|  |  |  |
| --- | --- | --- |
| 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 DataClick the forward arrow to begin. | הגנה על מידע רגישלחצו על החץ קדימה כדי להתחיל. |
| [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. | ב-Abbott, אנו מסתמכים על מידע לצורך קבלת החלטות – לעתים קרובות, המידע הזה מכיל נתונים רגישים.כדי שנוכל להגשים את המשימה שלנו לעזור לאנשים לחיות את חייהם בצורה הטובה ביותר באמצעות בריאות טובה, חיוני שנשמור על המידע הזה מאובטח ונציית לחוקים ולסטנדרטים האתיים שבהם Abbott דוגלת. קורס זה נועד לספק לכם את הכישורים הדרושים להגשמת משימה זו. |
| [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.
 | לאחר השלמת הקורס, תהיה לכם הבנה טובה יותר לגבי:* מהו מידע רגיש,
* כיצד אנו מגינים על המידע הזה ב-Abbott,
* מהו תפקידכם בהגנה על מידע רגיש, וכן
* מה עליכם לעשות אם אתם סבורים כי ייתכן שמידע רגיש נחשף באופן לא ראוי או שהוא נתון בסכנה.
 |
| [Screen 3](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4) [4\_C\_4](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx?showScreen=4_C_4)  | 1 | Personal InformationHere you will learn how governments, consumers, and the public have become increasingly concerned about the privacy and security of personal information.12 MinutesSection 1 | Personal InformationRecognizing Personal InformationLegal, Regulatory and Contractual RequirementsAbbott’s Privacy by Design PrinciplesReview2 | Confidential Business InformationHere you will learn how most of the business information we use in our day-to-day work activities is considered confidential.5 MinutesSection 2 | Confidential Business InformationRecognizing Confidential Business InformationCost of Not Protecting Confidential Business InformationInsider InformationReview3 | Protecting Sensitive DataHere you will learn what you can do to help protect sensitive data.8 MinutesSection 3 | Your Role in Protecting Sensitive DataAccessing and Using Sensitive DataSharing Sensitive DataRetaining and Disposing of Sensitive DataResponding to Improper DisclosuresReview4 | Knowledge CheckAssess your understanding of the key concepts and principles of this course.5 MinutesSection 4 | Knowledge CheckAssessmentClick 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 | מידע אישיכאן תלמדו מדוע ממשלות, צרכנים והציבור הכללי החלו לחשוש יותר ויותר בנוגע לפרטיות ואבטחת מידע אישי.12 דקותחלק 1 | מידע אישיזיהוי מידע אישידרישות משפטיות, רגולטוריות וחוזיותעקרונות "עיצוב לפרטיות" של Abbottסקירה2 | מידע עסקי חסויכאן תלמדו מדוע רוב המידע העסקי שאנו משתמשים בו בעבודה היומיומית שלנו נחשב חסוי.5 דקותחלק 2 | מידע עסקי חסויזיהוי מידע עסקי חסוימחיר אי ההגנה על מידע עסקי חסוימידע פניםסקירה3 | הגנה על מידע רגישכאן תלמדו מהם הצעדים שתוכלו לנקוט כדי לסייע להגן על מידע רגיש.8 דקותחלק 3 | תפקידכם בהגנה על מידע רגישגישה למידע רגיש ושימוש בושיתוף מידע רגיששמירת מידע רגיש והסרתותגובה לחשיפות בלתי ראויותסקירה4 | בדיקת ידעהעריכו את הבנתכם לגבי מושגי המפתח והעקרונות של הקורס.5 דקותחלק 4 | בדיקת ידעהערכהלחצו על הפאנל כדי להתחיל.לחצו על לחצן ההפעלה הצהוב כדי להתחיל.תוכן זה אינו זמין עדיין. עליכם להשלים את חלק{a} {b}. |
| [Screen 4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7) [5\_C\_7](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx?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. | אחד מסוגי המידע הרגיש הנפוצים שבו אנו משתמשים ב-Abbott הוא מידע אישי.בשנים האחרונות החלו ממשלות, צרכנים והציבור הכללי לחשוש יותר ויותר בנוגע לפרטיות ולאבטחת המידע האישי שלהם. |
| [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. | מידע אישי הוא כל מידע שניתן להשתמש בו כדי ליצור קשר עם אדם מסוים, לאתר אותו או לזהות אותו. |
| Screen 6 [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. | קנדיס | מנהלת שיווק אוכל לקבל כמה דוגמאות למידע אישי?מידע אישי יכול לכלול מידע ביוגרפי כגון שם, תאריך לידה, כתובת דוא"ל ומספר טלפון.הוא יכול לכלול מידע בקשר למראהו של אדם מסוים, כגון צבע שיער או משקל.הוא גם יכול לכלול מידע בקשר לחייו הפרטיים של אדם מסוים כגון תמונות, קובצי Cookie של דפדפן או מידע של מעקב אחר מיקום. |
| Screen 7 [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. | ג'רי | נציג מכירות האם מידע אישי כולל גם מידע בריאות מוגן?אכן כן.מידע בריאות מוגן (PHI) הוא סוג רגיש במיוחד של מידע אישי שבו משתמשים בענף הבריאות. הוא כולל כל מידע המאפשר זיהוי של אדם ברשומות רפואיות, כולל שיחות בין אנשי צוות רפואי בנוגע לטיפול. |
| [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. | ברוב המדינות שבהן Abbott מנהלת את עסקיה, קיימים חוקים ותקנות שנועדו להגן על המידע האישי, כולל מידע בריאות מוגן.החוקים הקשורים לפרטיות ולהגנה על מידע אישי משתנים ממדינה למדינה, אבל עקרונות היסוד הם לעתים קרובות זהים.לחצו על כל אחד מהאזורים המודגשים במסך כדי ללמוד על הסוגים השונים של חוקי ודרישות הפרטיות הנהוגים ברחבי העולם. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11) [10\_C\_11](file:///D%3A/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf?showScreen=10_C_11)  | EuropeIn 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. | אירופהבאירופה, האסדרה הכללית להגנה על מידע (GDPR) היא אחד מחוקי הפרטיות המקיפים בעולם; מאז הטמעתה ב-2018, היא קבעה סטנדרט להגנה על פרטיות שמדינות אחרות מנסות לחקות. תקנות ה-GDPR חלות על ארגונים הממוקמים באירופה, וכן על ארגונים מחוץ לאירופה שמציעים סחורות ושירותים לאנשים המתגוררים באירופה או מנטרים את התנהגותם.אחד ממושגי המפתח של ה-GDPR הוא הזכות למחיקה, הידועה גם בשם הזכות להישכח. זכות זו מעניקה לאנשים את היכולת לבקש כי המידע האישי שלהם יימחק מרשומותיו של ארגון מסוים. אם אדם מגיש בקשה שכזו, על הארגון הרלוונטי לנקוט צעדים למחיקת המידע ממערכותיו ולמנוע שימוש וחשיפה נוספים של המידע. ייתכנו חריגים לבקשות מצד נושאי מידע. עם זאת, Abbott תעדכן כל נושא מידע שזהותו אומתה לגבי הצעדים שתנקוט בעניין כל בקשה. הפרות של ה-GDPR עלולות לעלות לחברות בקנסות כבדים – עד 4% מהמחזור השנתי הגלובלי שלהן או 20 מיליון אירו (הגבוה מביניהם), בגין העבירות החמורות ביותר. |
