|  |  |  |
| --- | --- | --- |
| 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. | Захист конфіденційних даних  Натисніть стрілку вперед, щоб розпочати навчання. |
| [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. | У компанії Abbott ми приймаємо рішення на основі даних. У багатьох випадках вони мають у своєму складі конфіденційну інформацію.  Для реалізації нашої місії «допомагати людям жити найкращим життям завдяки міцному здоров’ю» нам вкрай важливо зберігати ці дані в таємниці, виконувати вимоги законів та діяти відповідно до етичних норм, що їх підтримує компанія Abbott. Цей курс створений для того, щоб ви набули навичок, необхідних для виконання цього завдання. |
| [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. | Після опанування цього курсу вам стане зрозумілішим:   * що таке конфіденційні дані, * яким чином ми захищаємо ці дані в компанії Abbott, * ваша роль у захисті конфіденційних даних і * що робити, якщо ви вважаєте, що конфіденційні дані могли бути розкриті або стати відомими не у встановленому порядку. |
| [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 | Персональні дані  У цьому розділі ви дізнаєтеся, що уряди, споживачі та широка громадськість дедалі більше турбуються про конфіденційність і безпеку персональних даних.  12 хвилин  Розділ 1 | Персональні дані  Визнання персональних даних  Правові, нормативні та договірні вимоги  Принципи спроектованої конфіденційності Abbott  Повторення  2 | Конфіденційна ділова інформація  У цьому розділі ви дізнаєтеся, що більшість ділової інформації, яку ми використовуємо у своїй щоденній роботі, вважається конфіденційною.  5 хвилин  Розділ 2 | Конфіденційна ділова інформація  Визнання конфіденційної ділової інформації  Наслідки незабезпечення захисту конфіденційної ділової інформації  Інсайдерська інформація  Повторення  3 | Захист конфіденційних даних  У цьому розділі ви дізнаєтеся, що ви можете зробити, щоб захистити конфіденційні дані.  8 хвилин  Розділ 3 | Ваша роль у захисті конфіденційних даних  Доступ та використання конфіденційних даних  Обмін конфіденційними даними  Зберігання та видалення конфіденційних даних  Реагування на неналежне розкриття  Повторення  4 | Перевірка знань  Оцініть свої знання головних концепцій і принципів цього курсу.  5 хвилин  Розділ 4 | Перевірка знань  Оцінка  Натисніть на панель, щоб запустити навчання.  Натисніть кнопку програвання жовтого кольору, щоб почати.  Ця інформація поки що недоступна. Ви повинні завершити вивчення розділу {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. | В Abbott одним із найбільш розповсюджених типів конфіденційних даних, які ми використовуємо, є персональні дані.  Протягом декількох останніх років споживачі та широка громадськість дедалі більше турбуються про конфіденційність та безпеку персональних даних. |
| [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. | Персональні дані — це будь-яка інформація, яку можна використати для встановлення контакту, визначення місцезнаходження або іншим чином ідентифікувати особу. |
| [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. | Кендіс | Менеджер із маркетингу  Ви можете навести кілька прикладів персональних даних?  Персональні дані можуть включати біографічну інформацію, таку як ім’я, дату народження, адресу електронної пошти та номер телефону.  Вони можуть включати інформацію, що стосується зовнішнього вигляду людини, наприклад колір волосся або вага.  Вони також можуть включати інформацію, що стосується особистого життя людини, наприклад, фотографії, файли cookie браузера або інформація про відстеження місцезнаходження. |
| [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. | Джеррі | Торговий представник  Чи включають персональні дані також закриту медичну інформацію?  Так, включають.  Закрита медична інформація є особливим конфіденційним видом персональних даних, що використовується у галузі охорони здоров’я. Вона включає будь-яку інформацію, що дозволяє встановити особу, в медичній документації, включно з розмовами медичних працівників про лікування. |
| [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. | У більшості країн, в яких працює компанія Abbott, є закони та нормативно-правові акти, розроблені для захисту персональних даних, включно із закритою медичною інформацією.  Закони, які стосуються приватного життя та захисту персональних даних, відрізняються залежно від країни, але часто охоплюють одні й ті самі основні принципи.  НАТИСНІТЬ НА КОЖНЕ З ВІДМІЧЕНИХ ПОЛІВ НА ЕКРАНІ, ЩОБ ДІЗНАТИСЯ ПРО РІЗНІ ВИДИ ЗАКОНІВ ПРО НЕДОТОРКАНІСТЬ ПРИВАТНОГО ЖИТТЯ ТА ВИМОГИ, ЯКІ ЗАСТОСОВУЮТЬСЯ У СВІТІ. |
| [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. | Європа  На території Європи одним із найбільш вичерпних законодавчих актів для всіх країн-учасниць є Загальний регламент про захист даних (GDPR). Після його запровадження в 2018 році він править за взірець у сфері захисту даних, який прагнуть наслідувати інші країни. GDPR застосовується не лише до організацій, які розташовані в Європі, він також застосовується до організацій, розташованих за межами Європи, якщо вони пропонують товари й послуги будь-яким фізичним особам, що проживають в Європі, або здійснюють моніторинг їхньої поведінки.  Однією з основних концепцій GDPR є право на стирання, інша назва — «право бути забутим». Це право надає можливість фізичним особам подати запит на видалення їхніх персональних даних із документації організації. Якщо особа подає такий запит, організація має вжити відповідних заходів, щоб видалити дані зі своїх систем і запобігти їхньому подальшому використанню або розкриттю. Для запитів суб’єктів даних можуть бути передбачені винятки. У будь-якому разі Abbott повідомлятиме кожному затвердженому суб’єкту даних, яких заходів було вжито по кожному запиту. За порушення GDPR із компаній стягуються великі штрафи в розмірі до 4 % від їхнього загального річного обороту по всьому світу або в сумі до 20 мільйонів євро (залежно від того, яка сума є більшою) за найтяжчі порушення. |
| [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. | США  У США немає єдиного закону, що регламентує захист усіх персональних даних. Натомість там є законодавчі та нормативно-правові акти про забезпечення конфіденційності, що застосовуються до окремих галузей і типів даних. Так, HIPAA захищає конфіденційність і безпеку даних у сфері охорони здоров’я, закон про надання точної інформації про кредиторів захищає кредитну інформацію.  Водночас деякі штати починають вводити в дію власні універсальні закони про захист конфіденційних даних. Наприклад, закон штату Каліфорнія про захист персональних даних споживачів (CCPA) дає мешканцям штату певні права на їхні дані, зокрема право знати, які персональні дані збираються про них, і право видалити будь-які зібрані персональні дані. У 2023 році в закон CCPA будуть внесені зміни законом штату Каліфорнія про захист прав щодо персональних даних (CPRA), який дасть людям навіть іще ширші права на їхні дані.  Окремі закони про захист персональних даних прийняли також у штатах Вірджинія, Колорадо, Юта та Коннектикут. Хоча закони в кожному штаті є неоднаковими, всі вони в цілому надають людям права щодо їхніх персональних даних і зобов’язують компанії розкривати певні відомості про свою діяльність з опрацювання їхніх даних.  Порушення законів штатів про захист персональних даних карається штрафом, розмір якого може бути доволі значним. Наприклад, у Каліфорнії за порушення CCPA компанію можуть оштрафувати на суму до 7500 доларів США.  