|  |  |  |
| --- | --- | --- |
| 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. | Proteção de Dados Sigilosos  Clique na seta para frente para começar. |
| [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. | Na Abbott, usamos os dados para tomar decisões e, frequentemente, esses dados contêm informações sigilosas.  Para cumprirmos nossa missão em ajudar as pessoas a viverem uma vida melhor por meio da boa saúde, é essencial mantermos esses dados protegidos e cumprir com as leis e padrões de ética que a Abbott defende. Este curso foi criado para proporcionar a você as habilidades necessárias para apoiar esta tarefa. |
| [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. | Após concluir este curso, você entenderá melhor:   * o que são dados sensíveis; * como protegemos esses dados na Abbott; * seu papel na proteção de dados sigilosos; e * o que fazer caso ache que dados sigilosos possam ter sido indevidamente divulgados ou comprometidos. |
| [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 | Informações pessoais  Aqui você aprenderá como governos, consumidores e o público em geral têm estado cada vez mais atentos à privacidade e segurança das informações pessoais.  12 minutos  Seção 1 | Informações pessoais  Como reconhecer informações pessoais  Exigências legais, regulatórias e contratuais  Princípios de Privacidade por Design da Abbott  Revisão  2 | Informações confidenciais de negócios  Aqui você aprenderá como a maioria das informações que usamos em nossas atividades profissionais cotidianas são consideradas confidenciais.  5 minutos  Seção 2 | Informações confidenciais de negócios  Como reconhecer informações confidenciais de negócios  Custo de não proteger as informações confidenciais de negócios  Informações privilegiadas  Revisão  3 | Proteção de dados sigilosos  Aqui você aprenderá sobre o que pode fazer para ajudar a proteger dados sigilosos.  8 minutos  Seção 3 | Seu papel na proteção de dados sigilosos  Acesso e uso de dados sigilosos  Compartilhamento de dados sigilosos  Retenção e descarte de dados sigilosos  Respondendo a divulgações indevidas  Revisão  4 | Teste de conhecimento  Avalie sua compreensão dos principais conceitos e princípios deste curso.  5 minutos  Seção 4 | Teste de conhecimento  Avaliação  Clique no painel para começar.  Clique no botão de reprodução amarelo para começar.  Este conteúdo ainda não está disponível. Você precisa concluir a Seção{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. | Na Abbott, um dos tipos comuns de dados sigilosos que utilizamos são as informações pessoais.  Nos últimos anos, governos, consumidores e o público em geral têm estado cada vez mais atentos à privacidade e segurança das informações pessoais. |
| [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. | Informações pessoais são informações que podem ser usadas para entrar em contato, localizar ou, de outra forma, identificar um indivíduo. |
| [Screen 6](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9)  [7\_C\_9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9) | Kandice | Marketing Manager  Can you give me some examples of personal information?  Personal information can include biographical information, such as name, date of birth, email address and phone number.  It can include information relating to an individual’s appearance, such as hair color or weight.  It can also include information relating to an individual’s personal life, such as photos, browser cookies or location tracking information. | Kandice | Gerente de marketing  Você poderia dar alguns exemplos de informações pessoais?  Informações pessoais podem incluir informações biográficas, como nome, data de nascimento, endereço de e-mail e número de telefone.  Isso pode incluir informações relacionadas à aparência de um indivíduo, como cor do cabelo ou peso.  Esses dados também podem incluir informações sobre a vida pessoal de um indivíduo, como fotos, cookies de navegador ou rastreamento de localização. |
| [Screen 7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10)  [8\_C\_10](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10) | Jerry | Sales Representative  Does personal information also include protected health information?  Yes, it does.  Protected health information (PHI) is a particularly sensitive type of personal information used in the healthcare industry. It includes any personally identifiable information in medical records, including conversations between medical professionals about treatment. | Jerry | Representante de vendas  Informações pessoais também podem abranger informações de saúde protegidas?  Podem sim.  Dados protegidos de saúde (Protected health information, PHI) representam uma categoria de informação pessoal especialmente sigilosa, que é utilizada na indústria de cuidados para saúde. Esses dados incluem qualquer informação de identificação pessoal que conste em registros médicos, incluindo conversas entre profissionais médicos a respeito do tratamento. |
