|  |  |  |
| --- | --- | --- |
| ID | SOURCE | TARGET |
| [Screen 0](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=1_C_1)  [1\_C\_1](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=1_C_1) | Protecting Sensitive Data  Click the forward arrow to begin. | Защита конфиденциальных данных  Чтобы начать обучение, нажмите стрелку вперед. |
| [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. | При принятии решений компания Abbott полагается на данные, которые часто содержат конфиденциальную информацию.  Для выполнения нашей миссии — помогать людям сохранять здоровье и жить полной жизнью — компания Abbott должна обеспечить безопасность этих данных, соблюдать законы и этические стандарты. Данный курс поможет вам получить навыки, необходимые для выполнения этой задачи. |
| [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. | После прохождения этого курса вы узнаете:   * что такое конфиденциальные данные; * как компания Abbott защищает эти данные; * какова ваша роль в защите конфиденциальных данных; * что делать, если вы считаете, что конфиденциальные данные были неправомерно раскрыты или поставлены под угрозу. |
| [Screen 3](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4)  [4\_C\_4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4) | 1 | Personal Information  Here you will learn how governments, consumers, and the public have become increasingly concerned about the privacy and security of personal information.  12 Minutes  Section 1 | Personal Information  Recognizing Personal Information  Legal, Regulatory and Contractual Requirements  Abbott’s Privacy by Design Principles  Review  2 | Confidential Business Information  Here you will learn how most of the business information we use in our day-to-day work activities is considered confidential.  5 Minutes  Section 2 | Confidential Business Information  Recognizing Confidential Business Information  Cost of Not Protecting Confidential Business Information  Insider Information  Review  3 | Protecting Sensitive Data  Here you will learn what you can do to help protect sensitive data.  8 Minutes  Section 3 | Your Role in Protecting Sensitive Data  Accessing and Using Sensitive Data  Sharing Sensitive Data  Retaining and Disposing of Sensitive Data  Responding to Improper Disclosures  Review  4 | Knowledge Check  Assess your understanding of the key concepts and principles of this course.  5 Minutes  Section 4 | Knowledge Check  Assessment  Click the panel to get started.  Click the yellow play button to begin.  This content is not yet available. You must complete Section{a} {b}. | 1 | Персональные данные  Из этого раздела вы узнаете, насколько больше внимания власти, потребители и общественность стали уделять конфиденциальности и безопасности персональных данных.  12 минут  Раздел 1 | Персональные данные  Распознавание персональных данных  Юридические, нормативные и договорные требования.  Принципы проектирования конфиденциальности компании Abbott  Просмотреть  2 | Конфиденциальная деловая информация  Из этого раздела вы узнаете, что бо́льшая часть деловой информации, которую мы используем в повседневной работе, считается конфиденциальной.  5 минут  Раздел 2 | Конфиденциальная деловая информация  Определение конфиденциальной деловой информации  Цена отсутствия защиты конфиденциальной деловой информации  Инсайдерская информация  Просмотреть  3 | Защита конфиденциальных данных  Из этого раздела вы узнаете, что вы можете предпринять для защиты конфиденциальных данных.  8 минут  Раздел 3 | Ваша роль в защите конфиденциальных данных  Доступ к конфиденциальным данным и их использование.  Передача конфиденциальных данных  Хранение и удаление конфиденциальных данных  Реагирование на ненадлежащее раскрытие информации  Просмотреть  4 | Проверка знаний  Проверьте, усвоили ли вы ключевые понятия и принципы этого курса.  5 минут  Раздел 4 | Проверка знаний  Оценка  Нажмите на панель, чтобы начать.  Нажмите желтую кнопку воспроизведения, чтобы начать.  Этот контент пока недоступен. Вы должны завершить раздел{a} {b}. |
| [Screen 4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7)  [5\_C\_7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7) | At Abbott, one common type of sensitive data we use is personal information.  In recent years, governments, consumers, and the general public have become increasingly concerned about the privacy and security of personal information. | Один из типов конфиденциальной информации, которую мы используем в компании — это персональные данные.  В последние годы власти, потребители и широкая общественность все больше беспокоятся о конфиденциальности и безопасности персональных данных. |
| [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. | Персональные данные — это любая информация, которая может быть использована для связи с конкретным лицом, определения его местонахождения или иной идентификации этого лица. |
| [Screen 6](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9)  [7\_C\_9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9) | Kandice | Marketing Manager  Can you give me some examples of personal information?  Personal information can include biographical information, such as name, date of birth, email address and phone number.  It can include information relating to an individual’s appearance, such as hair color or weight.  It can also include information relating to an individual’s personal life, such as photos, browser cookies or location tracking information. | Кэндис | Менеджер по маркетингу  Можете ли вы назвать несколько примеров персональных данных?  К персональным данным может относиться биографическая информация, такая как имя, дата рождения, адрес электронной почты и номер телефона.  Она также может включать информацию, относящуюся к внешнему виду человека, например, цвет волос или вес.  Она также может включать информацию, относящуюся к личной жизни человека, например, фотографии, файлы cookie или данные об отслеживании местонахождения. |
| [Screen 7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10)  [8\_C\_10](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10) | Jerry | Sales Representative  Does personal information also include protected health information?  Yes, it does.  Protected health information (PHI) is a particularly sensitive type of personal information used in the healthcare industry. It includes any personally identifiable information in medical records, including conversations between medical professionals about treatment. | Джерри | Торговый представитель  Относятся ли к персональным данным защищенная законом медицинская информация?  Да, относится.  Защищенная медицинская информация (ЗМИ) — это особый тип конфиденциальных персональных данных, которые используются в сфере здравоохранения. Она включает информацию, позволяющую установить личность в медицинских документах, включая обсуждение лечения медицинскими работниками. |
| [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. | В большинстве стран, в которых компания Abbott ведет свою деятельность, существуют законы и правила для защиты персональных данных, включая защищенную законом медицинскую информацию.  Законы, касающиеся конфиденциальности и защиты персональных данных, отличаются в разных странах, но часто они содержат одни и те же основные принципы.  НАЖМИТЕ НА КАЖДУЮ ВЫДЕЛЕННУЮ ОБЛАСТЬ НА ЭКРАНЕ, ЧТОБЫ УЗНАТЬ О РАЗЛИЧНЫХ ТИПАХ ЗАКОНОВ И ТРЕБОВАНИЙ В ОТНОШЕНИИ КОНФИДЕНЦИАЛЬНОСТИ, СУЩЕСТВУЮЩИХ ВО ВСЕМ МИРЕ. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11)  [10\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11) | Europe  In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate. GDPR applies to organizations located within Europe, as well as organizations located outside of Europe that offer goods and services to or monitor the behavior of any individual residing in Europe.  One of the key concepts of GDPR is the right to erasure, also known as the right to be forgotten. This right gives individuals the ability to request that their personal data be erased from an organization's records. If an individual makes such a request, the organization must take steps to erase the data from its systems and prevent its further use or disclosure. There may be exceptions to data subject requests. Nonetheless, Abbott will inform each validated data subject of what action is taken for each request. Violations of GDPR can result in heavy fines for companies, up to 4% of their annual global turnover, or 20 million euros (whichever is greater), for the most serious offenses. | Европа  В Европе действует Общий регламент по защите данных (GDPR), один из самых всеобъемлющих законов о защите персональных данных в мире, и с момента вступления в силу в 2018 году он установил стандарт защиты персональных данных, который пытаются перенять другие страны. GDPR применяется к организациям, расположенным как в Европе, так и за ее пределами, которые предлагают товары и услуги или отслеживают поведение лиц, проживающих в Европе.  Одним из ключевых понятий GDPR является право на удаление данных, также известное как право на забвение. Это означает, что человек может потребовать удаления своих персональных данных из документации организации. Если физическое лицо обращается с таким требованием, организация должна принять меры для удаления данных из своих систем и предотвращения их дальнейшего использования или раскрытия. Впрочем, из таких запросов могут быть исключения. Тем не менее, компания Abbott будет информировать каждого установленного субъекта данных о действиях, предпринимаемых по его запросу. Нарушение GDPR грозит компаниям крупными штрафами: до 4% от их годового мирового оборота или 20 миллионов евро (в зависимости от того, какая сумма больше) за самые серьезные нарушения. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11)  [11\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11) | United States  In the United States, there is no single law that protects all personal information. Instead, there are privacy laws and regulations that apply to specific industries and types of data. For example, HIPAA protects the privacy of healthcare data, while the Fair Credit Reporting Act protects credit information.  However, some states have begun enacting their own comprehensive data privacy laws. For instance, California has the California Consumer Privacy Act (CCPA), which gives Californians certain rights to their data, such as the right to know what personal information is being collected about them and the right to delete any personal information collected. The CCPA will be amended by the California Privacy Rights Act (CPRA) in 2023, which will give people even more rights to their data.  Other states that have passed their own data privacy laws include Virginia, Colorado, Utah, and Connecticut. While each state's law is different, they all generally give people rights to their data and require companies to provide certain disclosures about their data processing activities.  Fines for violating state privacy laws can be significant. For example, California can fine companies up to $7,500 USD per violation of the CCPA.  Canada  There are laws at both the federal and provincial levels in Canada that are designed to protect an individual's personal information. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that applies to private sector organizations and is enforced by the Office of the Privacy Commissioner of Canada.  At the provincial level, Quebec, Alberta, and British Columbia have enacted privacy laws that are similar to PIPEDA. Some other provinces also have rules in place that provide similar protections for personal information, including the provinces of Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia, which have enacted health information privacy laws.  These laws are in place to help prevent personal information from being mishandled or collected without the individual's knowledge, and give people the right to access their own information and correct any errors.  