Канада  Для захисту персональних даних фізичних осіб у Канаді діють закони федерального рівня та рівня провінцій. Так, федеральний закон про захист персональних даних і електронні документи (PIPEDA) застосовується до організацій приватного сектору, його виконання забезпечується офісом уповноваженого з питань захисту персональних даних у Канаді.  На рівні провінцій закони про захист персональних даних, подібні до PIPEDA, введено в дію у Квебеку, Альберті та Британській Колумбії. У деяких інших провінціях також діють правила, що забезпечують подібний захист персональних даних, зокрема в провінціях Онтаріо, Нью-Брансвік, Ньюфаундленд і Лабрадор, а також у Новій Шотландії, де введено в дію закони про захист персональної інформації про здоров’я.  Ці закони дозволяють запобігти порушенням під час опрацювання або збиранню персональних даних без відома фізичної особи і надають людям право доступу до їхньої інформації та виправлення помилок у ній.  Порушення цих законів може призвести до стягнення великих штрафів. Наприклад, порушнику PIPEDA може загрожувати штраф у сумі до 100 000 доларів. У провінції Альберта законом про захист персональних даних (PIPA) встановлено граничний розмір штрафів 10 000 доларів для фізичних осіб і 500 000 доларів для організацій. |
| [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. | Азійсько-Тихоокеанський регіон  Законодавство про захист персональних даних в Азійсько-Тихоокеанському регіоні постійно розвивається і стає дедалі ширшим. Деякі країни, як-от Китай, запровадили заходи з локалізації даних, які зобов’язують компанії зберігати деякі персональні дані на серверах, що знаходяться на території цих країн. До того ж у Китаї є вимоги для транскордонної передачі персональних даних стосовно оцінки впливу на конфіденційність і безпеку.  Інші країни, зокрема Австралія та Сінгапур, у питаннях конфіденційності більшою мірою зорієнтовані на споживача, завдяки чому люди можуть краще контролювати дані про себе: вони мають право знати, як саме компанії використовують їх, і мають можливість доступу до таких даних і виправлення їх у разі потреби.  Штрафи для компаній за порушення законів про захист персональних даних також будуть різними залежно від регіону. Так, у Китаї компаніям-порушницям законів про захист персональних даних може загрожувати штраф у сумі до 500 000 китайських юанів (приблизно 72 000 доларів США).  А от у Сінгапурі штраф за порушення закону країни про захист персональних даних може сягати 1 мільйона (сінгапурських) доларів (приблизно 737 000 доларів США). |
| [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. | Росія  У Росії також є закони, що стоять на захисті персональних даних її громадян, включаючи закон про локалізацію персональних даних, за яким компанії зобов’язані зберігати персональні дані росіян на серверах, що знаходяться в Росії.  Закон стосується компаній, що опрацьовують персональні дані росіян, незалежно від того, чи здійснюють такі компанії діяльність у РФ. Наприклад, якщо компанія, що здійснює діяльність у США, опрацьовує персональні дані росіян, їй необхідно буде дотримуватися цього закону.  Як і в багатьох інших країнах, закон також зобов’язує компанії вживати заходів для захисту опрацьовуваних ними персональних даних. Наприклад, компанії повинні забезпечувати точність і актуальність персональних даних, а також вживати заходів для запобігання їхньому неналежному опрацюванню, втраті або викраденню.  Штрафи за порушення закону можуть сягати 12 000–72 000 доларів США за перше порушення та 216 000 доларів США за повторне порушення. |
| [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. | Латиноамериканський регіон  У більшості країн Латинської Америки діють закони, які захищають право людини на недоторканність приватного життя. При цьому в багатьох країнах регіону, зокрема в Еквадорі, Аргентині та Бразилії, існуючі нормативні положення про права на недоторканність приватного життя були останнім часом переглянуті з метою забезпечення відповідності міжнародним стандартам.  Так, в Еквадорі нещодавно був прийнятий основний закон про захист персональних даних (LPPD), що набуде чинності в 2023 році. Цей закон стосується всіх компаній світу, що опрацьовують персональні дані еквадорців.  Як і в багатьох інших країнах регіону, закон LPPD зобов’язує компанії надавати повідомлення фізичним особам і отримувати від них згоду на використання їхніх даних, знищувати дані, коли вони стають непотрібними, і дотримуватися певних обмежень при передаванні даних в інші країни. Такі заходи дозволяють захистити персональні дані жителів латиноамериканського континенту і забезпечують відповідальне опрацювання персональних даних компаніями.  Порушення LPPD може призвести до стягнення великих штрафів у розмірі від 3 до 17 % від річного доходу організації за попередній рік, що неабияк стимулюватиме компанії дотримуватись закону. |
| [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. | На додаток до законів та нормативних актів, що регулюють порядок ведення бізнесу компанією Abbott, окремі контракти, укладені з клієнтами, можуть містити додаткові зобов’язання.  Наприклад, уряд США є клієнтом компанії Abbott. Відповідно до умов такої угоди, ми маємо виконувати зобов’язання, встановлені Законом США «Про конфіденційність» від 1974 року.  НАТИСНІТЬ КНОПКУ «ЗАКОН ПРО КОНФІДЕНЦІЙНІСТЬ», ЩОБ ОЗНАЙОМИТИСЯ З ДОДАТКОВОЮ ІНФОРМАЦІЄЮ. |
| [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. | Закон «Про конфіденційність»  Закон «Про конфіденційність» від 1974 року (5 USC 552a) є важливим федеральним законом. Він встановлює Кодекс добросовісної інформаційної практики, який регулює збір, зберігання, використання та розповсюдження інформації, що ідентифікує особу, про осіб, зазначених у системах федеральних органів. Для здійснення певних транзакцій компанії Abbott може бути наданий доступ до записів урядових установ. У таких випадках компанія Abbott має виконати кілька зобов’язань, включно з вимогою продемонструвати факт проведення тренінгу з питань захисту персональних даних.  Співробітники мають зв’язатися з юридичним відділом перш ніж укладати будь-які угоди з клієнтами, які передбачають зобов’язання щодо зберігання конфіденційності. |
| [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. | Вимоги законів, нормативних актів та контрактів, які ми щойно розглянули, часто є складними та можуть швидко змінюватися.  Компанія Abbott розробила політики та процедури, що забезпечують дотримання працівниками цих законів та норм. Якщо у вас є запитання або ви хочете дізнатись більше, зв’яжіться з ДЕДВ або представником підрозділу ДЕДВ із захисту персональних даних.  Для того щоб переглянути контактні дані та додаткову інформацію, натисніть позначку «Ресурси». |