| [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. | Na maioria dos países onde a Abbott realiza negócios, há leis e regulamentações em vigor com o objetivo de proteger informações pessoais, incluindo informações de saúde protegidas.  As leis relacionadas à privacidade e à proteção das informações pessoais diferem entre os países, mas, em geral, abrangem os mesmos princípios centrais.  CLIQUE EM CADA UMA DAS ÁREAS DESTACADAS NA TELA PARA SE INFORMAR SOBRE OS DIFERENTES TIPOS DE LEIS E REQUISITOS DE PRIVACIDADE EM VIGOR NO MUNDO INTEIRO. |
| [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. | Europa  Na Europa, o Regulamento Geral sobre a Proteção dos Dados (GDPR) é uma das leis de privacidade mais abrangentes em âmbito global, e desde sua implementação em 2018, determinou o padrão de proteção de privacidade que outros países tentam seguir. O GDPR se aplica a organizações localizadas na Europa e a organizações localizadas fora da Europa, caso ofereçam mercadorias e serviços para qualquer indivíduo que resida na Europa ou caso monitorem seu comportamento.  Um dos principais conceitos do GDPR é o direito de apagamento, também conhecido como o direito ao esquecimento. Esse direito concede a pessoas a capacidade de solicitar que seus dados pessoais sejam apagados do registro de uma organização. Se uma pessoa faz tal solicitação, a organização precisa adotar medidas para apagar os dados de seus sistemas e impedir seu uso ou divulgação futuros. Pode haver exceções a solicitações de titulares de dados. Contudo, a Abbott informará cada titular de dados validado sobre a ação adotada para cada solicitação. As violações do GDPR podem resultar em multas pesadas para as empresas, até 4% do faturamento anual global, ou 20 milhões de euros (o que for maior), para a maioria dos delitos graves. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11)  [11\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11) | United States  In the United States, there is no single law that protects all personal information. Instead, there are privacy laws and regulations that apply to specific industries and types of data. For example, HIPAA protects the privacy of healthcare data, while the Fair Credit Reporting Act protects credit information.  However, some states have begun enacting their own comprehensive data privacy laws. For instance, California has the California Consumer Privacy Act (CCPA), which gives Californians certain rights to their data, such as the right to know what personal information is being collected about them and the right to delete any personal information collected. The CCPA will be amended by the California Privacy Rights Act (CPRA) in 2023, which will give people even more rights to their data.  Other states that have passed their own data privacy laws include Virginia, Colorado, Utah, and Connecticut. While each state's law is different, they all generally give people rights to their data and require companies to provide certain disclosures about their data processing activities.  Fines for violating state privacy laws can be significant. For example, California can fine companies up to $7,500 USD per violation of the CCPA.  Canada  There are laws at both the federal and provincial levels in Canada that are designed to protect an individual's personal information. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that applies to private sector organizations and is enforced by the Office of the Privacy Commissioner of Canada.  At the provincial level, Quebec, Alberta, and British Columbia have enacted privacy laws that are similar to PIPEDA. Some other provinces also have rules in place that provide similar protections for personal information, including the provinces of Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia, which have enacted health information privacy laws.  These laws are in place to help prevent personal information from being mishandled or collected without the individual's knowledge, and give people the right to access their own information and correct any errors.  Violating these laws can result in significant fines. For example, violating PIPEDA can lead to a fine of up to $100,000. In Alberta, the Personal Information Protection Act (PIPA) allows for fines of up to $10,000 for individuals and $500,000 for organizations. | Estados Unidos  Nos Estados Unidos, não há uma única lei que proteja todas as informações pessoais. Em vez disso, existem leis de privacidade e regulamentos que se aplicam a setores e tipos de dados específicos. Por exemplo, a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) protege a privacidade dos dados de saúde, enquanto a Lei de Relatório de Crédito Justo protege as informações de crédito.  Todavia, alguns estados começaram a promulgar suas próprias leis abrangentes de privacidade de dados. Por exemplo, a Califórnia tem a Lei de Privacidade do Consumidor da Califórnia *(California Consumer Privacy Act, CCPA)*, que dá aos californianos certos direitos sobre seus dados, como o direito de saber quais informações pessoais estão sendo coletadas sobre eles e o direito de excluir quaisquer informações pessoais coletadas. A CCPA será alterada pela Lei de Direitos Privados da Califórnia *(California Privacy Rights Act, CPRA)* em 2023, dando às pessoas mais direitos sobre seus dados.  