Violating these laws can result in significant fines. For example, violating PIPEDA can lead to a fine of up to $100,000. In Alberta, the Personal Information Protection Act (PIPA) allows for fines of up to $10,000 for individuals and $500,000 for organizations. | Соединенные Штаты Америки  В США нет единого закона, защищающего персональные данные. Вместо этого существуют законы и нормативно-правовые акты о неприкосновенности частной жизни, которые применяются к конкретным отраслям и видам данных. Например, Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA) защищает конфиденциальность медицинских данных, а Закон о добросовестности в предоставлении сведений о кредитоспособности защищает кредитную информацию.  Однако некоторые штаты начали принимать собственные всеобъемлющие законы о защите персональных данных. Например, в Калифорнии действует Закон штата Калифорния о защите конфиденциальности потребителей (CCPA), который дает калифорнийцам определенные права в отношении принадлежащих им данных, такие как право знать, какие персональные данные о них собираются, и право удалять любые собранные персональные данные. В 2023 году на смену CCPA придет Закон Калифорнии о праве на неприкосновенность частной жизни, который расширит права частных лиц на принадлежащие им данные.  Собственные законы о защите персональных данных также приняли штаты Вирджиния, Колорадо, Юта и Коннектикут. Хотя законы каждого штата различаются, все они в целом предоставляют людям права на свои данные и требуют от компаний раскрывать сведения о деятельности по обработке данных.  За нарушение законов штатов о защите персональных данных предусмотрены крупные штрафы. Например, в Калифорнии за нарушение CCPA компанию могут оштрафовать на сумму до $7 500 долларов.  Канада  В Канаде законы, направленные на защиту персональных данных, приняты как на федеральном уровне, так и на уровне провинций. Например, Закон о защите персональных данных и электронных документов (PIPEDA) — федеральный закон, который распространяется на организации частного сектора, и за соблюдением которого следит Управление уполномоченного по вопросам конфиденциальности Канады.  Провинции Квебек, Альберта и Британская Колумбия приняли законы о защите персональных данных, аналогичные PIPEDA. В ряде других провинций также действуют правила, обеспечивающие аналогичную защиту персональных данных, в том числе в Онтарио, Нью-Брансуике, Ньюфаундленде и Лабрадоре, Новой Шотландии, которые приняли законы о защите медицинской информации.  Эти законы помогают предотвратить злоупотребление персональными данными и их сбор без ведома владельца, а также дают право на доступ к своим данным и исправление ошибок.  Нарушение таких законов грозит крупными штрафами. Например, нарушение PIPEDA карается штрафом до $100 000 долларов. В Альберте Закон о защите персональных данных (PIPA) допускает штрафы в размере до $10 000 долларов для физических лиц и $500 000 долларов для организаций. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=12_C_11)  [12\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=12_C_11) | Asia Pacific  The privacy laws in the Asia Pacific region are constantly expanding and becoming more comprehensive. Some countries, such as China, have implemented data localization measures which require companies to store some personal data on servers within their borders. Additionally, China has privacy and security impact assessment requirements for the cross-border transfer of personal information.  Others, like Australia and Singapore, have adopted a more consumer-focused approach to privacy that gives individuals greater control over their information, including the right to know how companies are using it and the ability to access and correct it if necessary.  The penalties for companies who violate data privacy laws also differ widely across the region. In China, for example, companies can be fined up to 500,000 RMB (about $72,000 USD) for violating data privacy laws.  However, in Singapore, companies can be fined up to 1 million (Singapore) dollars (about $737,000 USD) for violating the country’s privacy law. | Азиатско-Тихоокеанский регион  Законы о защите персональных данных в Азиатско-Тихоокеанском регионе постоянно расширяют сферу своего влияния и становятся более всеобъемлющими. Некоторые страны, такие как Китай, внедрили меры по локализации данных, которые требуют от компаний хранить ряд персональных данных на серверах в пределах их границ. Кроме того, в Китае действуют требования к оценке воздействия на конфиденциальность и безопасность при трансграничной передаче персональных данных.  Другие страны, такие как Австралия и Сингапур, приняли более ориентированный на потребителя подход к конфиденциальности, который дает людям бóльший контроль над своими данными, включая право знать, как компании используют их, а также возможность доступа к ним и их исправления в случае необходимости.  Штрафы для компаний, нарушающих законы о защите персональных данных, также сильно различаются в разных странах региона. В Китае, например, за нарушение законов о защите персональных данных компанию могут оштрафовать на сумму до 500 000 юаней (около $72 000 долларов).  В Сингапуре нарушение закона о защите персональных данных грозит компаниям штрафом в размере до 1 миллиона сингапурских долларов (около $737 000 долларов). |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11)  [13\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11) | Russia  Russia also has laws to protect its citizens' data, including a data localization law, which requires companies to store the personal data of Russian citizens on servers located in Russia.  The law applies to companies that process the data of Russia's citizens, regardless of whether those companies are based in Russia or not. So, for example, a U.S.-based company that processes the data of Russian citizens would need to comply with the law.  Like many countries, the law also requires companies to take steps to protect the personal data they process. For example, companies must ensure that the data is accurate and up-to-date and take steps to prevent it from being mishandled, lost, or stolen.  The fines for violating the law can range from $12,000 to $72,000 USD for the first offense and up to $216,000 USD for the second offense. | Россия  В России также действуют законы о защите данных граждан, в том числе закон о локализации данных, который требует от компаний хранить персональные данные российских граждан на серверах, расположенных в России.  Закон распространяется на компании, которые обрабатывают данные российских граждан, независимо от того, находятся ли эти компании на территории России. Так, например, компания, которая находится в США и обрабатывает данные российских граждан, обязана соблюдать этот закон.  Как и во многих странах, закон также требует от компаний принять меры для защиты обрабатываемых персональных данных. Например, компании должны обеспечить точность и актуальность данных и принять меры во избежание ненадлежащего обращения, потери и кражи.  Штрафы за нарушение закона варьируются от $12 000 до $72 000 долларов за первое нарушение и до $216 000 долларов за повторное нарушение. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=14_C_11)  [14\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=14_C_11) | Latin America  Most Latin American countries have laws in place that protect the privacy of individuals. However, many countries in the region, such as Ecuador, Argentina and Brazil, have recently revised their existing privacy regulations to stay current with international standards.  Ecuador, for example, recently passed the Organic Law on the Protection of Personal Data (LPPD), which will go into effect in 2023. This law applies to any company around the world that processes the personal data of individuals in Ecuador.  Like others in the region, the LPPD requires companies to provide notice and collect consent from individuals before using their data, destroy it when it is no longer needed, and meet certain restrictions before data is shared with other countries. These measures help protect the privacy of individuals across Latin America and ensure that companies are handling personal data responsibly.  Violations of the LPPD can result in significant fines, ranging from 3% to 17% of an organization’s annual revenue from the previous year, providing a strong incentive for companies to comply with the law. | Латинская Америка  В большинстве стран Латинской Америки действуют законы о неприкосновенности частной жизни. Однако многие страны региона, такие как Эквадор, Аргентина и Бразилия, недавно пересмотрели свои нормативно-правовые акты о неприкосновенности частной жизни и привели их в соответствие с международными стандартами.  Эквадор, например, недавно принял Органический закон о защите персональных данных (LPPD), который вступит в силу в 2023 году. Этот закон распространяется на компании по всему миру, которые обрабатывают персональные данные граждан Эквадора.  Как и другие законы в регионе, LPPD требует от компаний уведомлять физических лиц и заручаться их согласием, прежде чем использовать их данные, уничтожать данные, когда они больше не нужны, а также соблюдать определенные ограничения, если необходимо передать данные в другие страны. Эти меры помогают защитить данные жителей Латинской Америки и обеспечить ответственное обращение компаний с персональными данными.  Нарушение LPPD карается крупными штрафами в размере от 3% до 17% годового дохода организации за предыдущий год, что является мощным стимулом для соблюдения закона. |
| [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. | В дополнение к законам и положениям, регулирующим деятельность компании Abbott, могут существовать дополнительные обязательства для определенных видов договоров, которые мы заключаем с клиентами.  Например, правительство США является клиентом компании Abbott. В соответствии с условиями подобного соглашения, от нас требуется выполнять обязательства, определенные в Законе о неприкосновенности частной жизни США от 1974 года.  ЧТОБЫ УЗНАТЬ БОЛЬШЕ, НАЖМИТЕ «ЗАКОН О НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ». |
| [Screen 9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=16_C_12)  [16\_C\_12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=16_C_12) | Privacy Act  The Privacy Act of 1974 (5 U.S.C. 552a) is an important Federal regulation. It establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by federal agencies. For certain transactions, Abbott may be granted access to government agency records. In such cases, Abbott must meet several obligations, including the need to demonstrate that privacy training on protecting personally identifiable information has been conducted.  Employees should contact Legal before entering into any agreements with customers that have privacy obligations. | Закон о неприкосновенности частной жизни.  Закон о неприкосновенности частной жизни 1974 года (5 U.S.C. 552a) является важным федеральным нормативным актом. Он устанавливает Кодекс справедливой информационной политики, который регулирует сбор, хранение, использование и распространение информации, позволяющей установить личность и хранящейся в системах документов федеральных агентств. Для некоторых операций компании Abbott может быть предоставлен доступ к документам государственных учреждений. В таких случаях компания Abbott должна выполнить ряд требований, включая необходимость продемонстрировать, что она провела курс обучения для сотрудников о том, как защитить персональную идентифицирующую информацию .  Сотрудники должны обращаться в Юридический отдел перед тем, как заключать соглашения с клиентами, которые предусматривают обязательства по защите персональных данных. |
| [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. | Законы, нормативные положения и договорные требования, которые мы только что рассмотрели, часто являются сложными и могут быстро меняться.  Компания Abbott приняла положения и процедуры, чтобы обеспечить соблюдение сотрудниками этих законов и нормативных положений. Если у вас возникнут вопросы или вы захотите получить более подробную информацию, свяжитесь с Отделом этики и комплаенс или с сотрудником команды Global Privacy.  Для просмотра контактов и дополнительной информации нажмите на значок «Ресурсы». |