| [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 | Отримання   * Повідомлення * Згода   УПРАВЛІННЯ   * Цілісність даних * Доступ та виправлення   Використання   * Розкриття та використання   Розпорядження   * ЗБЕРІГАННЯ ТА РОЗПОРЯДЖЕННЯ   Політики та процедури забезпечення конфіденційності та захисту даних компанії Abbott організовані за простим набором принципів. Ми називаємо ці принципи «Спроектована конфіденційність».  Ці принципи розроблені, щоб допомогти працівникам захистити конфіденційні дані на кожному етапі життєвого циклу даних. Для ілюстрації розгляньмо конкретно персональні дані.  Першим етапом життєвого циклу даних є збір.  На цьому етапі Abbott використовує різноманітні методи збору персональних даних. Наприклад, ми можемо просити споживачів надати контактні дані на вебсайті Abbott або можемо зібрати персональні дані, створені одним із наших пристроїв.  З метою захисту прав фізичних осіб на забезпечення конфіденційності даних на цьому етапі ми підтримуємо процеси із забезпечення конфіденційності за принципами «Спроектована конфіденційність» та «Повідомлення» та «Згода».  Повідомлення означає повідомити людей про те, які персональні дані збираються, а також чітко та просто пояснити, як ми плануємо використовувати ці дані.  Наприклад, під час надсилання запиту на сайт abbott.com персональні дані, які ми збираємо, використовуються лише для надання відповіді на запит.  Згода передбачає надання відповідним особам змоги погодитись на збір та використання їхніх персональних даних.  Зазвичай коли ми запитуємо згоду, ми маємо забезпечити, щоб вона була:   * Надана добровільно. Відповідну особу не примушують і не кажуть, що згода є вимогою для подальшої діяльності. * Інформованою. Відповідній особі надається достатня інформація для прийняття обґрунтованого рішення, на яке вона погоджується. * Ствердною. Відповідна особа має надати згоду ствердно. Ми ніколи не приймаємо згоду без прямого підтвердження, наприклад, не сприймаємо мовчання в якості згоди, а також не вимагаємо від особи вчинити певні дії, наприклад, прибрати «галочку», щоб відмовитись від чогось. * Такою, що передбачає можливість відкликання. Відповідній особі чітко пояснюється, як відкликати згоду.   Наприклад, споживач, який реєструється у програмі винагород Abbott Nutrition Similac© Strong Moms© Rewards, може надати згоду на збір та використання його (її) персональних даних, вибравши (наприклад, встановивши «галочку») отримання додаткової рекламної інформації.  Другий етап життєвого циклу даних — це управління.  На цьому етапі інформація обробляється та зберігається.  З метою захисту персональних даних на цьому етапі ми впровадили процеси, які забезпечують дотримання принципів:   * цілісності даних; * доступу та виправлення.   Цілісність даних передбачає вжиття належних заходів для забезпечення того, щоб персональні дані, які ми зберігаємо, були точними, повними та актуальними.  Один із способів зробити це — відстежувати та реєструвати всі дії, які передбачають обробку персональних даних. У такий спосіб ми можемо визначити джерело даних, конкретні цілі, для яких дані були оброблені, та місце їхнього зберігання.  Доступ та виправлення передбачає надання відповідним особам належного доступу до їхніх даних та змоги реалізувати власні права у зв’язку з цими даними.  Тобто, відповідь на запит особи про доступ, видалення, передачу або зміну персональних даних, що зберігаються.  Третій етап життєвого циклу — використання.  На цьому етапі персональні дані використовуються для підтримки діяльності організації.  З метою захисту персональних даних на цьому етапі ми впровадили процеси, які забезпечують дотримання принципу «Розкриття та використання».  Розкриття та використання — це контроль за тим, хто має доступ до персональних даних, та обмеження використання до певних цілей.  Ми управляємо цим за допомогою засобів контролю доступу та інших процесів. Ці засоби контролю та процеси передбачають надання доступу лише певним особам, які виконують відповідні службові функції, а також обмежують використання конкретними цілями, викладеними в повідомленні, на які було надано згоду.  Завершальним етапом життєвого циклу є розпорядження.  Розпорядження — це те, що відбувається з даними, коли вони вже не використовуються активно. Можливі варіанти можуть включати видалення, архівування або зберігання даних для законних цілей.  З метою захисту персональних даних на цьому етапі ми впровадили політики та процеси, які забезпечують дотримання принципу «Зберігання та розпорядження».  Зберігання персональних даних і розпорядження ними означає зберігання персональних даних лише протягом періоду, необхідного для досягнення цілей, для яких вони були потрібні та оброблені.  Компанія Abbott запровадила процеси архівування або розпорядження персональними даними, які більше не потрібні в активному виробничому середовищі, в такий спосіб, який відповідає вимогам Abbott щодо управління, зберігання та розпорядження даними. Наші вимоги щодо зберігання та розпорядження також враховують усі вимоги щодо утримання даних на законних підставах, викликані юридичними питаннями.  Для отримання додаткової інформації, пов’язаної з вимогами щодо зберігання або розпорядження, див. Глобальну політику Abbott щодо записів та інформації (l1-02) або зверніться до відділу управління інформацією та записами. Детальну інформацію можна знайти в розділі «Ресурси» цього тренінгу.  Для того щоб переглянути контактні дані та додаткову інформацію, натисніть позначку «Ресурси».  Як ми щойно переконалися, наші політики та процедури розроблені для захисту персональних даних протягом усього життєвого циклу.  Ми робимо це, дотримуючись принципів:   * повідомлення; * згоди; * цілісності даних; * доступу та виправлення; * розкриття та використання; * зберігання та розпорядження.   ОТРИМАННЯ  Повідомлення  Згода  УПРАВЛІННЯ  Цілісність даних  Доступ та виправлення  ВИКОРИСТАННЯ  Розкриття та використання  РОЗПОРЯДЖЕННЯ  ЗБЕРІГАННЯ ТА РОЗПОРЯДЖЕННЯ |
| [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 | Будь ласка, натисніть стрілку, щоб почати повторення.  Повторення  Перегляньте деякі основні поняття, які ми розглянули в цьому розділі.  Персональні дані (ПД)  ПД — це будь-яка інформація, яку можна використати для   * встановлення контакту, * визначення місцезнаходження або * ідентифікації особи.   Захищена медична інформація (ЗМІ)  ЗМІ є особливим конфіденційним видом персональних даних, що використовується у галузі охорони здоров’я.  Закони про забезпечення конфіденційності  У різних країнах закони про забезпечення конфіденційності відрізняються, але часто мають однакові основні принципи.  Принципи спроектованої конфіденційності Abbott  Політики та процедури забезпечення конфіденційності та захисту даних компанії Abbott організовані за простим набором принципів, які разом називаються «Спроектована конфіденційність».  Повідомлення та згода  Повідомлення та згода означає повідомлення людей про те, які ПД збираються, і надання їм можливості дати свою згоду на такий збір.  Цілісність даних  Цілісність даних передбачає вжиття належних заходів для забезпечення того, щоб ПД, які ми зберігаємо, були точними, повними та актуальними.  Доступ та виправлення  Доступ та виправлення передбачає надання особам права доступу до їхніх даних і можливості виправляти їх.  Розкриття та використання  Розкриття та використання — це контроль за тим, хто має доступ до ПД.  ЗБЕРІГАННЯ ТА РОЗПОРЯДЖЕННЯ  Зберігання та розпорядження ПД означає зберігання персональних даних лише протягом періоду, необхідного для досягнення цілей, для яких вони були потрібні та оброблені.  Для того щоб перевірити успішність засвоєння вами матеріалу, натисніть кнопку «Меню»  Молодець!  Ви вивчили розділ 1 із 4  Будь ласка, натисніть стрілку вперед, щоб продовжити вивчення |
| [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. | Іншим типом конфіденційних даних, які ми можемо часто використовувати, є конфіденційна ділова інформація.  Конфіденційна ділова інформація має широке визначення. Вона включає велику частину ділової інформації, якою ми користуємось і з якою стикаємося щодня. Конфіденційна інформація — це інформація, яка відсутня в публічному доступі, і яка може бути використана на користь конкурентів компанії Abbott або може зашкодити компанії Abbott у разі розкриття. |