| [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 StatesIn 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.CanadaThere 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. | ארה"בבארה"ב, אין חוק אחד ויחיד שמגן על מידע אישי באשר הוא. במקום זאת, קיימים חוקים ותקנות בתחום הפרטיות שחלים על תעשיות וסוגי מידע ספציפיים. לדוגמה, חוק היבילות ואחריות הדיווח של ביטוח בריאות (HIPAA) מגן על פרטיות המידע הנוגע לשירותי הבריאות, בעוד שחוק דיווח האשראי ההוגן מגן על נתוני אשראי.עם זאת, יש מדינות שהחלו לחוקק חוקי פרטיות מידע מקיפים משלהן. לדוגמה, חוק פרטיות הצרכן של קליפורניה (CCPA) מעניק לתושבי קליפורניה זכויות מסוימות על המידע שלהם, למשל הזכות לדעת איזה מידע אישי נאסף עליהם והזכות למחוק כל פרט מידע אישי שנאסף. ה-CCPA יתוקן בשנת 2023 על ידי חוק זכויות הפרטיות של קליפורניה (CPRA), שיעניק לאנשים אפילו יותר זכויות בנוגע למידע שלהם.מדינות אחרות שקבעו חוקי פרטיות מידע משלהן כוללות את וירג'יניה, קולורדו, יוטה וקונטיקט. בזמן שהחוקים משתנים ממדינה למדינה, באופן כללי כל אחד מהם מעניק לאנשים זכויות על המידע שלהם ודורש מחברות לספק גילויים מסוימים לגבי פעילות עיבוד המידע שלהן.הקנסות המוטלים בגין הפרת חוקי פרטיות מדינתיים יכולים להגיע לסכומים משמעותיים. לדוגמה, קליפורניה יכולה לקנוס חברות בסכום של עד 7,500 דולר על כל הפרה של ה-CCPA.קנדהבקנדה קיימים חוקים הן ברמה הפדרלית והן ברמה המחוזית, במטרה להגן על המידע האישי של האדם הפרטי. לדוגמה, החוק בעניין הגנה על מידע אישי ומסמכים אלקטרוניים (PIPEDA) הוא חוק פדרלי שחל על ארגונים במגזר הפרטי ונאכף על ידי משרד נציבות הפרטיות של קנדה.ברמה המחוזית, קוויבק, אלברטה וקולומביה הבריטית חוקקו זה מכבר חוקי פרטיות דומים ל-PIPEDA. בנוסף, ניתן למצוא חוקים שמספקים הגנות דומות על מידע אישי בכמה מחוזות אחרים, לרבות אונטריו, ניו ברונסוויק, ניופאונדלנד ולברדור, ונובה סקוטיה, אשר חוקקו זה מכבר חוקים בנוגע לפרטיות מידע בריאותי.חוקים אלה קיימים כדי לסייע במניעת טיפול שגוי או איסוף מידע אישי ללא ידיעתו של הפרט, וכדי להעניק לאנשים את הזכות לגשת למידע שלהם ולתקן בו שגיאות כלשהן.הפרת חוקים אלה יכולה לגרור קנסות משמעותיים. לדוגמה, הפרת ה-PIPEDA יכולה להסתיים בקנס של עד 100,000 דולר. באלברטה, חוק הגנת המידע האישי (PIPA) מאפשר הטלת קנסות של עד 10,000 דולר ליחידים ו-500,000 דולר לארגונים. |
| [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 PacificThe 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. | אסיה ומדינות האוקיינוס השקטחוקי הפרטיות באזור אסיה והאוקיינוס השקט מתרחבים כל העת והופכים למקיפים יותר ויותר. מדינות מסוימות כמו סין יישמו זה מכבר צעדים ללוקליזציה של מידע, המחייבים חברות לאחסן מידע אישי מסוים בשרתים בגבולותיהן. כמו כן, בסין קיימות דרישות המחייבות הערכה של השפעת הפרטיות והאבטחה בכל הנוגע להעברה חוצת גבולות של מידע אישי.מדינות אחרות, כמו אוסטרליה וסינגפור, אימצו גישה יותר ממוקדת-צרכן לפרטיות המעניקה לאנשים שליטה רבה יותר על המידע שלהם, כולל הזכות לדעת כיצד חברות משתמשות בו והיכולת לגשת ולתקן אותו במידת הצורך.העונשים המוטלים על חברות שמפרות את חוקי פרטיות המידע משתנים אף הם ממקום למקום באזור. בסין, למשל, חברות עשויות לקבל קנס של עד 500,000 רנמינבי (כ-72,000 דולר) בגין הפרת חוקי פרטיות המידע שלה.עם זאת, בסינגפור חברות יכולות להיקנס בסכום של עד מיליון דולר סינגפורי (כ-737,000 דולר אמריקני) בגין הפרת חוק הפרטיות במדינה. |
| [Screen 8](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx?showScreen=13_C_11) [13\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11)  | RussiaRussia 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. | רוסיהרוסיה קבעה חוקים להגנה על המידע של אזרחיה, כולל חוק בעניין לוקליזציית מידע שמחייב חברות לאחסן מידע אישי של אזרחים רוסים בשרתים הממוקמים ברוסיה.החוק חל על חברות שעוסקות בעיבוד מידע של אזרחים רוסים, ללא קשר לשאלה אם החברות האלו מבוססות ברוסיה או לא. כך, לצורך העניין, גם חברה שפועלת מארה"ב ומעבדת מידע של אזרחים רוסים נדרשת לציית לחוק.בדומה למה שקורה במדינות רבות, החוק גם מחייב חברות לנקוט צעדים להגנה על המידע האישי שהן מעבדות. לדוגמה, חברות חייבות לוודא שהמידע מדויק ועדכני ולפעול למניעת טיפול שגוי, אובדן או גניבה.הקנסות בגין הפרת החוק יכולים לנוע בין 12,000 דולר ל-72,000 דולר עבור העבירה הראשונה ועד 216,000 דולר עבור העבירה השנייה. |
| [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 AmericaMost 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. | אמריקה הלטיניתברוב מדינות אמריקה הלטינית קיימים חוקים להגנה על פרטיותם של אנשים פרטיים. עם זאת, מדינות רבות ובהן אקוודור, ארגנטינה וברזיל עדכנו לאחרונה את תקנות הפרטיות שלהן כדי להישאר בסטנדרטים הבינלאומיים העדכניים.כך למשל, אקוודור העבירה לא מזמן את החוק האורגני להגנה על מידע אישי (LPPD), שייכנס לתוקף ב-2023. חוק זה חל על כל חברה ברחבי העולם העוסקת בעיבוד מידע אישי של אנשים פרטיים באקוודור.בדומה לחוקים אחרים באזור, ה-LPPD דורש מחברות לספק הודעה ולהשיג הסכמה מאנשים לפני השימוש במידע שלהם, להשמיד את המידע אם אין בו יותר צורך ולעמוד בהגבלות מסוימות לפני שישתפו את המידע עם מדינות אחרות. אמצעים אלה עוזרים להגן על פרטיותם של אנשים ברחבי אמריקה הלטינית ולהבטיח כי חברות יטפלו במידע האישי בצורה אחראית.הפרת ה-LPPD עלולה לגרור קנסות משמעותיים הנעים בין 3% ל-17% מהתשואות השנתיות של הארגון הרלוונטי מהשנה הקודמת, וכך יש לחברות תמריץ חזק לפעול בתאימות לחוק. |
| [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. | בנוסף לתקנות ולחוקים המסדירים את האופן שבו Abbott מנהלת את עסקיה, היא עשויה לקבל על עצמה התחייבויות נוספות במסגרת חוזים ספציפיים עם לקוחותיה.ממשלת ארה"ב היא לקוחה של Abbott, למשל. כחלק מתנאי ההסכם עימה, אנחנו מחויבים לעמוד בהתחייבויות המוגדרות בחוק הפרטיות של ארה"ב מ-1974.לקבלת מידע נוסף, לחצו על לחצן "חוק הפרטיות". |
| [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 ActThe 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. | חוק הפרטיותחוק הפרטיות מ-1974 (‎5 U.S.C. 552a) הוא תקנה פדרלית חשובה. החוק קובע את קוד ניהול המידע ההוגן המסדיר את האיסוף של מידע המאפשר זיהוי של אדם שנשמר ברשומות הסוכנויות הפדרליות, את תחזוקת המידע, השימוש בו והפצתו. עבור עסקאות מסוימות, Abbott עשויה לקבל גישה לרשומות של סוכנות ממשלתית. במקרים כאלו, על Abbott לעמוד במספר התחייבויות, כולל הצורך להוכיח השלמה של הדרכת פרטיות בנוגע להגנה על מידע המאפשר זיהוי אישי.על עובדי החברה ליצור קשר עם המחלקה המשפטית לפני חתימה על הסכמים עם לקוחות שדורשים התחייבויות לגבי פרטיות. |
| [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. | החוקים, התקנות והדרישות החוזיות שעליהם עברנו זה עתה הם לרוב מורכבים ועשויים להשתנות במהירות.ב-Abbott קיימים מדיניות ונהלים כדי להבטיח שעובדי החברה פועלים על פי החוקים והתקנות האלה. אם יש לכם שאלות או שברצונכם לקבל מידע נוסף, צרו קשר עם משרד האתיקה והציות (OEC) או עם אנשי צוות הפרטיות הגלובלי.לקבלת מספרי יצירת קשר ומידע נוסף, לחצו על סמל המשאבים. |
| [Screen 11](file:///D%3A/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf?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.