| [Screen 11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=18_C_14)  [18\_C\_14](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=18_C_14) | Collection   * Notice * Consent   MANAGEMENT   * Data Integrity * Access and Correction   Usage   * Disclosure and Use   Disposition   * Retention and Disposal   Abbott’s data privacy and protection policies and procedures are organized around a simple set of principles. We call this Privacy by Design.  These principles are designed to help employees protect sensitive data at each stage of the data lifecycle. To illustrate, let’s look specifically at personal information.  The first stage of the data lifecycle is collection.  During this stage, Abbott uses a variety of methods to collect personal information. For example, we may request consumers to provide contact details at an Abbott website, or we may capture personal data generated from one of our devices.  In order to protect the privacy rights of the individuals during this stage, we maintain processes to ensure we adhere to the Privacy by Design principles of Notice and Consent.  Notice is about letting people know what personal information is being collected and explaining in clear, precise, and unambiguous language how we plan to use that information.  For example, when submitting an inquiry at abbott.com, the personal information we collect is used for the sole purpose of responding to the inquiry.  Consent is about providing individuals with the opportunity to agree to the collection and use of their personal information.  Generally, when we seek consent, we ensure it is:   * Freely given. The individual is never coerced or told that consent is a requirement. * Informed. The individual is given sufficient information to make a reasonable decision to which they are consenting. * Affirmative. The individual must affirmatively provide consent. We never assign consent, for example, through an individual’s silence, nor do we require the individual to take some action, such as unchecking a box, to opt out of something. * Revocable. The individual is provided with a clear explanation of how to revoke consent.   For example, a consumer registering with the Abbott Nutrition Similac© Strong Moms© Rewards program can consent to the collection and use of their Personal Information by opting in (e.g., checking a box) to receive additional promotional information.  The second stage of the data lifecycle is management.  During this stage, information is processed and stored.  In order to protect personal information during this stage, we maintain processes that ensure we adhere to the principles of:   * Data Integrity, and * Access and Correction.   Data Integrity is about taking reasonable measures to ensure that the personal information we retain is accurate, complete, and current.  One way we do this is by tracking and recording all activities that process personal information. This ensures we can identify the source of the data, the specific purposes for which the data has been processed, and where it is stored.  Access and Correction is about providing individuals with reasonable access to their data and the opportunity to exercise their rights in connection with this data.  This includes responding to an individual’s request to access, delete, transfer, or amend the stored records of personal information.  The third stage of the lifecycle is usage.  During this stage, personal information is used to support activities across the organization.  In order to protect personal information during this stage, we maintain processes that ensure we adhere to the principle of Disclosure and Use.  Disclosure and Use is about controlling who has access to personal information and limiting use to specific purposes.  We manage this through access controls and other processes. These controls and processes limit access to individuals in specific job functions as well as limiting use to the specific purposes set out in the notice for which consent was provided.  The final stage of the lifecycle is disposition.  Disposition refers to what happens to data once it is no longer actively being used. Activities may include deletion, archiving, or retaining for legal hold purposes.  In order to protect personal information during this stage, we maintain policies and processes that ensure we adhere to the principle of Retention and Disposal.  Retention and Disposal of personal information is about retaining personal information for only the time necessary to achieve the purposes for which it was needed and processed.  Once personal information is no longer required in an active production environment, Abbott has put in place processes to either archive or dispose of it in a manner consistent with Abbott’s data management, retention, and disposal requirements. Our retention and disposal requirements are also subject to any legal hold requirements relating to legal matters.  For additional information related to retention or disposal requirements, see Abbott’s Global Records and Information Policy (l1-02) or contact Information Governance and Records. Details can be found in the Resources section of this training.  For contacts and additional information, click the Resources icon.  As we have just seen, our policies and procedures are designed to protect personal information throughout its lifecycle.  We do this by adhering to the principles of:   * Notice, * Consent, * Data Integrity, * Access and Correction, * Disclosure and Use, and * Retention and Disposal.   COLLECTION  Notice  Consent  MANAGEMENT  Data Integrity  Access and Correction  USAGE  Disclosure and Use  DISPOSITION  Retention and Disposal | Сбор   * Уведомление * Согласие   УПРАВЛЕНИЕ   * Целостность данных * Доступ к данным и их исправление   Использование   * Раскрытие и использование   Утилизация   * Хранение и утилизация   В основе положений и процедур компании Abbott лежит простой набор принципов. Мы называем их «проектируемая конфиденциальность».  Эти принципы разработаны для того, чтобы помочь сотрудникам защищать конфиденциальные данные на каждом этапе их жизненного цикла. Чтобы продемонстрировать этот процесс, давайте рассмотрим его на примере персональных данных.  Первая стадия жизненного цикла данных — это их получение.  В течение этой стадии компания Abbott использует различные методы сбора персональных данных. Например, мы можем запросить у посетителей сайта Abbott предоставить нам контактную информацию на сайте, или мы можем получить персональные данные, собранные одним из наших медицинских устройств.  Для того, чтобы защитить права неприкосновенности частной жизни физических лиц на этом этапе, мы используем процессы, направленные на обеспечение соблюдения принципов проектируемой конфиденциальности, таких как уведомление и согласие.  Уведомление — это сообщение о том, какие персональные данные собираются, и объяснение четким, понятным и недвусмысленным языком, как мы планируем использовать эту информацию.  Например, при подаче запроса на сайте abbott.com, персональные данные, которые мы получаем, используются исключительно в целях ответа на запрос.  Согласие — это предоставление людям возможности дать свое согласие на сбор и использование их персональных данных.  Обычно, когда мы спрашиваем согласие, мы должны убедиться в том, что оно:   * Предоставляется добровольно. Запрещается принуждать человека или говорить ему, что предоставление согласия является обязательным. * Является информированным. Человеку предоставляется достаточная информация для принятия разумного решения о том, давать ли свое согласие. * Является подтвержденным. Человек должен подтвердить свое согласие. Например, мы никогда не подразумеваем, что молчание является знаком согласия и не требуем от людей предпринимать какие-либо действия, такие как снятие галочки в поле, чтобы отказаться от чего-либо. * Подлежит отзыву. Человеку предоставляется четкое разъяснение того, как отозвать свое согласие.   Например, потребитель, регистрирующийся в программе Abbott Nutrition Similac© Strong Moms© Rewards может дать свое согласие на сбор и использование своих персональных данных, произведя определенное действие (например, проставив галочку в поле) для получения дополнительной рекламной информации.  Вторая стадия жизненного цикла данных — это управление ими.  Во время этой стадии информация обрабатывается и сохраняется.  Чтобы защитить персональные данные на этой стадии, мы используем процессы, которые обеспечивают выполнение нами принципов:   * целостности данных и * доступа к данным и их исправление.   Целостность данных подразумевает принятие необходимых мер для обеспечения того, чтобы персональные данные, которые мы храним, были точными, полными и актуальными.  Один из способов это сделать — это отслеживать и записывать все действия по обработке персональных данных. Благодаря этому мы можем определить источник данных, конкретные цели, для которых они обрабатываются, и место их хранения.  Доступ к данным и их исправление — это предоставление лицам необходимого доступа к своим данным и возможности реализовать свои права, связанные с этими данными.  Это включает ответ на запрос лица о доступе к своей хранящейся в компании информации, ее удалении, передаче или исправлении.  Третья стадия жизненного цикла — это использование.  На данной стадии персональные данные используются для различных целей по всей организации.  Для защиты персональных данных на данном этапе у нас есть процессы, которые обеспечивают соблюдение нами принципа раскрытия и использования информации.  Раскрытие и использование подразумевают контроль за лицами, имеющими доступ к личной информации, и ограничение ее использования определенными целями.  Мы осуществляем это за счет контроля доступа и других процессов. Эти механизмы и процессы контроля обеспечивают доступ только определенным сотрудникам и только для конкретных целей, которые были изложены в уведомлении, и на которые было дано согласие.  Заключительная стадия жизненного цикла — это утилизация.  Утилизация относится к тому, что происходит с данными после того, как они перестают активно использоваться. Это может быть удаление, архивация или сохранение информации по юридическим причинам.  Для защиты персональных данных на данном этапе у нас есть положения и процессы, которые обеспечивают соблюдение принципа хранения и утилизации информации.  Хранение и утилизация персональных данных — это хранение персональных данных строго в течение времени, необходимого для достижения целей, в которых они были получены и обработаны.  Если персональные данные больше не требуются в работе, компания Abbott архивирует либо утилизирует данные согласно требованиям Abbott в отношении управления данными, их хранения и утилизации. Наши требования по хранению и утилизации также подчиняются требованиям о хранении информации по юридическим причинам.  Чтобы узнать больше о требованиях по хранению и утилизации информации, см. Глобальную политику компании Abbott по хранению записей и информации (l1-02) или свяжитесь с Отделом информации и документации. Подробную информацию можно найти в разделе «Ресурсы» данного курса обучения.  Для просмотра контактов и дополнительной информации нажмите на значок «Ресурсы».  Как мы только что увидели, наши положения и процедуры разработаны для того, чтобы защитить персональные данные на протяжении их полного жизненного цикла.  Мы реализуем это, соблюдая принципы:   * уведомления; * согласия; * целостности данных; * доступа к данным и их исправления; * раскрытия и использования; * хранения и утилизации.   СБОР  Уведомление  Согласие  УПРАВЛЕНИЕ  Целостность данных  Доступ к данным и их исправление  ИСПОЛЬЗОВАНИЕ  Раскрытие и использование  УТИЛИЗАЦИЯ  Хранение и утилизация |