| [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. | Кендіс | Менеджер із маркетингу  Ви можете навести кілька прикладів конфіденційної ділової інформації?  Конфіденційна ділова інформація може зокрема включати: проекти продуктів та виробничі процеси, склади, організми, комп’ютерне програмне забезпечення, дані досліджень і розробок, клінічні та фармакологічні дані, дані пацієнтів, технічні дані, списки клієнтів і потенційних клієнтів, методи ведення бізнесу, маркетингові плани і стратегії, фінансові й операційні дані, а також дані персоналу.  Вона також може включати інформацію про придбання, як-от тендерні пропозиції, списки постачальників та інформацію про вартість. |
| [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. | Джеррі | Торговий представник  На вашу думку, чи є певні типи конфіденційної ділової інформації більш чутливими порівняно з іншими?  Так. Деякі типи конфіденційної ділової інформації вимагають більшої обережності, ніж зазвичай, оскільки неналежне розголошення або використання цієї інформації може завдати компанії серйозної шкоди.  Приклади:   * торгові секрети — формули та процеси виробництва; * клінічні та нормативні дані, реєстраційні досьє або дореєстраційна інформація; * фінансові дані, які не розкривалися широкому загалу. |
| [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. | Як бачите, більшість ділової інформації, яку ми використовуємо у своїй щоденній роботі, вважається конфіденційною.  Хороший спосіб перевірити, чи є ділова інформація, якою ви користуєтеся, конфіденційною, — це поставити собі просте питання:  Чи перебуває ця інформація у відкритому доступі?  Якщо відповідь негативна, то інформацію слід вважати конфіденційною та вживати відповідних заходів для її захисту. |
| [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. | Також важливо пам’ятати, що будь-яка конфіденційна ділова інформація, створена в межах виконання вами робочих обов’язків у компанії Abbott, належить компанії Abbott.  Отже, ви повинні захищати цю інформацію і не маєте права залишити її в себе після закінчення роботи в компанії Abbott. |
| [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. | Захищати конфіденційну ділову інформацію вкрай важливо.  Тож не дивно, що неналежне використання або розкриття цієї інформації може призвести до суттєвих збитків для компанії 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. | Неналежне використання або розкриття конфіденційної інформації може суттєво зашкодити відносинам компанії Abbott із її замовниками та клієнтами, призвести до негативного висвітлення в засобах масової інформації, а також спричинити втрату конкурентної переваги компанії Abbott. Це також може призвести до цивільних позовів проти поточних і колишніх працівників і притягнення їх до кримінальної відповідальності.  НАТИСНІТЬ КНОПКУ «ОСТАННІ СПРАВИ», ЩОБ ОТРИМАТИ ДОДАТКОВУ ІНФОРМАЦІЮ. |
| [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. | ОСТАННІ СПРАВИ  Останнім часом на користь компаній ухвалювалися судові рішення з великими сумами компенсації, яку мали сплатити колишні працівники за неправомірне отримання у своє розпорядження інформації, що належить компанії. Наприклад, на користь однієї компанії було ухвалено рішення про компенсацію в розмірі 240 мільйонів доларів США проти колишнього працівника, який неналежним чином розкрив конфіденційну інформацію компанії конкуренту. На користь іншої компанії було ухвалено рішення на суму 854 мільйони доларів США проти колишнього працівника та його нового роботодавця, коли колишній працівник неправомірно привласнив конфіденційну інформацію компанії й потім використав її на користь нового роботодавця.  Згідно з дослідженнями, крадіжка конфіденційної інформації спричиняє для компаній, акції яких продаються на фондовій біржі, збитки в розмірі від 209 до 625 мільярдів доларів США. |
| [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. | Тож не дивно, що органи влади дуже серйозно ставляться до крадіжки конфіденційної інформації.  Так, згідно з федеральним карним законодавством, за крадіжку конфіденційної інформації фізичним особам може загрожувати до десяти років ув’язнення та штраф у розмірі до 5 мільйонів дол. США. А компанія, яку визнають винною у крадіжці конфіденційної інформації, може отримати штраф у розмірі до 10 мільйонів дол. США або в розмірі потрійної вартості конфіденційної інформації.  НАТИСНІТЬ КНОПКУ «ШТРАФИ ТА ФІНАНСОВІ САНКЦІЇ», ЩОБ ОТРИМАТИ ДОДАТКОВУ ІНФОРМАЦІЮ. |
| [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. | ШТРАФИ ТА ФІНАНСОВІ САНКЦІЇ  Останніми роками за крадіжку конфіденційної інформації були оштрафовані та засуджені до позбавлення волі кілька фізичних осіб і компаній. Наприклад:   * конкурента було оштрафовано на суму 60 мільйонів дол. США за крадіжку конфіденційної інформації іншої компанії; * колишнього співробітника ІТ-відділу було засуджено до 97 місяців ув’язнення за крадіжку конфіденційної інформації; * колишнього співробітника відділу продажу було засуджено до 12 місяців ув’язнення за крадіжку конфіденційної інформації; * керівника вищої ланки було засуджено до 24 місяців ув’язнення за крадіжку конфіденційної інформації; і * ученого-дослідника було засуджено до 18 місяців ув’язнення за крадіжку конфіденційної інформації. |
| [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. | Інший тип конфіденційної ділової інформації, який важливо вміти розпізнавати та захищати, зазвичай називають *інсайдерською інформацією.*  Інсайдерська інформація — це важлива непублічна інформація, яка, у разі розкриття широкому загалу, з великою вірогідністю може вплинути на ринкову вартість цінних паперів компанії або вплинути на рішення інвесторів щодо купівлі або продажу цінних паперів. |
| [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. | Інші приклади інсайдерської інформації включають:   * новини про потенційне придбання; * затримку запуску продукту; * новини про збій в роботі внутрішніх ІТ-систем; * непередбачувані зміни доходів або ставок дивідендів; * подані тендерні пропозиції або подрібнення акцій компанії; * інформація про головні нові продукти; * присуджені контракти; * плани щодо розширення; * важливі судові провадження або регулятивні провадження тощо. |
| [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. | Торгівля цінними паперами Abbott або надання відповідних рекомендацій іншим щодо цього є незаконними, якщо ви знаєте або володієте інсайдерською інформацією.  Це також стосується купівлі-продажу цінних паперів інших компаній, зокрема тих, які працюють або планують співпрацювати з Abbott.  Щоб дізнатися більше про очікування компанії Abbott стосовно використання та захисту неоприлюдненої інформації, ознайомтеся із політикою компанії Abbott щодо інсайдерської торгівлі. Детальну інформацію можна знайти в розділі «Ресурси» цього тренінгу. |
| [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 | Будь ласка, натисніть стрілку, щоб почати повторення.  Повторення  Перегляньте деякі основні поняття, які ми розглянули в цьому розділі.  Конфіденційна ділова інформація  Усю ділову інформацію, яка відсутня в публічному доступі, слід вважати конфіденційною. Вона включає більшу частину ділової інформації, яку ми використовуємо у своїй щоденній роботі.  Неналежне використання конфіденційної ділової інформації  Неналежне використання або розкриття конфіденційної ділової інформації може призвести до суттєвих збитків для компанії, наших клієнтів і працівників.  Інсайдерська інформація  Інсайдерська інформація — це важлива непублічна інформація, яка, у разі розкриття широкому загалу, з великою вірогідністю може вплинути на ринкову вартість цінних паперів компанії або вплинути на рішення інвесторів щодо купівлі або продажу цінних паперів.  Для того щоб перевірити успішність засвоєння вами матеріалу, натисніть кнопку «Меню»  Молодець!  Ви вивчили розділ 2 з 4  Будь ласка, натисніть стрілку вперед, щоб продовжити вивчення |
