globálního týmu pro ochranu soukromí.   Nahlásíte-li takové zpřístupnění okamžitě, pomůže to společnosti Abbott příslušné údaje získat zpět, zabránit nezákonnému použití či zneužití údajů a v některých případech také s podáním žaloby v občanskoprávním nebo trestněprávním sporu. |
| [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. | Citlivé údaje společnosti Abbott byste neměli zpřístupnit nikomu, kdo nemá k přístupu k citlivým údajům oprávnění.  Citlivé údaje společnosti Abbott bystě měli používat pouze, když jednáte ve prospěch společnosti Abbott a při plnění pracovních povinností v rámci vaší pracovní pozice ve společnosti Abbott.  Pokud neoprávněně zveřejníte citlivé údaje, můžete čelit disciplinárnímu řízení, a to až do ukončení pracovního poměru. |
| [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. | Není povoleno, abyste během svého pracovního poměru u společnosti Abbott nebo po jeho ukončení údaje společnosti Abbott sdíleli s její konkurencí. |
| [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. | Nenavrátíte-li citlivé údaje zpět společnosti Abbott, přenesete-li citlivé údaje na neschválené zařízení, úložiště, účet nebo server nebo poskytnete-li citlivé údaje jiné osobě či subjektu bez oprávnění přístupu k těmto informacím, může to vést k soudnímu stíhání ze strany společnosti Abbott.  DALŠÍ INFORMACE ZÍSKÁTE KLIKNUTÍM NA TLAČÍTKO „SOUDNÍ STÍHÁNÍ“. |
| [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. | SOUDNÍ STÍHÁNÍ  Soudní stíhání může zahrnovat občanskoprávní žalobu ze strany společnosti Abbott, jejímž následkem by byly následující omezení:   * nebudete moct pracovat pro nového zaměstnavatele, dokud nebudou citlivé údaje společnosti Abbott navráceny a chráněny; * budete požádáni o poskytnutí všech elektronických zařízení ke kontrole a inspekci společností Abbott; * budete muset uhradit finanční odškodnění za nezákonné uchovávání a/nebo používání citlivých údajů společnosti Abbott a porušení povinností, které vůči společnosti Abbott máte, na základě vaší pracovní smlouvy se společností Abbott; * budete muset uhradit právní poplatky, které společnost Abbott vynaložila v souvislosti s podáním žaloby s cílem chránit své citlivé údaje.   Bude-li to nutné, společnost Abbott bude také spolupracovat s místními, státními a federálními úřady s cílem chránit a uchovávat své citlivé údaje. V takové situaci vám mohou hrozit také trestní postihy. |
| [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. | Jakékoliv události zahrnující možné narušení zabezpečení údajů, včetně ztráty nebo krádeže mobilního zařízení, musejí být ihned ohlášeny vaší Globální asistenční službě.  Pokud máte jakékoli pochybnosti o možném porušení nebo chcete nahlásit potenciální incident v oblasti soukromí, kontaktujte globální tým pro ochranu soukromí. |
| [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 | Kliknutím na šipku spustíte shrnutí.  Shrnutí  Podívejte se na shrnutí některých klíčových pojmů uvedených v této části.  Přístup k citlivým údajům a jejich používání  Přistupujte k citlivým údajům a používejte je pouze pro konkrétní účel, pro který vám byl přístup udělen.  Sdílení citlivých údajů  Před sdílením citlivých údajů:   * ověřte totožnost žadatele; * ověřte si potřebu přístupu dané osoby k těmto informacím; * ověřte, že tyto informace lze použít pro účely, pro které jsou požadovány; * sdílejte pouze takové množství informací, které jsou nezbytné ke splnění dané potřeby.   Uchovávání a likvidace citlivých údajů  Citlivé údaje vždy archivujte nebo likvidujte způsobem, který odpovídá požadavkům na správu, uchovávání a likvidaci údajů společnosti Abbott.  Reagování na neúmyslné zpřístupnění PHI  V reakci na jakékoliv nezákonné zpřístupnění chráněných zdravotních informací pacienta byste měli tuto skutečnost ihned nahlásit OEC nebo členovi globálního týmu pro ochranu soukromí.  Hlášení incidentu týkajícího se ochrany osobních údajů  Pokud chcete nahlásit potenciální incident týkající se ochrany osobních údajů, kontaktujte globální tým pro ochranu soukromí.  Pokud chcete zkontrolovat svůj pokrok, klikněte na tlačítko Nabídka  Skvělá práce!  Absolvoval/a jste část 3 ze 4  Pokračujte ve studiu kliknutím na šipku vpřed. |