| [Screen 12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=19_C_15)  [19\_C\_15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=19_C_15) | Click the arrow to begin your review.  Review  Take a moment to review some of the key concepts covered in this section.  Personal Information (PI)  PI is any information that can be used to   * Contact * Locate, or * Identify an individual.   Protected Health Information (PHI)  PHI is a particularly sensitive type of personal information used in the healthcare industry.  Privacy Laws  Privacy laws differ from one country to the next, but often embrace the same core principles.  Abbott’s Privacy by Design Principles  Abbott’s data privacy and protection policies and procedures are organized around a set of principles, called Privacy by Design.  Notice and Consent  Notice and Consent is about letting people know what PI is being collected and providing them the opportunity to agree to that collection.  Data Integrity  Data Integrity is about taking reasonable measures to ensure that PI is accurate, complete, and current.  Access and Correction  Access and Correction is about providing individuals the right to access and correct their data.  Disclosure and Use  Disclosure and Use is about controlling who has access to PI.  Retention and Disposal  Retention and Disposal of PI is about retaining personal information for only the time necessary to achieve the purposes for which it was needed and processed.  To check your progress, click the Menu button  Great job!  You have completed section 1 of 4  Click the forward arrow to continue learning | Нажмите на стрелку, чтобы начать просмотр.  Просмотреть  Повторите ключевые понятия, изученные в этом разделе.  Персональные данные  Это любая информация, которая позволяет:   * связаться с человеком; * найти человека; * идентифицировать человека.   Защищенная медицинская информация (ЗМИ)  ЗМИ — это особый тип конфиденциальных персональных данных, которые используются в сфере здравоохранения.  Законы о защите персональных данных  Законы о защите персональных данных различаются в разных странах, но часто содержат одинаковые ключевые принципы.  Принципы проектируемой конфиденциальности компании Abbott  В основе положений и процедур компании Abbott о конфиденциальности и защите данных лежит простой набор принципов так называемой проектируемой конфиденциальности.  Уведомление и согласие  Цель уведомления и получения согласия — проинформировать человека о том, какие персональные данные о нем собираются, и дать ему возможность предоставить свое согласие.  Целостность данных  Целостность данных подразумевает принятие мер для обеспечения точности, полноты и актуальности персональных данных.  Доступ к данным и их исправление  Доступ к данным и их исправление — это предоставление человеку права на доступ и исправление своих данных.  Раскрытие и использование  Раскрытие и использование касается контроля за доступом к персональным данным.  Хранение и утилизация  Хранение и утилизация персональных данных — это хранение персональных данных строго в течение времени, необходимого для достижения целей, в которых они были получены и обработаны.  Чтобы узнать, сколько вы уже изучили, нажмите кнопку меню.  Отлично!  Вы изучили разделов: 1 из 4  Для продолжения нажмите стрелку вперед. |
| [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. | Другой тип конфиденциальных данных, которые мы часто используем — это конфиденциальная деловая информация.  Конфиденциальная деловая информация — это широкая категория. К ней относится бо́льшая часть деловой информации, которую мы используем, и с которой сталкиваемся на повседневной основе. Конфиденциальная информация — это информация, не являющаяся общедоступной, которая может быть использована конкурентами компании Abbott или может нанести ущерб Abbott в случае раскрытия. |
| [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. | Кэндис | Менеджер по маркетингу  Можете ли вы дать примеры конфиденциальной деловой информации?  Конфиденциальная деловая информация может включать: разработку продуктов и процессов производства, составы,микроорганизмы, компьютерное программное обеспечение, данные исследований и разработок, клинические и фармакологические данные, данные пациентов, технические данные, списки покупателей и потенциальных клиентов, практики ведения бизнеса, маркетинговые планы и стратегии, финансовые и операционные данные, а также данные о персонале.  К ней также относится информация о закупках, например, тендерные предложения, списки поставщиков и информация о затратах. |
| [Screen 15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19)  [22\_C\_19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19) | Jerry | Sales Representative  Are there certain types of confidential business information that are more sensitive than others?  Yes. Certain types of confidential business information require greater care than normal because improper disclosure or use of this information can cause serious harm to the company.  Examples include:   * Trade secrets, manufacturing formulas and processes; * Clinical and regulatory data, regulatory submissions, or pre-approval information; and * Financial data that has not been released to the public. | Джерри | Торговый представитель  Есть ли определенные виды конфиденциальной деловой информации, которые считаются более конфиденциальными, чем другие?  Да. Определенные типы конфиденциальной деловой информации требуют большей осторожности, чем обычно, поскольку несанкционированное раскрытие или использование этой информации может нанести серьезный ущерб компании.  Например:   * коммерческая тайна, производственные формулы и процессы; * клинические и нормативные данные, документы для подачи в регулятивные органы или данные для предварительного согласования; * финансовые данные, которые не были опубликованы для общественности. |
| [Screen 16](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=23_C_20)  [23\_C\_20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=23_C_20) | As you can see, most of the business information we use in our day-to-day work activities is considered confidential.  A good way to confirm whether the business information you are using is confidential is to ask yourself a simple question:  Is this information publicly available?  If the answer is no, then the information should be considered confidential and appropriate steps must be taken to protect it. | Как вы видите, бо́льшая часть коммерческой информации, которую мы используем в повседневной работе, считается конфиденциальной.  Для проверки того, является ли информация, которую вы используете, конфиденциальной, рекомендуется задать себе простой вопрос:  Является ли эта информация общедоступной?  Если ответ отрицательный, тогда информация должна считаться конфиденциальной, и необходимо предпринять определенные меры для ее защиты. |
| [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. | Кроме того, любая конфиденциальная деловая информация, созданная во время выполнения вами должностных обязанностей в компании Abbott, является собственностью Abbott.  Поэтому вы обязаны защищать данную информацию и не хранить ее у себя после прекращения работы в компании 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. | Защита конфиденциальной деловой информации крайне важна для компании.  Неудивительно, что злоупотребление этой информацией или ее раскрытие могут нанести компании Abbott существенный ущерб. |
| [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. | Злоупотребление конфиденциальной информацией или ее раскрытие могут нанести значительный ущерб отношениям компании Abbott с клиентами и потребителями, привести к негативному освещению в прессе и СМИ, а также к потере конкурентных преимуществ Abbott. Еще одним последствием могут стать гражданские иски и уголовные наказания, в том числе в отношении нынешних и бывших сотрудников.  ЧТОБЫ УЗНАТЬ БОЛЬШЕ, НАЖМИТЕ «НЕДАВНИЕ СУДЕБНЫЕ РЕШЕНИЯ». |
| [Screen 19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=27_C_20d)  [27\_C\_20d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=27_C_20d) | RECENT CASES  In recent years, companies have received large jury verdicts and awards against former employees for improperly taking company information. For example, one company received $240 million award against a former employee who improperly disclosed the company’s confidential information to a competitor. Another company received an $854 million jury award against a former employee and his new employer when the former employee misappropriated the company’s confidential information and then used the company’s confidential information on behalf of the new employer.  Studies indicate that the theft of confidential information causes losses between $209 and $625 billion to publicly traded companies. | НЕДАВНИЕ СУДЕБНЫЕ РЕШЕНИЯ  В последние годы суды присяжных принимают решения о крупных выплатах в пользу компаний, бывшие сотрудники которых злоупотребили деловой информацией. Например, одна компания получила от бывшего сотрудника, неправомерно раскрывшего конфиденциальную информацию конкуренту, выплату в размере $240 миллионов долларов. Другая компания получила решение суда присяжных на сумму $854 миллиона долларов в отношении бывшего сотрудника и его нового работодателя. Бывший сотрудник незаконно присвоил конфиденциальную информацию компании, а затем использовал ее от имени нового работодателя.  По результатам исследований кража конфиденциальной информации наносит публичным компаниям убытки в размере от $209 до $625 миллиардов долларов. |
| [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. | Неудивительно, что власти очень серьезно относятся к краже конфиденциальной информации.  Например, согласно федеральному уголовному законодательству, за кражу конфиденциальной информации человеку грозит до 10 лет лишения свободы и штраф в размере $5 млн долларов. Кроме того, компания, признанная виновной в краже конфиденциальной информации, может быть оштрафована на $10 млн долларов или на сумму, в три раза превышающую ценность похищенной информации.  ЧТОБЫ УЗНАТЬ БОЛЬШЕ, НАЖМИТЕ КНОПКУ «ШТРАФЫ И ВЗЫСКАНИЯ». |
| [Screen 20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=29_C_20e)  [29\_C\_20e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=29_C_20e) | FINES AND PENALTIES  In recent years, several people and companies have been fined or sentenced to prison for stealing confidential information. For example:   * A competitor was fined $60 Million for stealing another company’s confidential information; * A former IT employee was sentenced to 97 months in prison for stealing confidential information; * A former salesman was sentenced to 12 months in prison for stealing confidential information; * A senior executive was sentenced to 24 months in prison for stealing confidential information; and * A research scientist was sentenced to 18 months in prison for stealing confidential information. | ШТРАФЫ И ВЗЫСКАНИЯ  В последние годы несколько компаний и физических лиц были оштрафованы или приговорены к тюремному заключению за кражу конфиденциальной информации. Например:   * Конкурирующую компанию оштрафовали на $60 млн долларов за кражу конфиденциальной информации другой компании; * бывшего сотрудника ИТ-отдела приговорили к 97 месяцам тюремного заключения за кражу конфиденциальной информации; * бывшего торгового представителя приговорили к 12 месяцам тюремного заключения за кражу конфиденциальной информации; * топ-менеджера компании приговорили к 24 месяцам тюремного заключения за кражу конфиденциальной информации; * научного сотрудника приговорили к 18 месяцам тюремного заключения за кражу конфиденциальной информации. |
| [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. | Другой тип конфиденциальной деловой информации, который важно уметь распознавать и защищать, называется *инсайдерской информацией*.  Инсайдерская информация — это важная закрытая информация, которая в случае раскрытия может повлиять на рыночную стоимость ценных бумаг компании или на решения инвесторов о покупке или продаже ценных бумаг. |
| [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. | Примеры инсайдерской информации:   * новости о потенциальной покупке компании; * задержки в выпуске продукта; * новости о взломе внутренней ИТ-системы; * незапланированные изменения в показателях прибыли или размере дивидендов; * предлагаемые тендеры или дробление акций; * информация о новых ведущих продуктах; * заключение контрактов; * планы расширения; * существенные судебные или надзорные процедуры и т. д. |
| [Screen 23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23)  [32\_C\_23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23) | If you are aware or in possession of insider information, it is illegal to trade in, or recommend others to trade in, Abbott securities.  This also applies to the buying and selling of securities of other companies, including those currently doing or expected to do business with Abbott.  To learn more about Abbott’s expectations with regard to the use and protection of unpublicized information, review Abbott’s policy on Insider Trading. Details can be found in the Resources section of this training. | Если вы обладаете инсайдерской информацией, то законом запрещается торговать самому или рекомендовать другим лицам торговать ценными бумагами компании Abbott.  Это также распространяется на покупку и продажу ценных бумаг других компаний, включая те, которые в настоящее время ведут или планируют вести бизнес с компанией Abbott.  Чтобы узнать больше о требованиях Abbott в отношении использования и защиты непубличной информации, ознакомьтесь с разделом «Инсайдерская торговля» в Политике о ценных бумагах Abbott. Подробную информацию можно найти в разделе «Ресурсы» данного курса обучения. |