| [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. | Тепер, коли ви добре розумієте різні типи даних, з якими ви можете зіткнутися в роботі, ось що ви можете зробити, щоб захистити їх. |
| [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. | Перш ніж отримати доступ до будь-яких конфіденційних даних, обов’язково переконайтеся, що для виконання вами посадових обов’язків вам потрібно мати доступ до даних.  Якщо у вас є запитання щодо того, чи варто отримувати доступ до даних, особливо до персональних даних, зверніться до свого керівника, ДЕДВ або представника глобального підрозділу із захисту персональних даних.  НАТИСНІТЬ КНОПКУ «ВИ ЗНАЛИ?», ЩОБ ОТРИМАТИ ДОДАТКОВУ ІНФОРМАЦІЮ. |
| [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. | ВИ ЗНАЛИ?  Компанія Abbott здійснює різні форми законного моніторингу, щоб знизити ризик неналежного використання даних.  Зокрема, моніторинг завантаження даних або передавання даних на адреси електронної пошти поза межами компанії 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. | Якщо у вас є дозвіл на доступ до конфіденційних даних, використовуйте їх лише з тією метою, для якої вам було надано доступ.  Що стосується персональних даних, використовуйте дані лише відповідно до наданої згоди або повідомлення. |
| [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. | Перш ніж передавати конфіденційні дані, переконайтесь, що особа, якій ви плануєте передати дані, має належний дозвіл.  Якщо у вас є запитання щодо того, чи варто отримувати доступ до даних, особливо до персональних даних, поговоріть зі своїм керівником або підрозділом Abbott із захисту персональних даних. |
| [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. | Запити із вашої країни  Якщо працівник представництва компанії Abbott у вашій країні запитує конфіденційні дані, слід:   * підтвердити особу працівника, який робить запит; * підтвердити потребу особи у доступі до інформації; * переконатися в тому, що особа уповноважена отримати інформацію; * перевірити, щоб інформація могла бути використана для цілей, для яких вона запитується; і * Передавати лише той обсяг інформації, який необхідний для задоволення потреб, і не більше.   Якщо ви сумніваєтеся, зв’яжіться з ДЕДВ або глобальним підрозділом із захисту персональних даних, перш ніж передавати конфіденційні дані. |
| [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. | Запити з інших країн  У багатьох країнах і регіонах є закони, розроблені для захисту прав їхніх громадян, які накладають обмеження на передачу персональних даних через національні кордони.  Якщо ви отримуєте запит на інформацію, що містить конфіденційні дані, від колеги в іншій країні, перевірте політику конфіденційності даних вашого підрозділу або відділу або проконсультуйтеся з ДЕДВ або глобальним підрозділом із захисту персональних даних, перш ніж продовжувати. Потім дійте за таким самим алгоритмом, як у випадку надання відповіді на запит від колеги із вашої країни. |
| [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. | Запити від третіх сторін  Якщо запит щодо конфіденційних даних надходить від третьої сторони, переконайтеся, що існує чинна та відповідна договірна угода. Якщо ви сумніваєтеся, зв’яжіться з глобальним підрозділом ДЕДВ із захисту персональних даних або юридичним департаментом, перш ніж передавати дані. |
| [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. | Завжди архівуйте або утилізуйте конфіденційні дані у спосіб, який відповідає вимогам Abbott щодо управління, зберігання та розпорядження даних. |
| [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. | Якщо ви отримали наказ про зберігання документації, вам забороняється викидати, знищувати або видаляти будь-яку інформацію, стосовно якої діє такий наказ.  Якщо у вас є запитання щодо наказів про зберігання документації або зберігання та розпорядження, зв’яжіться з юристом/помічником юриста, зазначеним у повідомленні про зберігання документації для законних цілей або зателефонуйте в департамент із судових справ за номером (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. | Завжди пильно перевіряйте конфіденційні дані, коли хтось звільняється з компанії Abbott.  Керівники повинні забезпечити припинення повноважень працівника, який залишає компанію, у відповідній системі (наприклад, Workday для співробітників або Fieldglass для працівників за наймом) одразу після отримання повідомлення про його звільнення. Це забезпечить належну організацію доступу до даних компанії Abbott, фізичного доступу до будівель та остаточного розрахунку. |
| [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. | Простежте за тим, аби працівник, який звільняється, не забрав із собою конфіденційні дані. Передайте всі файли співробітнику компанії Abbott, який обійматиме посаду або виконуватиме обов’язки працівника, який залишає компанію.  Нагадайте працівникові, який звільняється, про обов’язок не залишати в себе або не розкривати конфіденційну інформацію. При звільненні з компанії Abbott працівникам забороняється забирати із собою результат своєї діяльності або будь-яке інше майно Abbott (наприклад мобільні пристрої). Якщо у вас є запитання щодо локальних процедур припинення повноважень, зверніться в Департамент управління персоналом. |
| [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. | Ненавмисне розкриття ЗМІ може статися будь-коли.  Наприклад, ви можете підслухати, як медсестра обговорює стан здоров’я пацієнта, або вам можуть випадково відправити копію електронного листа, який містить інформацію пацієнта. |
| [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. | У відповідь на будь-яке ненавмисне або неналежне розкриття захищеної медичної інформації (ЗМІ) пацієнта ви повинні негайно повідомити про це ДЕДВ або представника глобального підрозділу із захисту персональних даних. |
| [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. | Якщо вам стане відомо про ненавмисне або неналежне розкриття конфіденційної ділової інформації, ви маєте негайно повідомити про розкриття:   * вашого безпосереднього керівника; і * ДЕДВ або представника глобального підрозділу ДЕДВ із захисту персональних даних.   Якщо ви негайно повідомите про розкриття, це допоможе компанії Abbott швидко повернути інформацію, попередити додаткове неналежне використання інформації та, якщо доцільно, допоможете компанії під час звернення до суду з цивільним або кримінальним позовом. |
| [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. | Вам заборонено будь-коли розкривати конфіденційні дані компанії Abbott будь-кому, хто не має права отримувати конфіденційну інформацію.  Так само вам дозволено використовувати конфіденційні дані компанії Abbott лише від імені компанії Abbott та під час виконання ваших робочих обов’язків у компанії Abbott.  Якщо ви розкриєте конфіденційні дані неналежним чином, ви можете зазнати дисциплінарних стягнень аж до звільнення. |
| [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. | Вам заборонено (як під час вашої роботи в компанії Abbott, так і після її завершення) передавати дані компанії Abbott будь-якому конкуренту компанії Abbott. |