COLLECTIONNoticeConsentMANAGEMENTData IntegrityAccess and CorrectionUSAGEDisclosure and UseDISPOSITIONRetention and Disposal | איסוף* הודעה
* הסכמה

ניהול* מהימנות המידע
* קבלת גישה ותיקון

שימוש* חשיפה ושימוש

הסדרה* שמירה וסילוק

המדיניות וההליכים של Abbott להגנה על פרטיות המידע מאורגנים באמצעות מערך עקרונות פשוט. אנחנו קוראים לו "עיצוב לפרטיות".עקרונות אלו נועדו לסייע לעובדים להגן על מידע רגיש בכל שלב של מחזור חיי המידע. כדי להדגים זאת, בואו נבחן באופן ספציפי את תחום המידע האישי.השלב הראשון במחזור חיי המידע הוא איסוף.בשלב זה Abbott משתמשת במגוון שיטות לאסוף מידע אישי. לדוגמה, אנחנו עשויים לבקש מצרכנים לספק פרטי קשר באתר האינטרנט של Abbott, או שאנחנו עשויים לקלוט מידע אישי שנאסף מאחד המכשירים שלנו.כדי להגן על זכויות הפרטיות של אנשים במהלך שלב זה, אנו מפעילים תהליכים כדי להבטיח עמידה בעקרונות של "עיצוב לפרטיות" לגבי הודעה והסכמה.המונח "הודעה" מתייחס לשיתוף האנשים בסוג המידע האישי שנאסף ולהסבר בשפה ברורה, מדויקת וחד-משמעית לגבי האופן שבו אנו מתכננים להשתמש בו.למשל, כאשר מגישים שאילתה באתר abbott.com, נעשה שימוש במידע האישי שאנו אוספים לצורכי מענה על השאילתה בלבד.המונח "הסכמה" מתייחס למתן אפשרות לאנשים להסכים לאיסוף המידע האישי שלהם ולשימוש בו.באופן כללי, כאשר אנו מבקשים הסכמה, אנו מוודאים שהיא:* ניתנת מרצון חופשי. מתן המידע לא נכפה על המסכימים ולא נאמר להם שההסכמה היא דרישה.
* מושכלת. המסכימים קיבלו מידע מספק כדי לקבל החלטה הגיונית לגבי ההסכמה שהם נותנים.
* הסכמה חיובית. על המסכימים לספק הסכמה חיובית. לעולם לא נניח הסכמה שבשתיקה, למשל, או נדרוש מאדם לנקוט בפעולה מסוימות, כגון ביטול סימון תיבה, כדי להורות שהוא אינו מסכים לדבר כלשהו.
* ברת-ביטול. המסכימים מקבלים הסבר ברור לגבי האופן שבו ניתן לבטל הסכמה.

לדוגמה, צרכן שנרשם לתוכנית ההטבות Strong Moms©‎ של Abbott Nutrition Similac©‎ יכול להסכים לאיסוף המידע האישי שלו ולשימוש בו על-ידי בחירה (למשל על-ידי סימון תיבה בטופס) באפשרות לקבל מידע שיווקי נוסף.השלב השני במחזור חיי המידע הוא ניהול.במהלך שלב זה המידע מעובד ומאוחסן.כדי להגן על המידע האישי בשלב זה אנו מיישמים תהליכים שיבטיחו עמידה בעקרונות הבאים:* מהימנות המידע, וכן
* קבלת גישה ותיקון.

הכוונה ב"מהימנות המידע" היא לנקוט באמצעים סבירים כדי להבטיח שהמידע האישי שבו אנו מחזיקים הוא מדויק, שלם ומעודכן.אחת הדרכים שבה אנו נוקטים היא מעקב ורישום של כל הפעילויות המעבדות מידע אישי. כך נבטיח שנוכל לזהות את מקור המידע, את המטרה הספציפית שעבורה נאסף המידע ואת מקום האחסון שלו.הכוונה ב"גישה ותיקון" היא לספק לאנשים גישה סבירה למידע שלהם ואפשרות לממש את זכויותיהם בקשר למידע זה.הדבר כולל מענה לבקשתו של אדם לגשת לרשומות המידע האישי המאוחסנות, למחוק אותן, להעביר אותן או לתקן אותן.השלב השלישי במחזור החיים הוא שימוש.בשלב זה נעשה שימוש במידע האישי לצורך תמיכה בפעילויות ברחבי הארגון.כדי להגן על המידע האישי בשלב זה אנו מיישמים תהליכים שיבטיחו עמידה בעקרונות של חשיפה ושימוש.הכוונה ב"חשיפה ושימוש" היא לשלוט בגישה למידע האישי ולהגביל את השימוש בו למטרות ספציפיות.אנו מנהלים זאת באמצעות בקרות גישה ותהליכים נוספים. בקרות ותהליכים אלו מגבילים את הגישה ליחידים בעלי תפקידים מסוימים, וכמו כן הם מגבילים את השימוש למטרות ספציפיות שהוגדרו בהודעה שעבורה ניתנה ההסכמה.השלב האחרון במחזור חיי המידע הוא הסדרה."הסדרה" מתייחסת למה שקורה למידע כאשר אין בו צורך יותר. פעולות הסדרה עשויות לכלול מחיקה, גניזה או החזקה לצרכים משפטיים.כדי להגן על המידע האישי בשלב זה, אנו מיישמים מדיניות ותהליכים שמבטיחים עמידה בעיקרון השמירה והסילוק.הכוונה ב"שמירה וסילוק של מידע אישי" היא שמירה על המידע האישי רק כל עוד הדבר הכרחי להשגת המטרות שלשמן הוא נדרש ועובד.כאשר אין יותר צורך במידע אישי בסביבת ייצור פעילה, קיימים תהליכים ש-Abbott קבעה לטובת גניזה או סילוק התואמים את דרישות החברה לניהול מידע, שמירתו וסילוקו. דרישות השמירה והסילוק שלנו כפופות גם לכל דרישת החזקה הקשורה לעניינים משפטיים.לקבלת מידע נוסף בקשר לדרישות השמירה והסילוק, ראו את מדיניות הרשומות והמידע הגלובלית של Abbott ‏(l1-02) או צרו קשר עם מחלקת ניהול המידע והרשומות. ניתן למצוא פרטים נוספים בחלק "משאבים" של הדרכה זאת.לקבלת מספרי יצירת קשר ומידע נוסף, לחצו על סמל המשאבים.כפי שראינו, המדיניות והנהלים שלנו נועדו להגן על המידע האישי במהלך מחזור החיים שלו.אנו מיישמים זאת באמצעות שמירה על העקרונות הבאים:* הודעה,
* הסכמה,
* מהימנות המידע,
* קבלת גישה ותיקון,
* חשיפה ושימוש, וכן
* שמירה וסילוק.

איסוףהודעההסכמהניהולמהימנות המידעקבלת גישה ותיקוןשימושחשיפה ושימושהסדרהשמירה וסילוק |
| [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.ReviewTake 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 LawsPrivacy laws differ from one country to the next, but often embrace the same core principles.Abbott’s Privacy by Design PrinciplesAbbott’s data privacy and protection policies and procedures are organized around a set of principles, called Privacy by Design.Notice and ConsentNotice and Consent is about letting people know what PI is being collected and providing them the opportunity to agree to that collection.Data IntegrityData Integrity is about taking reasonable measures to ensure that PI is accurate, complete, and current.Access and CorrectionAccess and Correction is about providing individuals the right to access and correct their data.Disclosure and UseDisclosure and Use is about controlling who has access to PI.Retention and DisposalRetention 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 buttonGreat job!You have completed section 1 of 4Click the forward arrow to continue learning | לחצו על החץ כדי להתחיל את הסקירה שלכם.סקירההקדישו רגע כדי לעבור על כמה מהמושגים המרכזיים שנכללו בחלק זה.מידע אישי (PI)מידע אישי הוא כל מידע שבו ניתן להשתמש כדי* ליצור קשר עם אדם
* לאתרו או
* לזהותו.