| [Screen 24](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=33_C_24)  [33\_C\_24](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=33_C_24) | Click the arrow to begin your review.  Review  Take a moment to review some of the key concepts covered in this section.  Confidential Business Information  Any business information that is not publicly available should be considered confidential. This includes much of the business information we use in our day-to-day work activities.  Improper Use of Confidential Business Information  The improper use or disclosure of confidential business information can result in significant harm to the Company, our customers and employees.  Insider Information  Insider information is any non-public, material information that, if publicly disclosed, could reasonably be expected to affect the market value of a company’s securities, or influence investors’ decisions on whether to buy or sell securities.  To check your progress, click the Menu button  Great job!  You have completed section 2 of 4  Click the forward arrow to continue learning | Нажмите на стрелку, чтобы начать просмотр.  Просмотреть  Повторите ключевые понятия, изученные в этом разделе.  Конфиденциальная деловая информация  Любая деловая информация, не являющаяся общедоступной, должна считаться конфиденциальной. Это касается большей части деловой информации, которую мы используем в повседневной работе.  Злоупотребление конфиденциальной деловой информацией  Злоупотребление конфиденциальной деловой информацией или ее раскрытие могут нанести значительный ущерб компании, клиентам и сотрудникам.  Инсайдерская информация  Инсайдерская информация — это важная закрытая информация, которая в случае раскрытия может повлиять на рыночную стоимость ценных бумаг компании или на решения инвесторов о покупке или продаже ценных бумаг.  Чтобы узнать, сколько вы уже изучили, нажмите кнопку меню.  Отлично!  Вы изучили разделов: 2 из 4  Для продолжения нажмите стрелку вперед. |
| [Screen 25](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=34_C_25)  [34\_C\_25](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=34_C_25) | Now that you have a good understanding of the different kinds of data you are likely to encounter during your workday, here is what you can do to help protect it. | Теперь, когда у вас есть понимание различных типов данных, с которыми вы можете встретиться в вашей работе, давайте рассмотрим, что вы можете сделать для их защиты. |
| [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. | Прежде чем получать доступ к каким-либо конфиденциальным данным, убедитесь, что ваша должность и служебные обязанности позволяют вам иметь доступ к этим данным.  Если у вас возникнут вопросы о том, можете ли вы получить доступ к данным (особенно когда это касается персональных данных), свяжитесь с Отделом этики и комплаенс или c сотрудником команды Global Privacy.  ЧТОБЫ УЗНАТЬ БОЛЬШЕ, НАЖМИТЕ «ЗНАЕТЕ ЛИ ВЫ?». |
| [Screen 26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=36_C_26)  [36\_C\_26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=36_C_26) | DID YOU KNOW  Abbott engages in various forms of lawful monitoring to reduce the risk of improper data usage.  This include monitoring the downloading of data or the sending of data to non-Abbott email addresses. | ЗНАЕТЕ ЛИ ВЫ?  Для снижения риска злоупотребления данными компания Abbott применяет различные формы законного мониторинга.  Сюда входит отслеживание загрузки данных и отправки данных на адреса электронной почты, не принадлежащие Abbott. |
| [Screen 27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27)  [37\_C\_27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27) | If you have permission to access sensitive data, only use it for the specific purpose for which you have been granted access.  In the case of personal information, only use the data according to the consent given or notice provided. | Если у вас есть разрешение на доступ к конфиденциальным данным, используйте его исключительно в тех целях, для которых вам был предоставлен этот доступ.  В случае с персональными данными используйте их только в соответствии с полученным согласием или предоставленным уведомлением. |
| [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. | Перед тем как передавать конфиденциальные данные, убедитесь, что человек, которому вы планируете их отправить, обладает необходимым разрешением.  Если у вас возникнут вопросы о необходимости доступа к данным, особенно когда это касается персональных данных, обратитесь к своему руководителю или к специалисту Отдела конфиденциальности компании Abbott. |
| [Screen 29](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=39_C_31)  [39\_C\_31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=39_C_31) | Requests from Your Own Country  If an Abbott employee located in your same country requests sensitive data, always:   * Confirm the identity of the person making the request; * Confirm the person’s need to access the information; * Check to make sure the person is authorized to receive the information; * Verify that the information can be used for the requested purpose; and * Share only the amount of information required to meet the need, not more.   If in doubt, contact OEC or Global Privacy prior to sharing sensitive data. | Запросы из вашей страны  Если сотрудник компании Abbott, который находится в вашей стране, запрашивает конфиденциальную информацию, во всех случаях следует:   * подтвердить личность человека, делающего запрос; * подтвердить необходимость его доступа к данной информации; * убедиться, что у него есть разрешение на получение этой информации; * убедиться, что информация может использоваться для заявленных целей; * передавать только тот объем информации, который необходим, и не более.   Если сомневаетесь, можно ли передавать конфиденциальные данные, обращайтесь в Отдел этики и комплаенс или в команду Global Privacy. |
| [Screen 30](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=40_C_32)  [40\_C\_32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=40_C_32) | Requests from Other Countries  Many countries and regions have laws designed to protect the rights of their citizens, and place restrictions on the transference of personal information across national borders.  If you receive a request for information containing sensitive data from a colleague in a different country than your own, check your division or function’s data privacy policies, or consult OEC or Global Privacy before proceeding. Then, follow the same steps you would if responding to a request from a colleague in your own country. | Запросы из других стран  Многие страны и регионы располагают рядом законов, направленных на защиту прав своих граждан, и устанавливают ограничения на передачу персональных данных через национальные границы.  Если вы получите от коллеги из другой страны запрос на информацию, содержащую конфиденциальные данные, прежде чем предпринимать что-либо, ознакомьтесь с политикой в отношении конфиденциальности данных своего подразделения или отдела либо обратитесь в Отдел этики и комплаенс или в команду Global Privacy. Затем выполните те же действия, что и при ответе на запрос коллеги из своей страны. |
| [Screen 31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33)  [41\_C\_33](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33) | Requests from Third Parties  If the request for sensitive data is from a third party, ensure there is a valid and appropriate contractual agreement in place. If you are unsure, contact OEC, Global Privacy, or Legal prior to sharing. | Запросы от третьих сторон  Если запрос на конфиденциальные данные поступил от третьей стороны, убедитесь в наличии соответствующего действительного договора с этой стороной. Если вы не уверены, можно ли предоставлять информацию, свяжитесь с Отделом этики и комплаенс, командой Global Privacy или Юридическим отделом. |
| [Screen 32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35)  [42\_C\_35](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35) | Always archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements. | Всегда помещайте в архив или удаляйте конфиденциальные данные в соответствии с требованиями Abbott к управлению, хранению и удалению данных. |
| [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. | Если вы получите требование о сохранении информации по юридическим причинам, ни при каких обстоятельствах не игнорируйте, не удаляйте и не уничтожайте информацию, на которую распространяется требование.  Если у вас есть вопросы, связанные с требованием о сохранении информации по юридическим причинам, а также ее хранением и утилизацией, обратитесь к юристу или ассистенту юриста, указанному в уведомлении о хранении информации по юридическим причинам, или позвоните в Отдел судопроизводства по телефону (224) 667-5701. |
| [Screen 34](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37)  [44\_C\_37](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37) | Always take special care with sensitive data when someone leaves Abbott.  Managers must ensure the departing employee is terminated in the appropriate system (e.g., Workday for Employees or Fieldglass for Contingent Workers) as soon as they are notified the employee is leaving. This will ensure access to Abbott data, physical access to buildings, and final pay will be properly managed. | Всегда уделяйте особое внимание конфиденциальным данным, когда сотрудник покидает компанию Abbott.  Руководители обязаны проследить за тем, чтобы увольняющийся сотрудник был удален из соответствующей системы (например, штатные сотрудники — из системы Workday, временные сотрудники — из системы Fieldglass), как только станет известно, что сотрудник увольняется. Это позволит обеспечить надлежащий доступ к данным Abbott, физический доступ в здания и окончательный расчет с сотрудником. |
| [Screen 35](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=45_C_37b)  [45\_C\_37b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=45_C_37b) | Ensure no sensitive data leaves with the departing employee. Transition all files to the Abbott employee who will be assuming the departing person’s role or responsibilities.  Remind the departing employee of the obligation not to keep or disclose sensitive information. Employees may not take their work product or any other Abbott property (e.g. mobile devices) with them when they leave Abbott. If you have questions about your local termination process, contact Human Resources. | Убедитесь, что увольняющийся сотрудник не забирает с собой конфиденциальные данные. Передайте все файлы, содержащие конфиденциальную информацию, сотруднику Abbott, который возьмет на себя роль или обязанности уволившегося сотрудника.  Напомните увольняющемуся сотруднику об обязательстве не хранить и не раскрывать конфиденциальную информацию. Сотрудникам, увольняющимся из компании Abbott, запрещается забирать с собой результаты работы и любое другое имущество Abbott (например, мобильные устройства). Если у вас есть вопросы о местном порядке увольнения сотрудников, обратитесь в Отдел по работе с персоналом. |
| [Screen 36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38)  [46\_C\_38](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38) | Inadvertent disclosures of PHI can happen at any time.  For example, you may overhear a nurse discussing details of a patient’s health status or you may accidentally be copied on an email containing details of a patient’s record. | Непреднамеренное раскрытие защищенной медицинской информации (ЗМИ) может произойти в любое время.  Например, вы можете случайно услышать, как медсестра обсуждает состояние здоровья пациента или случайно оказаться среди получателей электронного письма с подробностями истории болезни пациента. |
| [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. | О любом случайном или ином ненадлежащем раскрытии защищенной медицинской информации (ЗМИ) пациента немедленно сообщите в Отдел этики и комплаенс или сотруднику команды Global Privacy. |