| [Screen 41](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=51_C_38e)  [51\_C\_38e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=51_C_38e) | Failure to return sensitive data to Abbott, transmitting sensitive data to an unapproved device, storage, account or server, or providing sensitive data to any person or entity not authorized to possess the information can lead to Abbott pursuing legal action against you.  CLICK THE ‘LEGAL ACTION’ BUTTON FOR MORE INFORMATION. | У випадку якщо ви не повернете компанії Abbott конфіденційні дані, передаватимете конфіденційні дані на незатверджений пристрій, сховище, обліковий запис або сервер, або передаватимете конфіденційні дані будь-якій фізичній або юридичній особі, яка не має права володіти такою інформацією, це може спричинити здійснення проти вас юридичних дій компанією Abbott.  НАТИСНІТЬ КНОПКУ «ЮРИДИЧНА ДІЯ», ЩОБ ОТРИМАТИ ДОДАТКОВУ ІНФОРМАЦІЮ. |
| [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. | ЮРИДИЧНА ДІЯ  Юридична дія може включати звернення компанії Abbott до суду з позовом проти вас, який призведе до того, що:   * вам буде заборонено працювати на нового роботодавця, доки конфіденційну інформацію компанії Abbott не буде повернено та захищено; * ви будете зобов’язані передати всі електронні пристрої до компанії Abbott для огляду та перевірки; * ви будете зобов’язані компенсувати фінансові збитки, спричинені незаконним утриманням та (або) використанням конфіденційних даних компанії Abbott та порушенням ваших обов’язків перед компанією Abbott відповідно до вашого договору особистого найму з компанією Abbott; і * ви будете зобов’язані сплатити юридичні витрати, понесені компанією Abbott унаслідок подання позову до суду для захисту її конфіденційних даних.   Якщо необхідно, компанія Abbott співпрацюватиме з органами на федеральному, регіональному та місцевому рівнях влади для захисту та збереження конфіденційних даних компанії Abbott. У такому разі вам також може загрожувати кримінальне покарання. |
| [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. | Про будь-яку подію щодо потенційного порушення інформаційної безпеки, включно зі втратою або крадіжкою мобільного пристрою, слід негайно повідомити Глобальну службу підтримки.  Якщо у вас є якісь занепокоєння щодо можливого порушення або ви хочете повідомити про потенційний випадок порушення конфіденційності, зверніться до глобального підрозділу із захисту персональних даних. |
| [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 | Будь ласка, натисніть стрілку, щоб почати повторення.  Повторення  Перегляньте деякі основні поняття, які ми розглянули в цьому розділі.  Доступ та використання конфіденційних даних  Отримуйте доступ до конфіденційних даних і користуйтеся ними лише з тією метою, для якої вам було надано доступ.  Обмін конфіденційними даними  Перш ніж передавати конфіденційні дані:   * перевірте особу працівника, який робить запит; * переконайтеся, що в нього є потреба в доступі до інформації; * упевніться в тому, що інформація може бути використана для цілей, для яких вона запитується; і * передавайте лише той обсяг інформації, який необхідний для задоволення потреб.   Зберігання та видалення конфіденційних даних  Завжди архівуйте або утилізуйте конфіденційні дані у спосіб, який відповідає вимогам Abbott щодо управління, зберігання та розпорядження даних.  Реагування на ненавмисне розкриття ЗМІ  У відповідь на будь-яке ненавмисне або неналежне розкриття ЗМІ пацієнта негайно повідомте про розкриття ДЕДВ або представника глобального підрозділу із захисту персональних даних.  Повідомлення про порушення конфіденційності  Для того щоб повідомити про можливе порушення конфіденційності, зв’яжіться з глобальним підрозділом із захисту даних.  Для того щоб перевірити успішність засвоєння вами матеріалу, натисніть кнопку «Меню»  Молодець!  Ви вивчили розділ 3 з 4  Будь ласка, натисніть стрілку вперед, щоб продовжити вивчення |
| [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. | Де отримати допомогу  Департамент етики та дотримання вимог (ДЕДВ)  Глобальний підрозділ ДЕДВ із захисту персональних даних: зверніться до Глобального підрозділу ДЕДВ із захисту персональних даних за адресою [privacy@abbott.com](mailto:privacy@abbott.com). Додаткові контактні дані та важлива інформація про конфіденційність розміщені на сторінці Міжнародного порталу із захисту персональних даних [тут](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) у Abbott World.  Контакти Департаменту етики та дотримання вимог – звертайтеся до Департаменту етики та дотримання вимог у будь-який час з будь-якими запитаннями щодо етики або дотримання норм або щоб обговорити занепокоєння стосовно можливих порушень наших стандартів, викладених у письмовій формі, законів або нормативно-правових актів.   * Відвідайте сторінку [Контакти ДЕДВ](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) на [вебсайті ДЕДВ](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) у Abbott World або [OEC@abbott.com](mailto:OEC@abbott.com).   КОРПОРАТИВНА КІБЕРБЕЗПЕКА  Відвідайте сайт Корпоративної кібербезпеки [тут](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) у Abbott World.  Відвідайте сайт [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx), щоб дізнатися про безпечні способи передачі інформації.  Юридичний департамент  Звертайтеся до [юридичного департаменту](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) з питаннями або сумнівами щодо договірних зобов’язань перед третіми сторонами щодо конфіденційності та захисту даних.  Зверніться до команди з питань управління інформацією за адресою [information.governance@abbott.com](mailto:information.governance@abbott.com) із запитаннями чи зауваженнями про вимоги щодо зберігання або за вказівками щодо прийнятного використання технологічних рішень.  ВІДПОВІДНІ ПОЛІТИКИ   * Натисніть [тут](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), щоб ознайомитися з політикою з питань розкриття конфіденційної інформації * Натисніть [тут](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx), щоб ознайомитися з Політикою Abbott щодо інсайдерської торгівлі * Натисніть [тут](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), щоб ознайомитися з Політикою прийнятного використання технологій. * Натисніть [тут](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), щоб ознайомитися з політикою щодо записів та інформації в системі M-Files.   Правила та процедури Департаменту етики та дотримання вимог  Глобальні та спеціальні для кожної країни правила і процедури Департаменту етики та дотримання вимог:   * Співробітники Abbott повинні відвідати [iComply](https://icomply.abbott.com/Default.aspx).   Центр обслуговування департаменту управління персоналом   * Щоби переглянути список контактних номерів служби підтримки департаменту управління персоналом, натисніть [тут](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf).   Ресурси для курсу  Копія  Натисніть [тут,](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) щоб отримати повну копію курсу. |
| [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. | Перевірка знань складається з 10 запитань. Ви повинні набрати 80 % або більше, щоб успішно завершити цей курс.  Коли будете готові, натисніть кнопку **Перевірка знань**. |
| 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? | Нехай, ви кілька років працювали в компанії Abbott, а нещодавно прийняли пропозицію роботи в іншій компанії. Що з переліченого далі ви маєте право взяти із собою на законних підставах при звільненні? |