מידע בריאות מוגן (PHI)מידע בריאות מוגן הוא סוג רגיש במיוחד של מידע אישי שבו משתמשים בענף הבריאות.חוקי פרטיותחוקי הפרטיות משתנים ממדינה למדינה, אבל עקרונות היסוד שלהם זהים לעתים קרובות.עקרונות "עיצוב לפרטיות" של Abbottהמדיניות וההליכים של Abbott בעניין פרטיות והגנה על מידע מאורגנים באמצעות מערך עקרונות הנקרא "עיצוב לפרטיות".הודעה והסכמההכוונה ב"הודעה והסכמה" היא לעדכן אנשים מהו המידע הפרטי שנאסף ולתת להם את ההזדמנות להסכים לאיסוף זה.מהימנות המידעהכוונה ב"מהימנות המידע" היא לנקוט באמצעים סבירים כדי להבטיח שהמידע האישי מדויק, שלם ומעודכן.קבלת גישה ותיקוןהכוונה ב"גישה ותיקון" היא לספק לאנשים את הזכות לגשת למידע שלהם ולתקנו.חשיפה ושימושהכוונה ב"חשיפה ושימוש" היא לשלוט בגישה למידע האישי.שמירה וסילוקהכוונה ב"שמירה וסילוק של מידע אישי" היא לשמור על המידע האישי רק כל עוד הדבר הכרחי להשגת המטרות שלשמן הוא נדרש ועובד.כדי לבדוק את ההתקדמות שלכם, לחצו על לחצן התפריטמעולה!השלמתם את חלק 1 מתוך 4לחצו על החץ קדימה כדי להמשיך ללמוד |
| [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. | סוג נוסף של מידע רגיש שבו אנו עושים שימוש תכוף הוא מידע עסקי חסוי.מידע עסקי חסוי הוא קטגוריה רחבה. הוא כולל את רוב המידע העסקי שבו אנו משתמשים ושאיתו אנו באים במגע באופן יומיומי. מידע חסוי הוא מידע שאינו זמין לציבור ושיש בו כדי להועיל למתחריה של Abbott או להזיק ל-Abbott במקרה של חשיפה. |
| [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. | קנדיס | מנהלת שיווק אוכל לקבל כמה דוגמאות למידע עסקי חסוי?מידע עסקי חסוי עשוי לכלול, בין היתר: עיצוב מוצר ותהליכיו, הרכבים, אורגניזמים, תוכנות מחשב, נתוני מחקר ופיתוח, נתונים קליניים ופרמקולוגיים, נתוני מטופלים, נתונים טכניים, רשימות של לקוחות ולקוחות פוטנציאליים, שיטות עסקיות, תוכניות ואסטרטגיות שיווק, נתונים פיננסיים ותפעוליים, ונתוני אנשי צוות.הוא עשוי לכלול גם מידע הקשור לרכש, כגון הצעות מכרז לחוזים, רשימות ספקים ומידע על עלויות. |
| [Screen 15](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?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.
 | ג'רי | נציג מכירות האם ישנם סוגי מידע עסקי חסוי שהם רגישים יותר מאחרים?כן. סוגים מסוימים של מידע עסקי חסוי מחייבים טיפול קפדני יותר מהרגיל משום שחשיפה בלתי ראויה של מידע זה או שימוש בלתי ראוי בו עלולים לגרום לנזק משמעותי לחברה.הדוגמאות כוללות:* סודות מסחריים, נוסחאות ייצור ותהליכים;
* מידע קליני ורגולטורי, הגשות רגולטוריות, או מידע טרום-אישור, וגם
* מידע פיננסי שעדיין לא פורסם לציבור.
 |
| [Screen 16](http://abbottmfiles.oneabbott.com/?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. | כפי שראיתם, רוב המידע העסקי שאנו משתמשים בו בעבודה היומיומית שלנו נחשב חסוי.דרך טובה לוודא אם המידע העסקי שאתם משתמשים בו הוא חסוי היא לשאול את עצמכם שאלה פשוטה:האם מידע זה זמין לציבור?אם התשובה היא לא, על המידע להיחשב חסוי ויש לנקוט בצעדים המתאימים כדי להגן עליו. |
| [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. | כמו כן, חשוב לזכור כי כל מידע עסקי חסוי שנוצר כחלק מעבודתכם ב-Abbott הוא רכושה של Abbott.כתוצאה, עליכם להגן על מידע זה ואינכם יכולים לשמור אותו במקרה שאתם מסיימים את עבודתכם ב-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. | ההגנה על מידע עסקי חסוי היא פעולה חיונית.שלא במפתיע, שימוש לא ראוי במידע זה או חשיפתו עלולים לגרום לפגיעה משמעותית מבחינת 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. | שימוש לא ראוי במידע חסוי או חשיפתו עלולים לגרום לפגיעה משמעותית ביחסיה של Abbott עם לקוחותיה, לסיקור מביך בתקשורת, ולאובדן יתרונות תחרותיים מבחינת Abbott. הדבר אף יכול לגרור תביעות אזרחיות וענישה פלילית, לרבות נגד עובדים בהווה ובעבר.לחצו על לחצן "מקרים מהזמן האחרון" לקבלת מידע נוסף. |
| [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 CASESIn 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. | מקרים מהזמן האחרוןבשנים האחרונות, חברות קיבלו פסקי דין ופיצויים שנקבעו על ידי חבר מושבעים גדול נגד עובדים לשעבר בגין לקיחה בלתי ראויה של מידע השייך להן. לדוגמה, לטובת חברה אחת נפסקו פיצויים בגובה 240 מיליון דולר נגד עובד לשעבר שחשף באופן לא ראוי את המידע החסוי שלה בפני מתחרה. במקרה של חברה אחרת, חבר המושבעים פסק פיצוי בגובה 854 מיליון דולר נגד אחד מעובדיה לשעבר ומעסיקו החדש, זאת לאחר שהראשון ניצל את המידע החסוי של החברה ולאחר מכן השתמש בו בשם מעסיקו החדש.מחקרים מצביעים על כך שגניבת מידע חסוי גורמת לחברות ציבוריות הפסדים שנעים בין 209 ל-625 מיליארד דולר. |
| [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. | אין זה מפתיע שהרשויות מתייחסות ברצינות רבה לגניבת מידע חסוי.לדוגמה, על פי חוקי העונשין של הממשל הפדרלי, אדם עשוי להיות צפוי למאסר של עד עשר שנים ולקנס של 5 מיליון דולר בגין גניבת מידע חסוי. בנוסף, במקרה שחברה נמצאת אשמה בגניבת מידע חסוי, היא עשויה להיקנס ב-10 מיליון דולר או בסכום העומד על פי 3 מערך המידע החסוי.לחצו על לחצן "קנסות ועונשים" לקבלת מידע נוסף. |
| [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 PENALTIESIn 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.
 | קנסות ועונשיםבשנים האחרונות, מספר אנשים וחברות נקנסו או נידונו למאסר בגין גניבת מידע חסוי. לדוגמה:* מתחרה נקנס ב-60 מיליון דולר בגין גניבת מידע חסוי של חברה אחרת;
* עובד IT לשעבר נידון ל-97 חודשי מאסר בגין גניבת מידע חסוי;
* איש מכירות לשעבר נידון ל-12 חודשי מאסר בגין גניבת מידע חסוי;
* מנהל בכיר נידון ל-24 חודשי מאסר בגין גניבת מידע חסוי; וכן
* מדען-חוקר נידון ל-18 חודשי מאסר בגין גניבת מידע חסוי.
 |
| [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. | סוג נוסף של מידע עסקי חסוי שחשוב להכירו ולהגן עליו הוא *מידע פנים*.מידע פנים הוא מידע מהותי שאינו נחלת הציבור אשר, אם ייחשף בצורה פומבית, עלול ככל הנראה להשפיע על ערך השוק של ניירות הערך של החברה או להשפיע על החלטות המשקיעים אם לקנות או למכור ניירות ערך. |
| [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.
 | דוגמאות למידע פנים כוללות:* חדשות על רכישות פוטנציאליות,
* עיכוב בהשקת מוצר,
* חדשות על חדירה למערכות טכנולוגיית מידע (IT) פנימיות,
* שינויים בלתי צפויים בהכנסות או בשיעורי הדיבידנדים,
* הצעות למכרזים או לפיצול מניות,
* מידע בנוגע למוצרים חשובים חדשים,
* זכייה בחוזים,
* תוכניות התרחבות,
* התדיינות משפטית משמעותית או תביעה משפטית בענייני רגולציה, וכו'.
 |
| [Screen 23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23) [32\_C\_23](http://abbottmfiles.oneabbott.com/Default.aspx?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. | אם אתם מודעים למידע פנים או שבידיכם מידע כזה, אסור לכם לסחור בניירות ערך של Abbott או להמליץ לאחרים לסחור בהן.הדבר כולל קנייה ומכירה של ניירות ערך של חברות אחרות, כולל חברות שכרגע מנהלות עסקים או צפויות לנהל עסקים עם Abbott.לקבלת מידע נוסף על הציפיות של חברת Abbott בנוגע לשימוש במידע שטרם פורסם או להגנה עליו, אפשר לעיין במדיניות החברה בנוגע לשימוש במידע פנים. ניתן למצוא פרטים נוספים בחלק משאבים של הדרכה זאת. |
| Screen 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.ReviewTake a moment to review some of the key concepts covered in this section.Confidential Business InformationAny 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 InformationThe improper use or disclosure of confidential business information can result in significant harm to the Company, our customers and employees.Insider InformationInsider 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 buttonGreat job!You have completed section 2 of 4Click the forward arrow to continue learning | לחצו על החץ כדי להתחיל את הסקירה שלכם.סקירההקדישו רגע כדי לעבור על כמה מהמושגים המרכזיים שנכללו בחלק זה.מידע עסקי חסויכל מידע עסקי שאינו זמין לציבור צריך להיחשב כחסוי. בכך נכלל חלק גדול מהמידע העסקי שמשמש אותנו בעבודתנו היומיומיות.שימוש בלתי ראוי במידע עסקי חסוישימוש בלתי ראוי במידע עסקי חסוי או חשיפתו עלולים לגרום נזק משמעותי לחברה, ללקוחותינו ולעובדים שלנו.מידע פניםמידע פנים הוא מידע מהותי שאינו נחלת הציבור אשר, אם ייחשף בצורה פומבית, עלול ככל הנראה להשפיע על ערך השוק של ניירות הערך של החברה או להשפיע על החלטות המשקיעים אם לקנות או למכור ניירות ערך.כדי לבדוק את ההתקדמות שלכם, לחצו על לחצן התפריטמעולה!השלמתם את חלק 2 מתוך 4לחצו על החץ קדימה כדי להמשיך ללמוד |
| [Screen 25](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx?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. | כעת, כשאתם מכירים את סוגי המידע השונים שסביר כי תיתקלו בהם במהלך יום העבודה שלכם, אלה הצעדים שתוכלו לנקוט כדי לסייע להגן עליהם. |
| [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. | לפני שאתם ניגשים למידע רגיש כלשהו, ודאו שתפקידכם ותחומי האחריות שלכם מצריכים את גישתכם אליו.אם יש לכם שאלה בקשר לרשות הגישה למידע, במיוחד כשמדובר במידע אישי, פנו למנהלים שלכם, למשרד האתיקה והציות או לצוות הפרטיות הגלובלי.לחצו על לחצן "הידעתם" לקבלת מידע נוסף. |
| [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 KNOWAbbott 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. | הידעתם?Abbott עוסקת בצורות שונות של ניטור חוקי להפחתת הסיכון לשימוש לא ראוי במידע.בכך נכלל ניטור של הורדת מידע או של שליחת מידע לכתובות דוא"ל שאינן שייכות ל-Abbott. |
| [Screen 27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27) [37\_C\_27](http://abbottmfiles.oneabbott.com/Default.aspx?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. | אם מותר לכם לגשת למידע רגיש, השתמשו בו אך ורק למטרה שלשמה קיבלתם את הגישה.אם מדובר במידע אישי, השתמשו בו אך ורק בהתאם להסכמה שניתנה או להודעה שפורסמה. |
| [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. | לפני שאתם משתפים מידע רגיש, ודאו שלאדם שעימו אתם מתכננים לשתף יש הרשאה מתאימה.אם יש לכם שאלות בקשר לרשות הגישה למידע, במיוחד כשמדובר במידע אישי, פנו למנהלים שלכם או לצוות הפרטיות הגלובלי. |
| [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 CountryIf 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. | בקשות המגיעות מהמדינה שלכםאם עובד של Abbott מאותה מדינה כמו שלכם מבקש מידע רגיש, תמיד:* ודאו את זהות האדם שמגיש את הבקשה;
* ודאו שיש לו צורך בגישה למידע;
* ודאו שהמבקש מורשה לקבל את המידע;
* ודאו שניתן להשתמש במידע לטובת הצורך שלשמו ביקשו אותו; וכן
* שתפו את המידע אך ורק במידה הדרושה, ולא מעבר לכך.