| [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. | Если вам стало известно о ненадлежащем или непреднамеренном раскрытии конфиденциальной деловой информации, вы должны немедленно сообщить об этом раскрытии:   * вашему непосредственному руководителю, и * в Oтдел этики и комплаенс или сотруднику команды Global Privacy.   Ваше незамедлительное сообщение о раскрытии информации поможет компании Abbott оперативно вернуть информацию, предотвратить дополнительное ненадлежащее использование данной информации или злоупотребление информацией и, в случае необходимости, помочь компании в гражданском иске или уголовном процессе. |
| [Screen 39](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c)  [49\_C\_38c](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c) | You should never disclose Abbott sensitive data to anyone not authorized to receive the sensitive data.  Similarly, you should only use Abbott sensitive data on behalf of Abbott and while performing your Abbott business function.  If you improperly disclose sensitive data, you may face disciplinary action, up to and including termination of employment. | Вы никогда не должны раскрывать конфиденциальные данные Abbott лицам, не уполномоченным на их получение.  Аналогичным образом, вы должны использовать конфиденциальные данные Abbott только от имени Abbott и при выполнении своих должностных обязанностей в Abbott.  Неправомерное разглашение конфиденциальных данных грозит дисциплинарными мерами вплоть до увольнения. |
| [Screen 40](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=50_C_38d)  [50\_C\_38d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=50_C_38d) | You are not permitted, both during and after your Abbott employment, to share Abbott data with any Abbott competitor. | Вам также не разрешается передавать конфиденциальные данные Abbott конкурентам как во время работы в компании Abbott, так и после увольнения. |
| [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. | Отказ от возвращения конфиденциальных данных компании Abbott, передача конфиденциальных данных на неодобренное устройство, в хранилище, в учетную запись или на сервер, а также предоставление конфиденциальных данных любому физическому или юридическому лицу, у которого нет соответствующего разрешения, может привести к тому, что компания Abbott будет вынуждена обратиться в суд.  НАЖМИТЕ КНОПКУ «ЮРИДИЧЕСКИЕ МЕРЫ» ДЛЯ ПОЛУЧЕНИЯ ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ. |
| [Screen 41](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=52_C_38e)  [52\_C\_38e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=52_C_38e) | LEGAL ACTION  Legal action could include Abbott filing a civil lawsuit against you that would:   * Prevent you from working for a new employer until Abbott sensitive data has been returned and protected; * Require you to turn over all electronic devices to Abbott for review and inspection; * Cause you to pay monetary damages for illegally retaining and/or using Abbott sensitive data, and violating the duties and obligations you owe Abbott under your Abbott Employment Agreement; and * Obligate you to pay the legal fees Abbott incurs as a result of filing a lawsuit to protect its sensitive data.   If necessary, Abbott will also work with local, state and federal authorities to protect and retain Abbott sensitive data. In this scenario, you could also face criminal penalties. | ЮРИДИЧЕСКИЕ МЕРЫ  Юридические меры могут включать подачу Abbott гражданского иска против вас с целью:   * запретить вам работать у нового работодателя, пока конфиденциальные данные компании Abbott не будут возвращены и защищены; * потребовать, чтобы вы передали все электронные устройства компании Abbott для изучения и проверки; * потребовать выплату денежной компенсации за незаконное хранение и/или использование конфиденциальных данных компании Abbott, а также невыполнение обязанностей и обязательств, зафиксированных в трудовом договоре с компанией Abbott; * обязать вас оплатить судебные издержки, которые компания Abbott понесет в результате подачи иска о защите своих конфиденциальных данных.   При необходимости Abbott также будет сотрудничать с местными, государственными и федеральными органами власти для защиты и сохранения конфиденциальных данных Abbott. В этом случае вам также может грозить уголовное наказание. |
| [Screen 42](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=53_C_43)  [53\_C\_43](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=53_C_43) | Any event involving a potential compromise of information security, including a lost or stolen mobile device, should be reported immediately to your local Global Service Desk.  If you have any concerns about a potential violation or want to report a potential privacy incident, contact Global Privacy. | О любом событии, связанном с потенциальной угрозой информационной безопасности, включая утерю или кражу мобильного устройства, следует немедленно сообщить в местное отделение Глобальной службы поддержки.  Если вы подозреваете, что имело место нарушение конфиденциальности, обратитесь в команду Global Privacy. |
| [Screen 43](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=54_C_44)  [54\_C\_44](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=54_C_44) | Click the arrow to begin your review.  Review  Take a moment to review some of the key concepts covered in this section.  Accessing and Using Sensitive Data  Only access and use sensitive data for the specific purpose for which you have been granted access.  Sharing Sensitive Data  Before sharing sensitive data:   * Confirm the identity of the requestor; * Confirm their need to access the information; * Verify the information can be used for the purpose(s) requested; and * Share only the amount required to meet the need.   Retaining and Disposing of Sensitive Data  Always archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements.  Responding to Inadvertent Disclosure of PHI  In response to any inadvertent or improper disclosure of a patient’s PHI, immediately report the disclosure to OEC or a member of the Global Privacy team.  Reporting a Privacy Incident  Contact the Global Privacy team to report a potential privacy incident.  To check your progress, click the Menu button  Great job!  You have completed section 3 of 4  Click the forward arrow to continue learning | Нажмите на стрелку, чтобы начать просмотр.  Просмотреть  Повторите ключевые понятия, изученные в этом разделе.  Доступ к конфиденциальным данным и их использование.  Осуществляйте доступ к конфиденциальным данным и используйте их исключительно с целью, для которой вам был предоставлен доступ.  Передача конфиденциальных данных  До передачи конфиденциальных данных:   * проверьте личность запрашивающего их лица; * убедитесь, что у него есть рабочая необходимость в этой информации; * убедитесь, что информация может использоваться для заявленных целей; * передавайте информацию в строго необходимом объеме.   Хранение и удаление конфиденциальных данных  Всегда помещайте в архив или удаляйте конфиденциальные данные в соответствии с требованиями Abbott к управлению, хранению и удалению данных.  Реагирование на случайное раскрытие защищенной медицинской информации  О любом случайном или ином ненадлежащем раскрытии защищенной медицинской информации пациента немедленно сообщите в Отдел этики и комплаенс или в команду Global Privacy.  Сообщение о нарушении конфиденциальности  Свяжитесь с командой Global Privacy, чтобы сообщить о потенциальном нарушении конфиденциальности.  Чтобы узнать, сколько вы уже изучили, нажмите кнопку меню.  Отлично!  Вы изучили разделов: 3 из 4  Для продолжения нажмите стрелку вперед. |
| [Screen 44](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=55_C_45)  [55\_C\_45](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=55_C_45) | Where to Get Help  Office of Ethics and Compliance (OEC)  Global Privacy – Contact Global Privacy via email at [privacy@abbott.com](mailto:privacy@abbott.com). You can find additional contact details and important information about privacy on the Global Privacy Portal [here](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) on Abbott World.  OEC Contacts – You are encouraged to contact the OEC at any time with any ethics and compliance questions, or to discuss concerns about possible violations of our written standards, laws, or regulations.   * Visit the [Contact OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) page on the [OEC website](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) on Abbott World or [OEC@abbott.com](mailto:OEC@abbott.com).   ENTERPRISE CYBERSECURITY  Visit the Enterprise Cybersecurity site [here](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) on Abbott World.  Visit the [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) site to learn about secure ways to share information.  Legal Division  Contact the [Legal Division](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) with questions or concerns about third-party contractual obligations regarding privacy and data protection.  Contact the Information Governance team at [information.governance@abbott.com](mailto:information.governance@abbott.com) with questions or concerns regarding retention requirements or for guidance on acceptable use of technology solutions.  REFERENCE POLICIES:   * Click [here](http://abbottmfiles.oneabbott.com/#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?limit=499&00_p100=107&01_p1170*=GLB-CONF-INFO&06_p39=138_p2C131&resultsFromEachRepository=true&includeUnmanaged=true) to review the Confidential Information Policy * Click [here](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) to review Abbott’s policy on Insider Trading * Click [here](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0) to review the Acceptable Technology Use Policy. * Click [here](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0) to review the Records and Information Policy on M-Files.   OEC Policies and Procedures  For our company’s global and country-specific OEC policies and procedures:   * Abbott employees should visit [iComply](https://icomply.abbott.com/Default.aspx).   Human Resources Service Center   * Click [here](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) for a list of HR support contact numbers.   Course Resources  Transcript  Click [here](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) for a full transcript of the course. | Куда обращаться за помощью  Отдел этики и комплаенс (ОЕС)  Global Privacy — свяжитесь с головным отделом конфиденциальности по электронной почте: [privacy@abbott.com](mailto:privacy@abbott.com). Дополнительную контактную и другую важную информацию о неприкосновенности частной жизни вы найдете [здесь](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) в разделе Global Privacy на портале Abbott World .  Контакты OEC — Обращайтесь в OEC в любое время с вопросами относительно этики и нормативно-правового соответствия или для обсуждения проблем возможного нарушения наших письменных стандартов, законов или нормативно-правовых актов.   * Посетите страницу [«Связаться с Отделом этики и комплаенс»](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) на [веб-сайте Отдела этики и комплаенс](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) портала Abbott World или напишите по адресу [OEC@abbott.com](mailto:OEC@abbott.com).   ENTERPRISE CYBERSECURITY  Посетите сайт Enterprise Cybersecurity [здесь](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) на портале Abbott World.  Посетите сайт [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx), чтобы узнать о безопасных способах обмена информацией.  Юридический отдел  По вопросам и проблемам, связанным с договорными обязательствами третьих сторон в отношении конфиденциальности и защиты данных, обращайтесь в [Юридический отдел](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal).  Свяжитесь с Отделом по управлению информацией [information.governance@abbott.com](mailto:information.governance@abbott.com) с вопросами относительно требований к хранению или за консультацией в отношении правил пользования технологическими решениями.  СОПУТСТВУЮЩИЕ ПОЛОЖЕНИЯ   * Нажмите [здесь](http://abbottmfiles.oneabbott.com/#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?limit=499&00_p100=107&01_p1170*=GLB-CONF-INFO&06_p39=138_p2C131&resultsFromEachRepository=true&includeUnmanaged=true), чтобы ознакомиться с Политикой в отношении конфиденциальной информации. * Нажмите [здесь](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx), чтобы ознакомиться с Политикой Abbott в области инсайдерской торговли. * Нажмите [здесь](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0), чтобы ознакомиться с Политикой использования допустимых технологий. * Нажмите [здесь](http://abbottmfiles.oneabbott.com/Default.aspx?#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0), чтобы ознакомиться с Политикой по записи и информации в системе M-Files.   Положения и процедуры Oтдела этики и комплаенс  Глобальные и локальные положения и процедуры Oтдела этики и комплаенс:   * Сотрудники компании Abbott должны посетить [iComply](https://icomply.abbott.com/Default.aspx).   Сервисный центр отдела по работе с персоналом   * Нажмите [здесь](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) для получения списка контактных телефонов Отдела по работе с персоналом.   Материалы курса  Текстовая версия  Нажмите [здесь](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf), чтобы ознакомиться с полным текстом курса. |