| 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] Персональні дані пацієнтів, отримані під час клінічних досліджень  [2] Списки клієнтів компанії Abbott і презентаційну інформацію, створену вами під час роботи в компанії Abbott  [3] Прогнози продажів і фінансові дані вашого підрозділу або філії компанії Abbott  [4] Персональні фотографії та пам’ятні подарунки |
| 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. | Правильна відповідь — 4. Персональні дані, конфіденційна ділова інформація та закрита медична інформація вважаються конфіденційними даними, ви не маєте права брати їх із собою або використовувати після звільнення з Abbott. До того ж перед звільненням необхідно повернути всі електронні пристрої компанії Abbott та інше майно, що належить Abbott.  Для отримання додаткової інформації див. розділ 3.4 «Реагування на неналежне розкриття». |
| 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. | Менеджер із маркетингу готує випуск нової продукції. Йому потрібно розробити форму згоди для потенційних клієнтів. Форма дозволить збирати та використовувати персональні дані. Для того щоб форма відповідала практикам Abbott стосовно отримання згоди, які з наведених далі тверджень мають бути правильними для форми згоди?  Позначте всі правильні варіанти. |
| 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] Форма не повинна змушувати клієнтів дати свою згоду.  [2] Форма повинна надавати клієнтам всю інформацію про те, як саме використовуватимуться їхні персональні дані.  [3] Форма повинна наполягати, щоб клієнти активно погоджувалися на збір і використання їхніх персональних даних.  [4] Форма не повинна дозволяти клієнтам відкликати надану ними згоду. |
| 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. | Практики компанії Abbott стосовно отримання згоди вимагають, щоб форма:   * була зрозумілою та короткою; * не змушувала людей давати свою згоду; * містила вичерпну інформацію про те, як саме використовуватимуться їхні персональні дані; * наполягала, щоб люди активно погоджувалися на збір і використання їхніх персональних даних; * Дозволяла відкликати згоду за бажанням.   Для отримання додаткової інформації див. розділ 1.3 «Принципи спроектованої конфіденційності Abbott». |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Розкриття та використання конфіденційних даних, таких як персональні дані, здійснюється Abbott за рахунок: |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] Знеособлення всіх даних.  [2] Контролю доступу.  [3] Обидва варіанти 1 і 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. | Розкриття та використання персональних даних здійснюється за допомогою засобів контролю доступу та інших процесів, які передбачають надання права доступу та використання лише тим особам, які виконують певні робочі функції для конкретних цілей, вказаних у повідомленні, на яке була надано згода.  Для отримання додаткової інформації див. розділ 1.3 «Принципи спроектованої конфіденційності Abbott». |
| Screen 46  Question 4: Scenario  66\_C\_48 | Which of the following is true in relation to the retention and disposal of personal information?  Check all that apply. | Які з наведених далі тверджень є правильними для зберігання та розпорядження персональними даними?  Позначте всі правильні варіанти. |
| 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] Персональні дані зберігаються лише протягом періоду, необхідного для досягнення цілей, для яких вони були отримані та оброблені.  [2] Як тільки дані більше не потрібні в активному виробничому середовищі, їх слід знищити.  [3] Вимоги щодо зберігання та розпорядження персональними даними враховують усі накази про зберігання даних. |
| 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. | Зазвичай, персональні дані зберігаються в Abbott лише протягом періоду, необхідного для досягнення цілей, для яких вони були отримані та оброблені. Дані, які більше не потрібні в активному виробничому середовищі, мають бути заархівовані або знищені в такий спосіб який відповідає вимогам Abbott щодо управління, збереження та розпорядження даними. Наші вимоги щодо збереження та розпорядження також враховують будь-які затримки, викликані юридичними питаннями.  Для отримання додаткової інформації про правильну відповідь див. розділ 1.3 «Принципи спроектованої конфіденційності Abbott». |
| Screen 46  Question 5: Scenario  69\_C\_48 | An Engineer is working on developing a new product. Which of the following would be considered confidential business information that must be kept secure?  Check all that apply. | Інженер працює над розробкою нової продукції. Що з переліченого далі вважатиметься конфіденційною діловою інформацією, яку потрібно зберігати в таємниці?  Позначте всі правильні варіанти. |
| 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] Прогнози продажів нової продукції.  [2] Дані фінансової звітності із річного звіту компанії Abbott.  [3] Інформація про закупівлі, наприклад, тендерні пропозиції на отримання підряду на нову продукцію.  [4] Інформація про подібну продукцію конкурентів.  [5] Пропозиції сторонніх постачальників, пов’язані з новою продукцією. |
| 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. | Конфіденційна ділова інформація має широке визначення. Вона включає велику частину ділової інформації, якою ми користуємось і з якою стикаємося щодня. Хороший спосіб перевірити конфіденційність інформації, — це поставити собі просте питання:  Чи перебуває ця інформація у відкритому доступі?  Якщо відповідь негативна, то інформація майже напевно є конфіденційною, і вам слід вживати відповідних заходів для її захисту.  Для отримання додаткової інформації див. розділ 2.1 «Визнання конфіденційної ділової інформації». |
| 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: | Загальний регламент про захист даних (GDPR) є одним з найбільш вичерпних законодавчих актів у світі. Він був запроваджений у 2018 році і править за взірець у сфері захисту даних. Цей регламент був розроблений у: |
| Screen 46  Question 6: Options  73\_C\_48 | [1] Canada  [2] Asia  [3] Europe  [4] Russia  [5] United States  [6] Latin America | [1] Канаді  [2] Азії  [3] Європі  [4] Росії  [5] США  [6] Латиноамериканському регіоні |
| 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. | Правильна відповідь — в Європі. На території Європи одним із найбільш вичерпних законодавчих актів для всіх країн-учасниць є Загальний регламент про захист даних (GDPR). Після його запровадження в 2018 році він править за взірець у сфері захисту даних, який прагнуть наслідувати інші країни.  Для отримання додаткової інформації див. розділ 1.2 «Правові, нормативні та договірні угоди». |
| 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: | Ваш колега щойно закінчив роботу над проєктом, що передбачав збір і використання персональних даних. Після чого він отримав запит на доступ до цих даних від іншого департаменту. Ви радите своєму колезі: |
| 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] Перевірити особу працівника, який робить запит, і необхідність отримати доступ до інформації.  [2] Переконатися в тому, що працівник, який робить запит, уповноважений отримати копію інформації.  [3] Перевірити, щоб інформація могла бути використана для цілей, зазначених у запиті.  [4] Усі варіанти, зазначені вище. |