במקרה של ספק, צרו קשר עם משרד האתיקה והציות לפני שאתם משתפים מידע רגיש. |
| [Screen 30](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx?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 CountriesMany 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. | בקשות המגיעות ממדינות אחרותבמדינות ובאזורים רבים קיימים חוקים שנועדו להגן על זכויות האזרחים שלהם והם מטילים מגבלות על ההעברה של מידע אישי למדינות אחרות.אם אתם מקבלים בקשה למידע הכולל מידע רגיש מעמית הנמצא במדינה אחרת, בדקו את מדיניות פרטיות המידע של החטיבה או התפקיד שלכם או התייעצו עם משרד האתיקה והציות או עם צוות הפרטיות הגלובלי לפני שתמשיכו. לאחר מכן, בצעו את אותן פעולות שהייתם מבצעים אם הייתם משיבים לבקשה שהגיעה מעמית לעבודה במדינה שלכם. |
| [Screen 31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33) 41\_C\_33  | Requests from Third PartiesIf 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. | בקשות המגיעות מצדדים שלישייםאם הבקשה למידע רגיש מגיעה מצד שלישי, ודאו שקיים הסכם חוזי מתאים ובר-תוקף עם המבקש. במקרה של ספק, צרו קשר עם משרד האתיקה והציות או המחלקה המשפטית לפני השיתוף. |
| [Screen 32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35) [42\_C\_35](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx?showScreen=42_C_35)  | Always archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements. | תמיד גנזו מידע רגיש או היפטרו ממנו באופן שתואם את הדרישות של חברת Abbott לניהול, לשמירה ולסילוק של המידע. |
| [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. | אם אתם מקבלים הוראה להחזקת מידע לצרכים משפטיים, נאסר עליכם להיפטר ממידע כלשהו שנכלל בהוראה, להרוס אותו למחוק אותו.אם יש לכם שאלות בקשר להוראת החזקה משפטית או לשמירה וסילוק, צרו קשר עם עורכי הדין/העוזרים המשפטיים ששמותיהם מופיעים בהודעת הצו המשפטי או התקשרו למחלקת הליטיגציה בטלפון ‎(224) 667-5701. |
| [Screen 34](http://abbottmfiles.oneabbott.com/?showScreen=44_C_37) [44\_C\_37](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx?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. | תמיד היזהרו במיוחד בנוגע למידע רגיש כאשר מישהו עוזב את Abbott.על המנהלים לוודא כי העובד העוזב מוגדר כמי שהעסקתו הסתיימה במערכת המתאימה (למשל, Workday לעובדים או Fieldglass לעובדים זמניים) עם קבלת ההודעה על עזיבתו. פעולה זו תבטיח שהגישה לנתוני Abbott, הגישה הפיזית לבניינים והשכר הסופי ינוהלו כראוי. |
| [Screen 35](http://abbottmfiles.oneabbott.com/Default.aspx?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. | ודאו כי העובד שעוזב לא לוקח עימו כל מידע רגיש. העבירו את כל המסמכים לעובד Abbott שיבוא במקומו של העובד שעוזב.הזכירו לעובד העוזב את מחויבותו לאי שמירת מידע רגיש ואי חשיפתו. עובדים אינם רשאים לקחת עימם את תוצרי העבודה שלהם או כל רכוש אחר השייך ל-Abbott (למשל מכשירים ניידים) כאשר הם עוזבים את החברה. אם יש לכם שאלות כלשהן לגבי תהליך סיום ההעסקה המקומי שלכם, צרו קשר עם מחלקת משאבי האנוש. |
| [Screen 36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38) [46\_C\_38](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf?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. | חשיפה לא מכוונת של מידע בריאות מוגן יכולה להתרחש בכל עת.לדוגמה, אתם עשויים לשמוע במקרה אחות מדברת על מצבו הרפואי של מטופל או להיות מכותבים בטעות על דוא"ל המכיל פרטים מתיקו של מטופל. |
| [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. | בתגובה לכל חשיפה לא מכוונת או לא ראויה של מידע בריאות מוגן של מטופל (PHI), עליכם לדווח על התקרית למקורות באופן מיידי למשרד האתיקה והציות או לצוות הפרטיות הגלובלי. |
| [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. | אם אתם מקבלים ידיעה על כל חשיפה בלתי ראויה או לא מכוונת של מידע עסקי חסוי, עליכם לדווח עליה מיידית לשני הגורמים הבאים:* המנהל/ת הישיר/ה שלכם, וכן
* משרד האתיקה והציות או אנשי צוות הפרטיות הגלובלי.