| [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. | Проверка знаний состоит из 10 вопросов. Для успешного прохождения курса вам необходимо набрать как минимум 80%.  Когда будете готовы, нажмите кнопку **«Проверка знаний»**. |
| Screen 46  Question 1: Scenario  57\_C\_48 | Assuming you have worked for Abbott for several years and have recently accepted an offer to work for another company, which of the following would you be legally allowed to take with you when you leave? | Если предположить, что вы проработали в компании Abbott несколько лет и недавно приняли предложение о работе в другой компании, что из перечисленного вы по закону имеете право взять с собой при увольнении? |
| Screen 46  Question 1: Options  58\_C\_48 | [1] Personal Patient Information from clinical studies  [2] Abbott customers lists and presentation information that you created while working for Abbott  [3] Sales projections and financial data for your Abbott Division or Business Unit  [4] Personal photos and mementos | [1] Персональные данные о пациенте, полученные в ходе клинических исследований.  [2] Списки клиентов компании Abbott и информацию из презентации, которую вы создали во время работы в Abbott.  [3] Прогнозы продаж и финансовые данные вашего отдела или подразделения компании Abbott.  [4] Личные фотографии и памятные подарки. |
| Screen 46  Question 1: Feedback  59\_C\_48 | The correct answer is 4. Personal information, confidential business information, and Protected Health Information are all considered sensitive data that you cannot take with you or use after leaving Abbott. Additionally, all Abbott electronic devices and other Abbott property must be returned prior to leaving.  For more information, see  Section 3.4, Responding to Improper Disclosures. | 4 — это правильный ответ. Персональные данные, конфиденциальная деловая информация и защищенная медицинская информация считаются конфиденциальными данными, которые запрещено забирать и использовать после увольнения из компании Abbott. Кроме того, перед уходом из компании вы должны вернуть все электронные устройства и другое имущество компании Abbott.  Чтобы узнать больше, см. Раздел 3.4 «Реагирование на ненадлежащее раскрытие информации». |
| Screen 46  Question 2: Scenario  60\_C\_48 | A Marketing Manager is working on a new product launch and must create a consent form for potential customers. The form will allow for the collection and use of personal information. To align with Abbott’s practices for consent, which of the following must be true for the consent form?  Check all that apply. | Менеджер по маркетингу работает над запуском нового продукта и составляет форму согласия для потенциальных клиентов. Форма позволит собирать и использовать персональные данные. Что из перечисленного ниже верно для формы согласия, соответствующей требованиям получения согласия в компании Abbott?  Отметьте все подходящие варианты. |
| Screen 46  Question 2: Options  61\_C\_48 | [1] The form must not pressure customers into giving their consent.  [2] The form must provide customers with all the information about how their personal information will be used.  [3] The form must require customers to actively agree to the collection and use of their personal information.  [4] The form must not allow customers to withdraw their consent once they have given it. | [1] Форма не должна вынуждать клиентов давать согласие.  [2] Форма должна предоставить клиентам всю информацию о том, как будут использоваться их персональные данные.  [3] Форма должна мотивировать клиентов дать активное согласие на сбор и использование их персональных данных.  [4] Форма не должна позволять клиентам отзывать свое согласие после того, как они его дали. |
| Screen 46  Question 2: Feedback  62\_C\_48 | Abbott's practices for consent require that the form:   * Be clear and concise. * Not pressure people into giving their consent. * Provide all information about how personal information will be used. * Require people to actively agree to the collection and use of their personal information. * Allow withdrawal of consent if desired.   For more information, see  Section 1.3, Abbott’s Privacy by Design Principles. | Практика получения согласия Abbott требует, чтобы форма:   * была понятной и краткой; * не вынуждала людей давать согласие; * содержала всю информацию о том, как будут использоваться персональные данные; * мотивировала клиентов дать активное согласие на сбор и использование их персональных данных; * разрешала отзыв согласия, если это необходимо.   Чтобы узнать больше, см. Раздел 1.3 «Принципы проектируемой конфиденциальности компании Abbott». |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Раскрытие и использование конфиденциальных данных, таких как персональные данные, осуществляется в компании Abbott путем: |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] Обезличивания всех данных.  [2] Контроля доступа.  [3] Оба варианта. |
| Screen 46  Question 3: Feedback  65\_C\_48 | Disclosure and Use of personal information are managed through access controls and other processes that limit access and use to individuals in specific job functions and for the specific purposes set out in the notice for which consent was given.  For more information, see  Section 1.3, Abbott’s Privacy by Design Principles. | Раскрытие и использование персональных данных осуществляется с помощью механизмов контроля доступа и других процессов, которые обеспечивают доступ только определенным сотрудникам, а также строго для конкретных целей, которые были изложены в уведомлении и на которые получено согласие.  Чтобы узнать больше, см. Раздел 1.3 «Принципы проектируемой конфиденциальности компании Abbott». |
| Screen 46  Question 4: Scenario  66\_C\_48 | Which of the following is true in relation to the retention and disposal of personal information?  Check all that apply. | Что из перечисленного верно в отношении хранения и утилизации персональных данных?  Отметьте все подходящие варианты. |
| Screen 46  Question 4: Options  67\_C\_48 | [1] Personal information is only retained for the time necessary to achieve the purposes for which it was collected and processed.  [2] Once data is no longer required in an active production environment, it should always be disposed of.  [3] Retention and disposal of personal information is subject to any holds relating to legal matters. | [1] Персональные данные хранятся только в течение времени, необходимого для достижения целей, в которых они была получены и обработаны.  [2] После того, как данные больше не требуются в производстве, их всегда нужно утилизировать.  [3] Хранение и утилизация персональных данных всегда должны осуществляться с учетом требований о хранении информации по юридическим причинам. |
| Screen 46  Question 4: Feedback  68\_C\_48 | Generally, Abbott should only retain personal information for the time necessary to achieve the purposes for which it was collected and processed. Once data is no longer required in an active production environment, it should be either archived or disposed of, in a manner consistent with Abbott’s data management, retention, and disposal requirements. Retention and disposal requirements are also subject to any holds relating to legal matters.  For more information about the correct answer, Section 1.3, Abbott’s Privacy by Design Principles. | Как правило, компания Abbott должна хранить персональные данные не дольше, чем это необходимо для достижения целей, для которых они были собраны и обработаны. После того, как данные больше не требуются в производстве, они должны быть помещены в архив либо утилизированы согласно требованиям Abbott по работе с данными, их хранению и утилизации. Требования к хранению и утилизации также подпадают под действие любых ограничений, связанных с юридическими причинами.  Чтобы узнать больше о правильном ответе, см. Раздел 1.3 «Принципы проектируемой конфиденциальности компании Abbott». |
| Screen 46  Question 5: Scenario  69\_C\_48 | An Engineer is working on developing a new product. Which of the following would be considered confidential business information that must be kept secure?  Check all that apply. | Инженер разрабатывает новый продукт. Что из перечисленного будет считаться конфиденциальной деловой информацией, которую необходимо хранить в безопасности?  Отметьте все подходящие варианты. |
| Screen 46  Question 5: Options  70\_C\_48 | [1] Sales projections and forecasts for the new product.  [2] Financial reporting data from Abbott’s Annual Report.  [3] Purchasing information, such as bids for contracts for the new product.  [4] Competitive information about similar products.  [5] Proposals from third-party suppliers related to the new product. | [1] Прогнозы продаж и прогнозы для нового продукта.  [2] Данные финансовой отчетности, взятые из годового отчета Abbott.  [3] Информация о закупках, например, тендерные предложения по новому продукту.  [4] Информация об аналогичных продуктах конкурентов.  [5] Предложения сторонних поставщиков по новому продукту. |
| Screen 46  Question 5: Feedback  71\_C\_48 | Confidential Business Information is a broad category. It includes much of the business information we use and come in contact with on a daily basis. A good way to confirm whether something is confidential is to ask yourself a simple question:  Is this information publicly available?  If the answer is no, then the information is most certainly confidential, and you should take appropriate steps to protect it.  For more information, see Section 2.1, Recognizing Confidential Business Information. | Конфиденциальная деловая информация — это широкая категория. К ней относится бо́льшая часть деловой информации, которую мы используем, и с которой встречаемся повседневно. Для проверки того, является ли информация конфиденциальной, рекомендуется задать себе простой вопрос:  Является ли эта информация общедоступной?  Если ответ отрицательный, то информация, скорее всего, является конфиденциальной, и необходимо принять определенные меры для ее защиты.  Чтобы узнать больше, см. Раздел 2.1 «Определение конфиденциальной деловой информации». |
| Screen 46  Question 6: Scenario  72\_C\_48 | The Global Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws in the world. Implemented in 2018, it is the standard for privacy protection. This regulation was designed in: | Общий регламент ЕС по защите персональных данных (GDPR) — один из самых всеобъемлющих законов о защите персональных данных в мире. Принят в 2018 году и является стандартом защиты неприкосновенности частной жизни. Регламент был разработан в…: |
| Screen 46  Question 6: Options  73\_C\_48 | [1] Canada  [2] Asia  [3] Europe  [4] Russia  [5] United States  [6] Latin America | [1] Канаде  [2] Азии  [3] Европе  [4] России  [5] США  [6] Латинской Америке |