| 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. | Однією з найпоширеніших причин порушення конфіденційності даних в організації є неналежний обмін даними з неуповноваженим персоналом. Перш ніж передавати будь-який документ або файл, що містить конфіденційні дані, слід:   * Підтвердити особу працівника, який робить запит, і необхідність отримати доступ до інформації. * Переконатися у тому, що особа уповноважена отримати копію інформації. * Перевірити, щоб інформація могла бути використана для цілей, для яких вона запитується. * Передавати лише той обсяг інформації, який необхідний для задоволення потреб, і не більше.   Для отримання додаткової інформації див. розділ 3.2 «Передача конфіденційних даних». |
| 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? | Ви — торговий представник. Ви приходите у свою районну лікарню. Очікуючи в зоні прийому, ви випадково кладете не на місце конфіденційні документи, що містять закриту медичну інформацію. Що ви зробите? |
| 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] Повідомите працівника, відповідального за конфіденційність персональних даних.  [2] Зв’яжетеся зі своїм керівником.  [3] Повідомите про інцидент ДЕДВ або представника глобального підрозділу ДЕДВ із захисту персональних даних. |
| 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. | У відповідь на будь-яке ненавмисне розкриття захищеної медичної інформації пацієнта слід негайно повідомити про це:   * ДЕДВ або представника глобального підрозділу ДЕДВ із захисту персональних даних.   Для отримання додаткової інформації див. розділ 3.4 «Реагування на неналежне розкриття». |
| 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? | Ви їдете на роботу поїздом. Виходячи з вагона, ви випадково залишаєте на сидінні ноутбук, в якому є конфіденційні робочі документи. Ви усвідомлюєте, що сталося, лише на роботі, коли починаєте гарячково шукати свій ноут і не можете знайти. Що ви повинні робити передусім? |
| 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] Зателефонувати в залізничну компанію і спитати, чи не повернув хто ваш ноутбук.  [2] Повернутися на залізничну станцію і пошукати ноутбук там.  [3] Звернутися до місцевого відділення Глобальної служби підтримки. |
| 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. | Якщо ви вважаєте, що конфіденційні дані могли бути стати відомими іншим не у встановленому порядку, наприклад із ноутбука, який був загублений або вкрадений, негайно зверніться до місцевого відділення Глобальної служби підтримки.  Для отримання додаткової інформації див. розділ 3.4 «Повідомлення про інцидент із даними». |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | Ви повинні використовувати персональні дані лише:  Позначте всі правильні варіанти. |
| 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] з тією метою, для якої вам було надано доступ;  [2] так, як зазначено в повідомленні, наданому суб’єкту даних;  [3] так, як це передбачено згодою, наданою суб’єктом даних. |
| 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. | Якщо у вас є дозвіл на доступ до персональних даних, використовуйте його лише:   * з тією метою, для якої вам було надано доступ; * так, як зазначено в повідомленні, наданому суб’єкту даних; * так, як це передбачено згодою, наданою суб’єктом даних.   Для отримання додаткової інформації див. розділ 3.1 «Доступ та використання конфіденційних даних». |
| [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 | Усі запитання залишаються без відповіді |
| [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. | Результати недоступні, тому що ви не завершили перевірку знань.  Вітаємо! Ви успішно пройшли перевірку знань і завершили курс.  Перегляньте результати нижче, натиснувши на кожне запитання.  Після завершення натисніть кнопку **ВИХІД [X]** на панелі заголовку курсу, перед тим як закрити вікно або вкладку браузера.  На жаль, ви не пройшли перевірку знань. Перегляньте результати нижче, натиснувши на кожне запитання.  Коли будете готові, натисніть кнопку **Пройти перевірку знань повторно.** |
| 89\_toc\_1 | Introduction | Вступ |
| 90\_toc\_2 | Welcome | Привітання |
| 91\_toc\_3 | Objectives | Цілі |
| 92\_toc\_4 | Menu | Меню |
| 93\_toc\_5 | Personal Information | Персональні дані |
| 94\_toc\_6 | Recognizing Personal Information | Визнання персональних даних |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Правові, нормативні та договірні вимоги |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Принципи спроектованої конфіденційності Abbott |
| 97\_toc\_9 | Review | Повторення |
| 98\_toc\_10 | Confidential Business Information | Конфіденційна ділова інформація |
| 99\_toc\_11 | Recognizing Confidential Business Information | Визнання конфіденційної ділової інформації |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Наслідки незабезпечення захисту конфіденційної ділової інформації |
| 101\_toc\_13 | Insider Information | Інсайдерська інформація |
| 102\_toc\_14 | Review | Повторення |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Ваша роль у захисті конфіденційних даних |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Доступ та використання конфіденційних даних |
| 105\_toc\_17 | Sharing Sensitive Data | Обмін конфіденційними даними |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Зберігання та видалення конфіденційних даних |
| 107\_toc\_19 | Responding to Improper Disclosures | Реагування на неналежне розкриття |
| 108\_toc\_20 | Review | Повторення |
| 109\_toc\_21 | Knowledge Check | Перевірка знань |
| 110\_toc\_22 | Introduction | Вступ |
| 111\_toc\_23 | Assessment | Оцінка |
| 112\_toc\_24 | Question 1 | Запитання 1 |
| 113\_toc\_25 | Question 2 | Запитання 2 |
| 114\_toc\_26 | Question 3 | Запитання 3 |
| 115\_toc\_27 | Question 4 | Запитання 4 |
| 116\_toc\_28 | Question 5 | Запитання 5 |
| 117\_toc\_29 | Question 6 | Запитання 6 |
| 118\_toc\_30 | Question 7 | Запитання 7 |
| 119\_toc\_31 | Question 8 | Запитання 8 |
| 120\_toc\_32 | Question 9 | Запитання 9 |
| 121\_toc\_33 | Question 10 | Запитання 10 |
| 122\_toc\_34 | Feedback | Коментарі та зауваження |
| 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 | Курс не може з’єднатися із системою управління навчанням (СУН). Натисніть «OK», щоб продовжити і переглянути курс. Майте на увазі, Атестація по курсу може бути недоступною. Натисніть «Відмінити», щоб вийти |
| 124\_string\_2 | All questions remain unanswered | Усі запитання залишаються без відповіді |
| 125\_string\_3 | Questions | Запитання |
| 126\_string\_4 | Question | Запитання |
| 127\_string\_5 | not answered | немає відповіді |
| 128\_string\_6 | That's correct! | Правильно! |
| 129\_string\_7 | That's not correct! | Неправильно! |
| 130\_string\_8 | Feedback: | Коментарі та зауваження: |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ |
| 132\_string\_10 | Knowledge Check | Перевірка знань |
| 133\_string\_11 | Submit | Надіслати |
| 134\_string\_12 | Retake Knowledge Check | Пройти перевірку знань повторно |
| 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. | Опис курсу: У Abbott ми часто використовуємо конфіденційні дані для прийняття важливих ділових рішень. Оскільки у багатьох зацікавлених сторін виникають занепокоєння щодо того, яким чином ці дані збираються та використовуються, компанія Abbott запровадила політику та процедури для захисту цих даних. Цей курс пояснює, що таке конфіденційні дані, чому вони життєво важливі для нашого бізнесу та які кроки ми можемо зробити, щоб забезпечити безпечну та надійну обробку цих даних. Щоби пройти курс повністю, знадобиться приблизно 30 хвилин. |
| 136\_string\_14 | Menu | Меню |
| 137\_string\_15 | Resources | Ресурси |
| 138\_string\_16 | Reference Material | Довідкові матеріали |
| 139\_string\_17 | Audio | Аудіо |
| 140\_string\_18 | Exit | Вийти |
| 141\_string\_19 | Record My Results | Записати мої результати |