| [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. | Kde získat pomoc  Oddělení pro etiku a dodržování předpisů (OEC)  Globální tým pro ochranu soukromí – Kontaktujte globální tým pro ochranu soukromí na e-mailu [privacy@abbott.com](mailto:privacy@abbott.com). Doplňující kontaktní údaje a důležité informace o ochraně osobních údajů můžete najít na portálu globálního týmu pro ochranu soukromí [zde](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) na stránkách Abbott World.  Kontakty na oddělení pro etiku a dodržování předpisů (OEC) – s dotazy týkajícími se etiky a dodržování předpisů se neváhejte kdykoli obrátit na oddělení pro etiku a dodržování předpisů; totéž platí v případě, že budete potřebovat probrat pochybnosti o možném porušení našich psaných norem, zákonů či předpisů.   * Navštivte stránku [Kontaktujte OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) na [webu OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) na portálu Abbott World nebo zašlete e-mail na adresu [OEC@abbott.com](mailto:OEC@abbott.com).   FIREMNÍ KYBERNETICKÉ ZABEZPEČENÍ  Navštivte webovou stránku kybernetické bezpečnosti [zde](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) na stránkách Abbott World.  Navštivte web [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx), kde se dozvíte o bezpečných způsobech sdílení informací.  Právní oddělení  Na [právní oddělení](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) se obracejte s otázkami nebo pochybnostmi souvisejícími se smluvními povinnostmi třetích stran, které se týkají ochrany soukromí a dat.  Pokud máte otázky nebo pochybnosti ohledně požadavků na uchovávání nebo pokynů k přijatelnému používání technologických řešení, kontaktujte tým Správy informací na adrese [information.governance@abbott.com](mailto:information.governance@abbott.com).  ODKAZY NA ZÁSADY:   * Pokud se chcete dozvědět něco o Zásadách předávání důvěrných informací, klikněte zde. * Pokud se chcete dozvědět něco o Zásadách společnosti Abbott o zneužívání důvěrných interních informací v obchodním styku, klikněte zde. * Pokud si chcete projít Zásady přijatelného používání technologií, klikněte zde. * Pokud si chcete projít Zásady o záznamech a informacích u souborů M-Files, klikněte zde.   Zásady a postupy OEC  Pokud jde o naše firemní globální a místní zásady a postupy OEC:   * Zaměstnanci společnosti Abbott by měli použít [nástroj iComply](https://icomply.abbott.com/Default.aspx).   Centrum služeb personálního oddělení   * Seznam kontaktních čísel podpory HR najdete kliknutím zde.   Zdroje kurzu  Přepis  Úplný přepis kurzu zobrazíte kliknutím zde. |
| [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. | Kontrola získaných znalostí má 10 otázek. Úspěšné dokončení tohoto kurzu vyžaduje skóre minimálně 80 %.  Až budete připravení, klikněte na tlačítko **Kontrola získaných znalostí**. |
| 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? | Za předpokladu, že jste pro společnost Abbott pracovali několik let a nedávno jste přijali nabídku pracovat pro jinou společnost, které z následujících položek byste si mohli při odchodu legálně vzít s sebou? |
| 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] Osobní údaje pacientů z klinických studií  [2] Seznamy zákazníků společnosti Abbott a informace z prezentace, kterou jste během svého zaměstnání ve společnosti Abbott připravili  [3] Prognózy prodeje a finanční údaje pro vaše oddělení nebo obchodní jednotku ve společnosti Abbott  [4] Osobní fotky a věci na památku |
| 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. | Správná je odpověď číslo 4. Osobní údaje, důvěrné obchodní údaje a chráněné zdravotní informace jsou považovány za citlivé údaje, které si po odchodu ze společnosti Abbott nemůžete vzít s sebou ani je používat. Kromě toho je třeba před odchodem vrátit všechna elektronická zařízení a další majetek společnosti Abbott.  Další informace o správné odpovědi získáte v  oddílu 3.4, Reagování na nezákonné zpřístupnění údajů. |
| 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. | Marketingový manažer pracuje na uvedení nového produktu na trh a musí vytvořit formulář souhlasu pro potenciální zákazníky. Formulář umožní shromažďování a používání osobních údajů. Která z následujících položek musí být pro formulář souhlasu pravdivá, aby byl v souladu s postupy společnosti Abbott pro udělování souhlasu?  Označte všechny platné odpovědi. |