הדיווח המיידי שלכם על החשיפה יסייע ל-Abbott לאחזר את המידע באופן מיידי, למנוע תקלות נוספות או שימוש לרעה במידע, ובמידת הצורך יעזור לחברה בנקיטת צעדים אזרחיים או פליליים. |
| [Screen 39](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c) [49\_C\_38c](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx?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. | לעולם אל תחשפו נתונים רגישים של Abbott בפני מי שאינו מורשה לקבלם.באופן דומה, עליכם להשתמש בנתונים רגישים של Abbott אך ורק מטעמה ובמהלך ביצוע תפקידכם העסקי במסגרת עבודתכם ב-Abbott.אם תחשפו מידע רגיש באופן לא ראוי, ייתכן שתעמדו בפני צעדים משמעתיים, עד וכולל סיום העסקה. |
| [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. | אינכם מורשים, לא במהלך עבודתכם ב-Abbott ולא לאחר מכן, לשתף מידע של Abbott עם מי מבין מתחריה. |
| [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. | אי החזרת מידע רגיש ל-Abbott, העברת מידע רגיש למכשיר, לאמצעי אחסון, לחשבון או לשרת בלתי מורשים, או מסירת מידע רגיש לכל אדם או ישות שאינם מורשים להחזיק בו, יכולים להוביל לכך ש-Abbott תנקוט צעדים משפטיים נגדכם.לחצו על לחצן "צעדים משפטיים" לקבלת מידע נוסף. |
| [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 ACTIONLegal 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. | צעדים משפטייםנקיטת צעדים משפטיים עשויה לכלול הגשת תביעה אזרחית נגדכם מטעם Abbott, אשר עלולה:* למנוע מכם לעבוד אצל מעסיק חדש עד שהמידע הרגיש יוחזר ל-Abbott ויהיה מוגן;
* לדרוש מכם להעביר ל-Abbott כל מכשיר אלקטרוני לצורך סקירה ובדיקה;
* לגרום לכם לשלם פיצויים כספיים בגין החזקה ו/או שימוש לא חוקיים במידע רגיש של Abbott והפרת החובות וההתחייבויות שלכם כלפי Abbott כפי שהם מופיעים בהסכם ההעסקה שלכם עבור Abbott; וכן
* לחייב אתכם בתשלום ההוצאות המשפטיות שיוטלו על Abbott כתוצאה מהגשת תביעה שנועדה להגן על המידע הרגיש שלה.

במידת הצורך, Abbott תעבוד גם עם רשויות מקומיות, ממלכתיות ופדרליות כדי להגן על המידע הרגיש שלה. בתרחיש זה, אתם אף עלולים לעמוד בפני עונשים פליליים. |
| Screen 42 [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. | יש לדווח מייד על כל אירוע המערב פגיעה אפשרית באבטחת מידע, כולל אובדן או גניבה של מכשיר נייד, לנציגות המקומית של מוקד השירות העולמי.אם יש לכם חשש כלשהו לגבי הפרה פוטנציאלית או שברצונכם לדווח על תקרית פוטנציאלית בעניין פרטיות, צרו קשר עם צוות הפרטיות הגלובלי. |
| [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.ReviewTake a moment to review some of the key concepts covered in this section.Accessing and Using Sensitive DataOnly access and use sensitive data for the specific purpose for which you have been granted access.Sharing Sensitive DataBefore 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 DataAlways archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements.Responding to Inadvertent Disclosure of PHIIn 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 IncidentContact the Global Privacy team to report a potential privacy incident.To check your progress, click the Menu buttonGreat job!You have completed section 3 of 4Click the forward arrow to continue learning | לחצו על החץ כדי להתחיל את הסקירה שלכם.סקירההקדישו רגע כדי לעבור על כמה מהמושגים המרכזיים שנכללו בחלק זה.גישה למידע רגיש ושימוש בוגשו למידע רגיש והשתמשו בו אך ורק למטרה שלשמה קיבלתם את הגישה אליו.שיתוף מידע רגישלפני שיתוף מידע רגיש:* ודאו את זהות המבקש;
* ודאו שיש לו צורך בגישה למידע;
* ודאו שניתן להשתמש במידע לטובת הצרכים שלשמם ביקשו אותו; וכן
* שתפו אך ורק את מה שנדרש כדי לענות על הצורך במידע.

שמירת מידע רגיש והסרתותמיד גנזו מידע רגיש או היפטרו ממנו באופן שתואם את הדרישות של חברת Abbott לניהול, לשמירה ולסילוק של המידע.תגובה לחשיפה לא מכוונת של מידע בריאות מוגןבתגובה לכל חשיפה לא מכוונת או לא ראויה של מידע בריאות מוגן השייך למטופלים, דווחו מייד על החשיפה למשרד האתיקה והציות או לצוות הפרטיות הגלובלי.דיווח על תקרית בעניין פרטיותצרו קשר עם צוות הפרטיות הגלובלי כדי לדווח על תקרית פוטנציאלית בעניין פרטיות.כדי לבדוק את ההתקדמות שלכם, לחצו על לחצן התפריטמעולה!השלמתם את חלק 3 מתוך 4לחצו על החץ קדימה כדי להמשיך ללמוד |
| [Screen 44](https://icomply.abbott.com/Default.aspx?showScreen=55_C_45) [55\_C\_45](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf?showScreen=55_C_45)  | Where to Get HelpOffice of Ethics and Compliance (OEC)Global Privacy – Contact Global Privacy via email at [privacy@abbott.com](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html). You can find additional contact details and important information about privacy on the Global Privacy Portal [here](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.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](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) on Abbott World or [OEC@abbott.com](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html).

ENTERPRISE CYBERSECURITYVisit the Enterprise Cybersecurity site [here](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) on Abbott World.Visit the [Simply Digital](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) site to learn about secure ways to share information.Legal DivisionContact the [Legal Division](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?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](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) with questions or concerns regarding retention requirements or for guidance on acceptable use of technology solutions.REFERENCE POLICIES:* Click [here](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html#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](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) to review Abbott’s policy on Insider Trading
* Click [here](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html#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](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/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 ProceduresFor 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://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) for a list of HR support contact numbers.

Course ResourcesTranscriptClick [here](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) for a full transcript of the course. | לאן לפנות לעזרהמשרד האתיקה והציות (OEC)צוות הפרטיות הגלובלית – צרו קשר עם צוות הפרטיות גלובלית באמצעות שליחת דוא"ל לכתובת [privacy@abbott.com](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html). ניתן למצוא פרטים נוספים ליצירת קשר ומידע חשוב נוסף בנושאי פרטיות בפורטל הפרטיות הגלובלי [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) ב-Abbott World.אנשי קשר במשרד האתיקה והציות – אל תהססו לפנות למשרד האתיקה והציות בכל עת ועם כל שאלה בנושאי אתיקה וציות, או כדי לשוחח על חששות להפרות אפשריות של הסטנדרטים, החוקים והתקנות הכתובים שלנו.* בקרו בעמוד [יצירת קשר עם משרד האתיקה והציות (OEC)](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) שנמצא [באתר משרד האתיקה והציות](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) שב-Abbott World, או צרו קשר בכתובת [OEC@abbott.com](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html).

אבטחת סייבר תאגידיתבקרו באתר אבטחת הסייבר התאגידית [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) ב-Abbott World.בקרו באתר [Simply Digital](http://abbottmfiles.oneabbott.com/Default.aspx) לקבלת מידע נוסף על דרכים מאובטחות לשיתוף מידע.המחלקה המשפטיתצרו קשר עם [המחלקה המשפטית](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) למענה על שאלות או חששות בקשר להתחייבויות חוזיות עם צדדים שלישיים בנוגע לפרטיות ולהגנה על מידע.צרו קשר עם צוות ניהול מידע בכתובת [information.governance@abbott.com](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) למענה על שאלות או חששות בקשר לדרישות שמירה או להנחיות בנוגע לשימוש קביל בפתרונות טכנולוגיים.הפניות למסמכי מדיניות:* לחצו [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html#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) כדי לעיין במדיניות בעניין מידע חסוי.
* לחצו [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) כדי לעיין במדיניות השימוש במידע פנים של Abbott.
* לחצו [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0) כדי לעיין במדיניות השימוש הקביל בטכנולוגיה.
* לחצו [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0) כדי לעיין במדיניות הרשומות והמידע בנוגע ל-M-Files.

לכללי המדיניות והנהלים של משרד האתיקה והציות (OEC)למדיניות ולנוהלי משרד האתיקה והציות הגלובליים והייחודיים לכל מדינה של החברה:* מומלץ לעובדי Abbott לבקר באתר [iComply](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html).

מרכז השירות של מחלקת משאבי אנוש* לחצו [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) לקבלת רשימת מספרי הקשר לתמיכה מטעם מחלקת משאבי אנוש.