| Screen 46  Question 6: Feedback  74\_C\_48 | The correct answer is Europe. In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate.  For more information, see Section 1.2, Legal, Regulatory and Contractual Agreements. | Правильный ответ — в Европе. В Европе действует Общий регламент по защите персональных данных (GDPR), один из самых всеобъемлющих законов о защите персональных данных в мире, и с момента вступления в силу в 2018 году он установил стандарт защиты персональных данных, который пытаются перенять другие страны.  Для получения дополнительной информации см. Раздел 1.2 «Юридические, нормативные и договорные требования». |
| Screen 46  Question 7: Scenario  75\_C\_48 | Your colleague just completed a project that involved collecting and using personal data. He's since received a request from another department to access that data. You advise your colleague to: | Ваш коллега только что завершил проект, связанный со сбором и использованием персональных данных. Другой отдел прислал ему запрос на доступ к этим данным. Вы посоветуете коллеге: |
| Screen 46  Question 7: Options  76\_C\_48 | [1] Confirm the requester's identity and their need to access the information.  [2] Verify that the requester is authorized to have a copy of the information.  [3] Make sure that the data can be used for the requested purposes.  [4] All of the above. | [1] Проверить личность запрашивающего лица и наличие у него служебной необходимости.  [2] Убедиться, что запрашивающее лицо имеет разрешение на получение этой информации.  [3] Убедиться, что данные могут быть использованы для запрошенных целей.  [4] Все вышеперечисленное. |
| Screen 46  Question 7: Feedback  77\_C\_48 | One of the most common causes of data incidents within an organization is the improper sharing of data with unauthorized personnel. Before sharing any document or file containing sensitive data, always:   * Confirm the identity of the person making the request and the person’s need to access the information. * Check to make sure the person is authorized to have a copy of the information. * Verify that the information can be used for the purposes they are requesting to use it for. * Share only the amount of information required to meet the need, not more.   For more information, see Section 3.2, Sharing Sensitive Data. | Одна из самых распространенных причин инцидентов связанных с утечкой данных в организации — это ненадлежащее их раскрытие лицам, не имеющим соответствующих полномочий. Перед тем как передать какой-либо документ, содержащий конфиденциальные данные, во всех случаях следует:   * Подтвердить личность человека, делающего запрос, и необходимость получения им информации. * Убедиться, что у человека есть разрешение на получение информации. * Убедиться, что запрашиваемая им информация может использоваться для заявленных целей. * Передавать только тот объем информации, который необходим, и не более.   Чтобы узнать больше, см. Раздел 3.2 «Передача конфиденциальных данных». |
| Screen 46  Question 8: Scenario  78\_C\_48 | You are a Sales Representative visiting a clinic in your area. While waiting in the reception area, you accidentally misplace sensitive documents containing a patient's protected health information. What do you do? | Вы торговый представитель и заехали в клинику в своем районе. Ожидая в приемной, вы случайно потеряли конфиденциальные документы, содержащие защищенную законом медицинскую информацию пациента. Что вы должны сделать? |
| Screen 46  Question 8: Options  79\_C\_48 | [1] Notify the clinic's privacy officer.  [2] Contact your supervisor.  [3] Report the incident to OEC or a member of the Global Privacy team. | [1] Сообщить специалисту клиники по вопросам конфиденциальности.  [2] Связаться со своим руководителем.  [3] Сообщить об инциденте в Отдел этики и комплаенс или сотруднику команды Global Privacy. |
| Screen 46  Question 8: Feedback  80\_C\_48 | In response to any inadvertent disclosure of a patient’s protected health information, you should immediately report the incident to:   * OEC or a member of the Global Privacy team.   For more information, see Section 3.4, Responding to Improper Disclosures. | О любом случайном раскрытии защищенной медицинской информации пациента немедленно сообщите:   * в Отдел этики и комплаенс или в команду Global Privacy.   Чтобы узнать больше, см. Раздел 3.4 «Реагирование на ненадлежащее раскрытие информации». |
| Screen 46  Question 9: Scenario  81\_C\_48 | While traveling to work on the train, you accidentally leave your laptop containing sensitive work documents at your seat and exit the train. You realize your mistake when you reach your office and frantically search for your laptop, but it is nowhere to be found. What should you do first? | По дороге на работу вы случайно оставили в поезде ноутбук с конфиденциальными рабочими документами. Вы поняли это только в офисе, когда принялись лихорадочно искать ноутбук, но его нигде не оказалось. Что вы сделаете в первую очередь? |
| Screen 46  Question 9: Options  82\_C\_48 | [1] Call the train company and ask if someone turned in your laptop.  [2] Go back to the train station and search for your laptop.  [3] Contact your local Global Service Desk. | [1] Позвоните в железнодорожную компанию и спросите, нашел ли кто-нибудь ваш ноутбук.  [2] Вернетесь на вокзал и будете искать ноутбук.  [3] Свяжетесь с местным отделением Глобальной службы поддержки. |
| Screen 46  Question 9: Feedback  83\_C\_48 | If you believe that sensitive information may have been compromised, such as through a lost or stolen laptop, please contact your local Global Service Desk immediately.  For more information, see Section 3.4, Reporting a Data Incident. | Если вы считаете, что конфиденциальная информация могла быть раскрыта в результате, например, утери или кражи ноутбука, немедленно обратитесь в местное отделение Глобальной службы поддержки.  Чтобы узнать больше, см. Раздел 3.4 «Сообщение об инциденте, связанном с утечкой данных». |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | Вы должны использовать персональные данные только:  Отметьте все подходящие варианты. |
| Screen 46  Question 10: Options  85\_C\_48 | [1] For the specific purpose for which you have been granted access.  [2] According to the notice provided to the data subject.  [3] According to the consent granted by the data subject. | [1] Для конкретной цели, для которой вам предоставили доступ.  [2] Согласно уведомлению, предоставленному субъекту данных.  [3] В соответствии с согласием, которое дал субъект данных. |
| Screen 46  Question 10: Feedback  86\_C\_48 | If you have permission to access personal information, only use it:   * For the specific purpose for which you have been granted access. * According to the notice provided to the data subject. * According to the consent granted by the data subject.   For more information, see Section 3.1 Accessing and Using Sensitive Data. | Если у вас есть разрешение на доступ к персональным данным, используйте их только:   * Для конкретной цели, для которой вам предоставили доступ. * Согласно уведомлению, предоставленному субъекту данных. * В соответствии с согласием, которое дал субъект данных.   Чтобы узнать больше, см. Раздел 3.1 «Доступ к конфиденциальным данным и их использование». |
| [Screen 46](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48)  [87\_C\_48](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48) | All questions remain unanswered | Вы не ответили ни на один вопрос. |
| [Screen 47](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49)  [88\_C\_49](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49) | No results are available, as you have not completed the Knowledge Check.  Congratulations! You have successfully passed the Knowledge Check and completed the course.  Please review your results below by clicking on each question.  Once you are done, you must click the EXIT [X] icon in the course title bar before closing your browser window or browser tab.  Sorry, you did not pass the Knowledge Check. Take a few minutes to review your results below by clicking on each question.  When you are done, click the Retake Knowledge Check button. | Вы не прошли проверку знаний, поэтому результаты недоступны.  Поздравляем! Вы успешно прошли проверку знаний и завершили курс.  Просмотрите свои результаты ниже, нажимая на каждый вопрос.  По окончании нажмите кнопку **ВЫХОД [X]** в строке заголовка курса, прежде чем закрывать окно или вкладку браузера.  К сожалению, вы не прошли проверку знаний. Просмотрите свои результаты ниже, нажимая на каждый вопрос.  Когда будете готовы, нажмите на кнопку **Retake Knowledge Check** (повторить проверку знаний). |
| 89\_toc\_1 | Introduction | Введение |
| 90\_toc\_2 | Welcome | Добро пожаловать |
| 91\_toc\_3 | Objectives | Цели |
| 92\_toc\_4 | Menu | Меню |
| 93\_toc\_5 | Personal Information | Персональные данные |
| 94\_toc\_6 | Recognizing Personal Information | Распознавание персональных данных |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Юридические, нормативные и договорные требования. |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Принципы проектируемой конфиденциальности компании Abbott |
| 97\_toc\_9 | Review | Просмотреть |
| 98\_toc\_10 | Confidential Business Information | Конфиденциальная деловая информация |
| 99\_toc\_11 | Recognizing Confidential Business Information | Определение конфиденциальной деловой информации |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Цена отсутствия защиты конфиденциальной деловой информации |
| 101\_toc\_13 | Insider Information | Инсайдерская информация |
| 102\_toc\_14 | Review | Просмотреть |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Ваша роль в защите конфиденциальных данных |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Доступ к конфиденциальным данным и их использование. |
| 105\_toc\_17 | Sharing Sensitive Data | Передача конфиденциальных данных |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Хранение и удаление конфиденциальных данных |
| 107\_toc\_19 | Responding to Improper Disclosures | Реагирование на ненадлежащее раскрытие информации |
| 108\_toc\_20 | Review | Просмотреть |
| 109\_toc\_21 | Knowledge Check | Проверка знаний |
| 110\_toc\_22 | Introduction | Введение |
| 111\_toc\_23 | Assessment | Оценка |
| 112\_toc\_24 | Question 1 | Вопрос 1 |
| 113\_toc\_25 | Question 2 | Вопрос 2 |
| 114\_toc\_26 | Question 3 | Вопрос 3 |
| 115\_toc\_27 | Question 4 | Вопрос 4 |
| 116\_toc\_28 | Question 5 | Вопрос 5 |
| 117\_toc\_29 | Question 6 | Вопрос 6 |
| 118\_toc\_30 | Question 7 | Вопрос 7 |
| 119\_toc\_31 | Question 8 | Вопрос 8 |
| 120\_toc\_32 | Question 9 | Вопрос 9 |
| 121\_toc\_33 | Question 10 | Вопрос 10 |
| 122\_toc\_34 | Feedback | Комментарий |
| 123\_string\_1 | The Course cannot contact the LMS. Click 'OK' to continue and review the course. Note, Course Certification may not be available. Click 'Cancel' to exit | Курс не может связаться с системой LMS. Нажмите «ОК», чтобы продолжить изучение курса. Обращаем ваше внимание, что аттестация по курсу недоступна. Нажмите «Отменить» для выхода |
| 124\_string\_2 | All questions remain unanswered | Вы не ответили ни на один вопрос. |
| 125\_string\_3 | Questions | Вопросы |
| 126\_string\_4 | Question | Вопрос |
| 127\_string\_5 | not answered | ответ не предоставлен |
| 128\_string\_6 | That's correct! | Правильно! |
| 129\_string\_7 | That's not correct! | Это неверно! |
| 130\_string\_8 | Feedback: | Комментарий: |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ |
| 132\_string\_10 | Knowledge Check | Проверка знаний |
| 133\_string\_11 | Submit | Отправить |
| 134\_string\_12 | Retake Knowledge Check | Пройти проверку знаний заново |
| 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. | Описание курса: Работая в компании Abbott, мы часто используем конфиденциальные данные при принятии важных деловых решений. Поскольку многие наши стейкхолдеры проявляют озабоченность о том, как собираются и используются конфиденциальные данные, Abbott внедрила правила и процедуры для обеспечения их защиты. В данном курсе рассматривается, что представляют собой конфиденциальные данные, почему они имеют чрезвычайно важное значение для нашей компании и какие меры мы предпринимаем для обеспечения защиты и безопасности при обработке этой информации. Прохождение курса займет около 30 минут. |
| 136\_string\_14 | Menu | Меню |
| 137\_string\_15 | Resources | Ресурсы |
| 138\_string\_16 | Reference Material | Справочные материалы |
| 139\_string\_17 | Audio | Аудио |
| 140\_string\_18 | Exit | Выход |
| 141\_string\_19 | Record My Results | Сохранить результаты |