| 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] Formulář nesmí zákazníky nutit k udělení souhlasu.  [2] Formulář musí zákazníkům poskytnout veškeré informace o tom, jak budou jejich osobní údaje použity.  [3] Formulář musí vyžadovat aktivní souhlas zákazníků se shromažďováním a používáním jejich osobních údajů.  [4] Formulář nesmí zákazníkům umožnit odvolání souhlasu, jakmile jej udělili. |
| 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. | Postupy společnosti Abbott pro udělení souhlasu vyžadují, aby formulář:   * byl jasný a přehledný, * netlačil zákazníky, aby dali souhlas, * poskytoval všechny informace o tom, jak se budou osobní údaje používat, * požadoval po lidech, aby aktivně souhlasili se shromažďováním a používáním svých osobních údajů, * umožňoval stažení souhlasu, pokud to bude potřeba.   Další informace o správné odpovědi získáte v  části 1.3, Pravidla společnosti Abbott týkající se ochrany soukromí již od návrhu. |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Zveřejnění a používání citlivých údajů, jako jsou osobní údaje, řídí společnost Abbott prostřednictvím: |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] Deidentifikace všech údajů.  [2] Kontrol přístupů.  [3] Platí 1 i 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. | Zveřejnění a používání osobních údajů se řídí prostřednictvím kontrol přístupů a dalších procesů, které omezují přístup a používání na osoby v konkrétních pracovních funkcích a na konkrétní účely uvedené v oznámení, pro které byl udělen souhlas.  Další informace o správné odpovědi získáte v  části 1.3, Pravidla společnosti Abbott týkající se ochrany soukromí již od návrhu. |
| 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. | Která z následujících možností je pravdivá v souvislosti s uchováváním a likvidací osobních údajů?  Označte všechny platné odpovědi. |
| 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] Osobní údaje jsou uchovávány pouze po dobu nezbytnou pro dosažení účelů, pro které byly shromážděny a zpracovávány.  [2] Jakmile přestanou být osobní údaje zapotřebí v aktivním provozním prostředí, měly by být vždy zlikvidovány.  [3] Uchovávání a likvidace osobních údajů se řídí veškerým zadržováním údajů týkajících se právních záležitostí. |
| 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. | Obecně by společnost Abbott měla uchovávat osobní údaje pouze po dobu nezbytnou pro dosažení účelů, pro které byly shromážděny a zpracovávány. Jakmile přestanou být osobní údaje zapotřebí v aktivním provozním prostředí, měly by být buď archivovány, nebo zlikvidovány způsobem, který je v souladu s požadavky společnosti Abbott na správu, uchovávání a likvidaci. Požadavky na uchovávání a likvidaci se také řídí veškerým zadržováním údajů týkajících se právních záležitostí.  Další informace o správné odpovědi získáte v části 1.3, Pravidla společnosti Abbott týkající se ochrany soukromí již od návrhu. |
| 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. | Inženýr pracuje na vývoji nového produktu. Které z následujících informací jsou považovány za důvěrné obchodní informace, jež musí být zabezpečeny?  Označte všechny platné odpovědi. |
| 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] Plány a prognózy prodeje nového produktu.  [2] Finanční údaje vykazované ve výroční zprávě společnosti Abbott.  [3] Údaje o nákupech, jako jsou například výběrová řízení na smlouvy na nový produkt.  [4] Konkurenční informace o podobných produktech.  [5] Návrhy dodavatelů třetích stran týkající se nového produktu. |
| 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. | Důvěrné obchodní údaje jsou širokým pojmem. Zahrnují většinu obchodních informací, které používáme a s nimiž denně přicházíme do styku. Dobrým způsobem, jak ověřit, zda je něco důvěrného, je položit si jednoduchou otázku:  Jsou tyto informace veřejně dostupné?  Pokud je odpověď záporná, informace jsou téměř určitě důvěrné a vy byste měli podniknout příslušné kroky k zajištění jejich ochrany.  Další informace získáte v části 2.1, Rozpoznání důvěrných obchodních údajů. |
| 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: | Globální nařízení o ochraně osobních údajů (GDPR) je jedním z nejkomplexnějších zákonů o ochraně osobních údajů na světě. Bylo zavedeno v roce 2018 a představuje standard ochrany soukromí. Toto nařízení bylo vydáno v některé z těchto oblastí: |
| Screen 46  Question 6: Options  73\_C\_48 | [1] Canada  [2] Asia  [3] Europe  [4] Russia  [5] United States  [6] Latin America | [1] Kanada  [2] Asie  [3] Evropa  [4] Rusko  [5] USA  [6] Latinská Amerika |