מקורות הקורסתמליללחצו [כאן](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html) כדי לקבל תמליל מלא של הקורס. |
| [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. | בדיקת הידע להלן מורכבת מ-10 שאלות. עליכם להשיג ציון של 80% ומעלה כדי להשלים בהצלחה את הקורס.כשתהיו מוכנים, לחצו על לחצן **בדיקת ידע**. |
| Screen 46Question 1: Scenario57\_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? | נניח שעבדתם עבור Abbott מספר שנים ולא מזמן קיבלתם הצעה לעבוד בחברה אחרת, איזה מהדברים הבאים החוק מתיר לכם לקחת בעת עזיבתכם? |
| Screen 46Question 1: Options58\_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] מידע אישי של מטופלים מתוך מחקרים קליניים[2] רשימות של לקוחות Abbott ומידע המופיע במצגות שיצרתם במהלך עבודתכם עבור החברה[3] תחזיות של מכירות ונתונים פיננסיים הנוגעים לחטיבה או ליחידה העסקית שלכם ב-Abbott[4] תמונות ומזכרות אישיות |
| Screen 46Question 1: Feedback59\_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.  | התשובה הנכונה היא 4. מידע אישי, מידע עסקי חסוי ומידע בריאות מוגן נחשבים כולם למידע רגיש שאינכם יכולים לקחת עימכם או לעשות בו שימוש לאחר שאתם עוזבים את Abbott. בנוסף, עליכם להחזיר כל מכשיר אלקטרוני ורכוש אחר של Abbott לפני עזיבתכם.לקבלת מידע נוסף, ראו את חלק 3.4, תגובה לחשיפות בלתי ראויות.  |
| Screen 46Question 2: Scenario60\_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. | מנהל שיווק עובד על השקת מוצר חדש ועליו ליצור טופס הסכמה עבור לקוחות פוטנציאליים. הטופס יאפשר איסוף של מידע אישי ושימוש בו. כדי ליישר קו עם נוהלי ההסכמה של Abbott, מה מהבאים חייב להיות נכון לגבי טופס ההסכמה?סמנו את כל מה שרלוונטי. |
| Screen 46Question 2: Options61\_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] אסור שהטופס יפעיל לחץ על לקוחות לתת את הסכמתם.[2] על הטופס לספק ללקוחות את כל המידע על אופן השימוש בנתונים האישיים שלהם.3] הטופס חייב לכלול אפשרות הסכמה אקטיבית מצד הלקוחות לאיסוף המידע האישי שלהם ולשימוש בו.[4] אסור שהטופס יאפשר ללקוחות לחזור בהם מהסכמתם לאחר שנתנו אותה. |
| Screen 46Question 2: Feedback62\_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.  | נוהלי ההסכמה של Abbott דורשים כי הטופס:* יהיה ברור ותמציתי.
* לא ילחץ על אנשים לתת את הסכמתם.
* יספק את כל המידע על אופן השימוש במידע האישי.
* יכלול אפשרות של הלקוחות להסכים באופן אקטיבי לאיסוף המידע האישי שלהם ולשימוש בו.
* יאפשר את ביטול ההסכמה אם הלקוחות ירצו בכך.

לקבלת מידע נוסף, ראו את חלק 1.3, 'עקרונות עיצוב לפרטיות של Abbott'.  |
| Screen 46Question 3: Scenario63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | החשיפה של מידע רגיש כמו מידע אישי והשימוש בו מנוהלים ב-Abbott באמצעות: |
| Screen 46Question 3: Options64\_C\_48 | [1] De-identification of all data.[2] Access controls.[3] Both 1 and 2. | [1] ביטול הפרטים המזהים של כל המידע.[2] בקרות גישה.[3] גם 1 וגם 2. |
| Screen 46Question 3: Feedback65\_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.  | החשיפה של מידע אישי והשימוש בו מנוהלים באמצעות בקרות גישה ותהליכים נוספים, המגבילים את הגישה והשימוש לנושאי תפקידים מסוימים ולמטרות ספציפיות שהוגדרו בהודעה שעבורה ניתנה ההסכמה.לקבלת מידע נוסף, ראו את חלק 1.3, 'עקרונות עיצוב לפרטיות של Abbott'.  |
| Screen 46Question 4: Scenario66\_C\_48 | Which of the following is true in relation to the retention and disposal of personal information?Check all that apply. | מה מהבאים נכון ביחס לשמירת מידע אישי וסילוקו?סמנו את כל מה שרלוונטי. |
| Screen 46Question 4: Options67\_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] המידע האישי נשמר רק כל עוד הוא נדרש כדי להשיג את המטרות שלשמן הוא נאסף ועובד.[2] כאשר אין יותר צורך במידע בסביבת העבודה הפעילה, יש להיפטר ממנו תמיד.[3] השמירה והסילוק של מידע אישי כפופים לכל תקנות ההחזקה לצרכים משפטיים. |
| Screen 46Question 4: Feedback68\_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. | באופן כללי, Abbott שומרת מידע אישי רק כל עוד הוא נדרש כדי להשיג את המטרות שלשמן הוא נאסף ועובד. כאשר אין יותר צורך במידע בסביבת ייצור פעילה, יש לגנוז או לסלק את המידע באופן התואם את הדרישות של Abbott לניהול, לשמירה ולסילוק של המידע. דרישות השמירה והסילוק שלנו כפופות לכל תקנות ההחזקה לצרכים משפטיים.לקבלת מידע נוסף על התשובה הנכונה ראו את חלק 1.3, 'עקרונות עיצוב לפרטיות של Abbott'. |
| Screen 46Question 5: Scenario69\_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. | מהנדסת עובדת על פיתוח מוצר חדש. מה מהבאים ייחשב למידע עסקי חסוי שיש לאבטחו?סמנו את כל מה שרלוונטי. |
| Screen 46Question 5: Options70\_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] תחזיות לגבי מכירות ותחזיות לגבי המוצר החדש.[2] נתוני דוחות פיננסיים מתוך הדוח השנתי של חברת Abbott.[3] מידע על רכש, כגון מכרזים לחוזים עבור המוצר החדש.[4] מידע תחרותי אודות מוצרים דומים.[5] הצעות של ספקי צד שלישי בקשר למוצר החדש. |
| Screen 46Question 5: Feedback71\_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. | מידע עסקי חסוי הוא קטגוריה רחבה. הוא כולל את רוב המידע העסקי שבו אנו משתמשים ושאיתו אנו באים במגע באופן יומיומי. דרך טובה לוודא אם משהו הוא חסוי היא לשאול את עצמכם שאלה פשוטה:האם מידע זה זמין לציבור?אם התשובה היא לא, המידע כמעט בוודאות חסוי ויש לנקוט בצעדים הדרושים כדי להגן עליו.לקבלת מידע נוסף, ראו את חלק 2.1, זיהוי מידע עסקי חסוי. |
| Screen 46Question 6: Scenario72\_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: | האסדרה הכללית להגנה על מידע (GDPR) היא אחד מחוקי הפרטיות המקיפים בעולם. מאז הטמעתה ב-2018, היא נחשבת לאמת המידה בכל הנוגע להגנה על פרטיות. רגולציה זו גובשה בתחומי: |
| Screen 46Question 6: Options73\_C\_48 | [1] Canada[2] Asia[3] Europe[4] Russia[5] United States[6] Latin America | [1] קנדה[2] אסיה[3] אירופה[4] רוסיה[5] ארה"ב[6] אמריקה הלטינית |
| Screen 46Question 6: Feedback74\_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. | התשובה הנכונה היא אירופה. באירופה, האסדרה הכללית להגנה על מידע (GDPR) היא אחד מחוקי הפרטיות המקיפים בעולם; מאז הטמעתה ב-2018, היא קבעה סטנדרט להגנה על פרטיות שמדינות אחרות מנסות לחקות.למידע נוסף, ראו את חלק 1.2, דרישות משפטיות, רגולטוריות וחוזיות. |
| Screen 46Question 7: Scenario75\_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: | אחד מעמיתיכם לעבודה השלים זה עתה פרויקט שכלל איסוף מידע אישי ושימוש בו. מאז, מחלקה אחרת כבר ביקשה ממנו לקבל גישה למידע הזה. אתם מייעצים לעמיתכם: |
| Screen 46Question 7: Options76\_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] לוודא את זהות מבקשי המידע ואת הצורך שלהם בגישה למידע.[2] לוודא שהמבקשים מורשים לקבל עותק של המידע.[3] לוודא שניתן להשתמש במידע לטובת הצרכים שלשמם ביקשו אותו.[4] כל הנזכר לעיל. |
| Screen 46Question 7: Feedback77\_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. | אחת הסיבות הנפוצות ביותר לתקריות מידע בתוך ארגונים היא שיתוף לא ראוי של מידע עם עובדים בלתי מורשים. לפני שיתוף של מסמך או קובץ כלשהו המכילים מידע רגיש, תמיד:* ודאו את זהות מבקש המידע ואת הצורך שלו בגישה למידע.
* ודאו שהמבקש מורשה לקבל עותק מהמידע.
* ודאו שניתן להשתמש במידע שהוא מבקש לצרכים שהוא מבוקש עבורם.
* שתפו את המידע אך ורק במידה הדרושה, ולא מעבר לכך.