| Screen 46  Question 6: Feedback  74\_C\_48 | The correct answer is Europe. In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate.  For more information, see Section 1.2, Legal, Regulatory and Contractual Agreements. | Správná odpověď je Evropa. Obecné nařízení o ochraně osobních údajů (GDPR) je v Evropě jedním z nejkomplexnějších zákonů o ochraně osobních údajů na světě a od svého zavedení v roce 2018 zavedlo standard ochrany osobních údajů, který se snaží napodobit i další země.  Další informace naleznete v části 1.2, Právní, regulační a smluvní dohody. |
| 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: | Váš kolega právě dokončil projekt, který zahrnoval shromažďování a používání osobních údajů. Od té doby obdržel žádost o přístup k těmto údajům od jiného oddělení. Poradíte svému kolegovi, aby: |
| 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] Ověřil totožnost osoby, která zaslala žádost, a její potřebu přístupu k těmto informacím.  [2] Ověřil, zda je žadatel oprávněn získat kopii informací.  [3] Ujistil se, že údaje lze použít pro požadované účely.  [4] Vše výše uvedené. |
| 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. | Jednou z nejběžnějších příčin incidentů s údaji v rámci organizace je nevhodné sdílení dat s neoprávněnými osobami. Před sdílením jakéhokoli dokumentu nebo souboru obsahujícího citlivé údaje vždy dbejte na následující:   * Ověřte si totožnost osoby, která zaslala žádost, a její potřebu přístupu k těmto informacím. * Ujistěte se, že má daná osoba oprávnění pořídit si kopii údajů. * Zkontrolujte, že tyto informace lze použít pro účely, pro které je požaduje. * Sdílejte pouze takové množství informací, které jsou potřeba ke splnění dané potřeby, ne více.   Další informace získáte v části 3.2, Sdílení citlivých údajů. |
| 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? | Jste obchodní zástupce, který navštěvuje kliniku ve vaší oblasti. Při čekání v recepci omylem ztratíte citlivé dokumenty obsahující chráněné zdravotní informace pacienta. Jak se zachováte? |
| 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] Informujete pracovníka kliniky odpovědného za ochranu osobních údajů.  [2] Obrátíte se na svého nadřízeného.  [3] Nahlásíte incident OEC nebo členovi globálního týmu pro ochranu soukromí. |
| 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. | V reakci na jakékoliv neúmyslné zveřejnění chráněných zdravotních informací pacienta (PHI) byste měli případ ihned nahlásit těmto subjektům:   * Oddělení pro etiku a dodržování předpisů nebo členovi globálního týmu pro ochranu soukromí.   Další informace o správné odpovědi získáte v  oddílu 3.4, Reakce na nezákonné zpřístupnění údajů. |
| 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? | Při cestě do práce ve vlaku omylem necháte notebook s citlivými pracovními dokumenty na sedadle a vystoupíte z vlaku. Svou chybu si uvědomíte, až když dorazíte do kanceláře a horečně hledáte svůj notebook, ale nikde není k nalezení. Co byste měli udělat jako první? |
| 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] Zavolat do železniční společnosti a zeptat se, zda někdo neodevzdal váš notebook.  [2] Vrátit se na nádraží a hledat notebook.  [3] Kontaktovat vaši místní Globální asistenční službu. |
| 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. | Pokud se domníváte, že mohlo dojít k ohrožení citlivých informací, například v důsledku ztráty nebo krádeže notebooku, neprodleně kontaktujte místní Globální asistenční službu.  Další informace naleznete v části 3.4, Nahlášení incidentu s údaji. |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | Měli byste výhradně používat osobní údaje:  Označte všechny platné odpovědi. |
| 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] Pro konkrétní účel, pro který vám byl přístup udělen.  [2] Podle oznámení poskytnutého subjektu údajů.  [3] Podle souhlasu uděleného subjektem údajů. |
| 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. | Pokud máte povolení k přístupu k osobním údajům, používejte je pouze:   * Pro konkrétní účel, pro který vám byl přístup udělen. * Podle oznámení poskytnutého subjektu údajů. * Podle souhlasu uděleného subjektem údajů.   Další informace naleznete v části 3.1 Přístup k citlivým údajům a jejich používání. |
| [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 | Všechny otázky zůstaly bez odpovědi. |
| [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. | Nejsou k dispozici žádné výsledky, protože jste nedokončili kontrolu získaných znalostí.  Blahopřejeme! Úspěšně jste absolvovali ověření získaných znalostí a dokončili kurz.  Níže si prosím zkontrolujte své výsledky kliknutím na jednotlivé otázky.  Po dokončení kurzu musíte kliknout na ikonu **KONEC [X]** na liště nadpisů kurzu a teprve potom zavřít okno prohlížeče.  Je nám líto, v ověření získaných znalostí jste neuspěli. Věnujte pár minut překontrolování výsledků kliknutím na jednotlivé otázky.  Po dokončení klikněte na tlačítko **Znovu zkusit kontrolu získaných znalostí**. |
| 89\_toc\_1 | Introduction | Úvod |
| 90\_toc\_2 | Welcome | Vítejte |
| 91\_toc\_3 | Objectives | Cíle |
| 92\_toc\_4 | Menu | Nabídka |
| 93\_toc\_5 | Personal Information | Osobní údaje |
| 94\_toc\_6 | Recognizing Personal Information | Rozpoznání osobních údajů |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Právní, regulační a smluvní požadavky |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Pravidla společnosti Abbott týkající se ochrany soukromí již od návrhu |
| 97\_toc\_9 | Review | Shrnutí |
| 98\_toc\_10 | Confidential Business Information | Důvěrné obchodní údaje |
| 99\_toc\_11 | Recognizing Confidential Business Information | Rozpoznání důvěrných obchodních údajů |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Následky nedostatečné ochrany důvěrných obchodních údajů |
| 101\_toc\_13 | Insider Information | Důvěrné interní informace |
| 102\_toc\_14 | Review | Shrnutí |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Vaše úloha při ochraně citlivých údajů |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Přístup k citlivým údajům a jejich používání |
| 105\_toc\_17 | Sharing Sensitive Data | Sdílení citlivých údajů |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Uchovávání a likvidace citlivých údajů |
| 107\_toc\_19 | Responding to Improper Disclosures | Reakce na nezákonné zveřejnění údajů |
| 108\_toc\_20 | Review | Shrnutí |
| 109\_toc\_21 | Knowledge Check | Prověření získaných znalostí |
| 110\_toc\_22 | Introduction | Úvod |
| 111\_toc\_23 | Assessment | Hodnocení |
| 112\_toc\_24 | Question 1 | Otázka 1 |
| 113\_toc\_25 | Question 2 | Otázka 2 |
| 114\_toc\_26 | Question 3 | Otázka 3 |
| 115\_toc\_27 | Question 4 | Otázka 4 |
| 116\_toc\_28 | Question 5 | Otázka 5 |
| 117\_toc\_29 | Question 6 | Otázka 6 |
| 118\_toc\_30 | Question 7 | Otázka 7 |
| 119\_toc\_31 | Question 8 | Otázka 8 |
| 120\_toc\_32 | Question 9 | Otázka 9 |
| 121\_toc\_33 | Question 10 | Otázka 10 |
| 122\_toc\_34 | Feedback | Zpětná vazba |
| 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 | Kurz nemůže kontaktovat LMS. Pokračujte kliknutím na tlačítko OK a projděte si kurz. Certifikace kurzu nemusí být k dispozici. Kurz ukončete kliknutím na tlačítko Konec. |
| 124\_string\_2 | All questions remain unanswered | Všechny otázky zůstaly bez odpovědi. |
| 125\_string\_3 | Questions | Otázky |
| 126\_string\_4 | Question | Otázka |
| 127\_string\_5 | not answered | bez odpovědi |
| 128\_string\_6 | That's correct! | To je správně! |
| 129\_string\_7 | That's not correct! | To není správně! |
| 130\_string\_8 | Feedback: | Zpětná vazba: |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | OCHRANA CITLIVÝCH ÚDAJŮ |
| 132\_string\_10 | Knowledge Check | Prověření získaných znalostí |
| 133\_string\_11 | Submit | Odeslat |
| 134\_string\_12 | Retake Knowledge Check | Znovu zkusit ověření získaných znalostí |
| 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. | Popis kurzu: Ve společnosti Abbott často používáme citlivé údaje pro důležitá obchodní rozhodnutí. Vzhledem k tomu, že má většina našich zainteresovaných subjektů obavy, jak jsou tyto údaje shromažďovány a používány, společnost Abbott zavedla zásady a postupy pro zajištění, že jsou tyto údaje chráněné. Tento kurz vysvětluje, co jsou to citlivé údaje, proč jsou zásadně důležité pro naše podnikání, a jaké kroky můžeme podniknout, abychom zajistili, že tyto údaje zpracováváme bezpečně, nakládáme s nimi bezpečně a že jsou zabezpečené. Kurz vám zabere přibližně 30 minut. |
| 136\_string\_14 | Menu | Nabídka |
| 137\_string\_15 | Resources | Zdroje |
| 138\_string\_16 | Reference Material | Referenční materiály |
| 139\_string\_17 | Audio | Audio |
| 140\_string\_18 | Exit | Konec |
| 141\_string\_19 | Record My Results | Nahrát moje výsledky |