לקבלת מידע נוסף על התשובה הנכונה ראו את חלק 3.2, שיתוף מידע רגיש. |
| Screen 46Question 8: Scenario78\_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? | אתם נציגי מכירות שמבקרים במרפאה באזורכם. בזמן ההמתנה באזור הקבלה, אתם מאבדים בטעות מסמכים רגישים המכילים מידע בריאות מוגן אודות מטופל. מה תעשו? |
| Screen 46Question 8: Options79\_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] איידע בכך את קצין הפרטיות של המרפאה.[2] אצור קשר עם הממונה שלי.[3] אדווח על התקרית למשרד האתיקה והציות (OEC) או לצוות הפרטיות הגלובלי. |
| Screen 46Question 8: Feedback80\_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. | בתגובה לכל חשיפה לא מכוונת של מידע בריאות מוגן הנוגע למטופלים, עליכם לדווח על התקרית באופן מיידי בפני:* משרד האתיקה והציות או אנשי צוות הפרטיות הגלובלי.

לקבלת מידע נוסף, ראו את חלק 3.4, תגובה לחשיפות בלתי ראויות. |
| Screen 46Question 9: Scenario81\_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? | בעת נסיעה לעבודה ברכבת, אתם משאירים בטעות על המושב את המחשב הנייד שלכם, המכיל מסמכי עבודה רגישים, ויוצאים מהרכבת. אתם מבינים את הטעות שלכם עם הגעתכם למשרד ומחפשים בטירוף את המחשב הנייד שלכם, אבל לא מצליחים למצוא אותו. מה עליכם לעשות תחילה? |
| Screen 46Question 9: Options82\_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] להתקשר לחברה המפעילה את הרכבת ולשאול אם מישהו מסר את המחשב הנייד שלכם.[2] לחזור לתחנת הרכבת ולחפש אחר המחשב הנייד.[3] ליצור קשר עם הנציגות המקומית של מוקד השירות העולמי. |
| Screen 46Question 9: Feedback83\_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. | אם אתם סבורים כי יש אפשרות שמידע רגיש נפגע, למשל דרך מחשב נייד שאבד או נגנב, פנו מייד למוקד השירות העולמי באזורכם.לקבלת למידע נוסף, ראו את חלק 3.4, דיווח על תקרית בעניין פרטיות. |
| Screen 46Question 10: Scenario84\_C\_48 | You should only use personal information:Check all that apply. | עליכם להשתמש במידע אישי רק:סמנו את כל מה שרלוונטי. |
| Screen 46Question 10: Options85\_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] לטובת המטרה המסוימת שעבורה קיבלתם גישה.[2] בהתאם להודעה שסופקה לנושא המידע.[3] בהתאם להסכמה שניתנה על ידי נושא המידע. |
| Screen 46Question 10: Feedback86\_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. | אם יש לכם הרשאה לגשת למידע אישי, השתמשו בו רק:* לטובת המטרה המסוימת שעבורה קיבלתם גישה.
* בהתאם להודעה שסופקה לנושא המידע.
* בהתאם להסכמה שניתנה על ידי נושא המידע.

לקבלת מידע נוסף, ראו את חלק 3.1, גישה למידע רגיש ושימוש בו. |
| [Screen 46](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48) [87\_C\_48](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx?showScreen=87_C_48)  | All questions remain unanswered | כל השאלות נותרו ללא מענה |
| [Screen 47](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49) 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. | אין כעת תוצאות זמינות משום שלא השלמתם את בדיקת הידע.ברכותינו! עברתם בהצלחה את בדיקת הידע והשלמתם את הקורס.אנא עיינו בתוצאות שלכם להלן באמצעות לחיצה על כל שאלה.לאחר שתסיימו, לחצו על סמל **יציאה [X]** בסרגל הכותרת של הקורס, לפני שתסגרו את חלון הדפדפן או את לשונית הדפדפן.מצטערים, לא עברתם את בדיקת הידע. הקדישו כמה דקות כדי לעבור על התוצאות שלכם להלן באמצעות לחיצה על כל שאלה.לאחר שתסיימו, לחצו על לחצן **בצעו שוב בדיקת ידע**. |
| 89\_toc\_1 | Introduction | מבוא |
| 90\_toc\_2 | Welcome | ברוכים הבאים |
| 91\_toc\_3 | Objectives | יעדים |
| 92\_toc\_4 | Menu | תפריט |
| 93\_toc\_5 | Personal Information | מידע אישי |
| 94\_toc\_6 | Recognizing Personal Information | זיהוי מידע אישי |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | דרישות משפטיות, רגולטוריות וחוזיות |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | עקרונות "עיצוב לפרטיות" של Abbott |
| 97\_toc\_9 | Review | סקירה |
| 98\_toc\_10 | Confidential Business Information | מידע עסקי חסוי |
| 99\_toc\_11 | Recognizing Confidential Business Information | זיהוי מידע עסקי חסוי |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | מחיר אי ההגנה על מידע עסקי חסוי |
| 101\_toc\_13 | Insider Information | מידע פנים |
| 102\_toc\_14 | Review | סקירה |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | תפקידכם בהגנה על מידע רגיש |
| 104\_toc\_16 | Accessing and Using Sensitive Data | גישה למידע רגיש ושימוש בו |
| 105\_toc\_17 | Sharing Sensitive Data | שיתוף מידע רגיש |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | שמירת מידע רגיש והסרתו |
| 107\_toc\_19 | Responding to Improper Disclosures | תגובה לחשיפות בלתי ראויות |
| 108\_toc\_20 | Review | סקירה |
| 109\_toc\_21 | Knowledge Check | בדיקת ידע |
| 110\_toc\_22 | Introduction | מבוא |
| 111\_toc\_23 | Assessment | הערכה |
| 112\_toc\_24 | Question 1 | שאלה 1 |
| 113\_toc\_25 | Question 2 | שאלה 2 |
| 114\_toc\_26 | Question 3 | שאלה 3 |
| 115\_toc\_27 | Question 4 | שאלה 4 |
| 116\_toc\_28 | Question 5 | שאלה 5 |
| 117\_toc\_29 | Question 6 | שאלה 6 |
| 118\_toc\_30 | Question 7 | שאלה 7 |
| 119\_toc\_31 | Question 8 | שאלה 8 |
| 120\_toc\_32 | Question 9 | שאלה 9 |
| 121\_toc\_33 | Question 10 | שאלה 10 |
| 122\_toc\_34 | Feedback | משוב |
| 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  | הקורס לא מסוגל להתחבר ל-LMS. לחצו על "אישור" כדי להמשיך ולעיין בקורס. שימו לב, ייתכן שאישור השלמת הקורס לא יהיה זמין. לחצו על "ביטול" כדי לצאת  |
| 124\_string\_2 | All questions remain unanswered | כל השאלות נותרו ללא מענה |
| 125\_string\_3 | Questions | שאלות |
| 126\_string\_4 | Question | שאלה |
| 127\_string\_5 | not answered | ללא מענה |
| 128\_string\_6 | That's correct! | נכון! |
| 129\_string\_7 | That's not correct! | לא נכון! |
| 130\_string\_8 | Feedback:  | משוב:  |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | הגנה על מידע רגיש |
| 132\_string\_10 | Knowledge Check | בדיקת ידע |
| 133\_string\_11 | Submit | הגשה |
| 134\_string\_12 | Retake Knowledge Check | בצעו שוב בדיקת ידע |
| 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. | תיאור הקורס: אנו ב-Abbott מסתמכים לעתים קרובות על מידע רגיש לצורך קבלת החלטות עסקיות חשובות. מפני שרבים מבעלי העניין שלנו חוששים מהאופן שבו נאסף המידע ונעשה בו שימוש, Abbott ביססה מדיניות ותהליכים כדי להבטיח הגנה על המידע הזה. קורס זה מסביר מהו מידע רגיש, מדוע הוא חיוני לעסק שלנו ובאילו צעדים אנחנו יכולים לנקוט כדי להבטיח שאנחנו מעבדים את המידע הזה ומטפלים בו באופן בטוח. להשלמת הקורס יידרשו כ-30 דקות. |
| 136\_string\_14 | Menu | תפריט |
| 137\_string\_15 | Resources | משאבים |
| 138\_string\_16 | Reference Material | חומרי עיון |
| 139\_string\_17 | Audio | שמע |
| 140\_string\_18 | Exit | יציאה |
| 141\_string\_19 | Record My Results | תיעוד התוצאות שלי |