Outros estados que passaram a ter suas próprias leis de privacidade de dados incluem Virgínia, Colorado, Utah e Connecticut. Embora a lei de cada estado seja diferente, todas elas dão às pessoas direitos sobre seus dados e exigem que as empresas divulguem algumas de suas atividades de processamento de dados.  As multas por violação das leis estaduais de privacidade podem ser pesadas. Por exemplo, a Califórnia pode multar uma empresa em até US$ 7.500 por violação da CCPA.  Canadá  Existem leis tanto no âmbito federal como provincial no Canadá que foram elaboradas para proteger as informações pessoais de um indivíduo. Por exemplo, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos *(Personal Information Protection and Electronic Documents Act, PIPEDA)* é uma lei federal que se aplica a organizações do setor privado e é aplicada pelo Escritório do Comissário de Privacidade do Canadá.  Em nível provincial, Quebec, Alberta e Colúmbia Britânica promulgaram leis de privacidade que se assemelham à PIPEDA. Outras províncias têm regras em vigor que oferecem proteções similares das informações pessoais, como as províncias de Ontário, Nova Brunswick, Newfoundland e Labrador e Nova Escócia que promulgaram leis de privacidade de informações de saúde.  Essas leis existem para evitar a coleta ou manipulação indevida de informações pessoais sem o conhecimento do indivíduo e para dar às pessoas o direito de acessar seus próprios dados e corrigirem erros.  A violação dessas leis pode resultar em multas consideráveis. Por exemplo, uma violação da PIPEDA pode resultar em uma multa de até US$ 100.000. Em Alberta, a Lei de Proteção de Informações Pessoais (PIPEDA) prevê multas de até US$ 10.000 para pessoas físicas e US$ 500.000 para organizações. |
| [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 $737,000 USD) for violating the country’s privacy law. | Ásia-Pacífico  As leis de privacidade na região do Pacífico Asiático estão em constante expansão e se tornando mais abrangentes. Alguns países, como a China, implementaram medidas de localização de dados que exigem que as empresas armazenem alguns dados pessoais em seus servidores em território nacional. Além disso, a China tem requisitos de avaliação de impacto à privacidade e segurança para transferência transfronteiriça de informações pessoais.  Outros países, como Austrália e Singapura, adotaram uma abordagem da privacidade mais focada no consumidor, que dá às pessoas maior controle sobre suas informações, inclusive o direito de saber como as empresas utilizam suas informações, e a capacidade de acessá-las e corrigi-las, se necessário.  As penalidades de empresas que violam as leis de privacidade de dados também diferem bastante entre as regiões. Na China, por exemplo, as empresas podem ser multadas em até 500.000 RMB (US$ 72.000 aproximadamente) por violar as leis de privacidade de dados.  Em Singapura, todavia, as empresas podem ser multadas em até 1 milhão de dólares (Singapura) (cerca de US$ 737.000) por violar as leis de privacidade do país. |
| [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 $216,000 USD for the second offense. | Rússia  A Rússia também tem leis que protegem os dados dos cidadãos, incluindo uma lei de localização de dados que exige que as empresas armazenem os dados pessoais de cidadãos russos em servidores localizados na Rússia.  A lei se aplica a empresas que processam dados de cidadãos russos, independentemente de estarem ou não localizadas na Rússia. Dessa forma, por exemplo, uma empresa americana que processa dados de cidadãos russos precisa cumprir a lei.  Como em muitos países, a lei também exige que a empresa adote medidas para proteger os dados pessoais que ela processa. Por exemplo, as empresas precisam garantir que os dados sejam precisos e atualizados e adotar medidas para impedir sua utilização indevida, roubo ou perda.  As multas por violação da lei podem variar de US$ 12.000 a US$ 72.000 na primeira vez, e até US$ 216.000 na reincidência. |
| [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. | América Latina  A maioria dos países da América Latina têm leis em vigor que protegem a privacidade das pessoas. Entretanto, muitos países da região, como Equador, Argentina e Brasil, recentemente revisaram as regulamentações de privacidade existentes para atualizá-las de acordo com os padrões internacionais.  O Equador, por exemplo, aprovou recentemente a Lei Orgânica de Proteção de Dados Pessoais *(Law on the Protection of Personal Data, LPPD)*, que entrará em vigor em 2023. Esta lei se aplica a qualquer empresa no mundo que processe dados pessoais de indivíduos no Equador.  Como outras leis na região, a LPPD exige que as empresas notifiquem e obtenham o consentimento das pessoas antes de usar seus dados, destruí-los quando não são mais necessários e atender a certas restrições antes que os dados sejam compartilhados com outros países. Essas medidas ajudam a proteger a privacidade das pessoas na América Latina e garantem que as empresas sejam responsabilizadas pelo tratamento de dados pessoais.  As violações da LPPD podem resultar em multas significativas que variam de 3 a 17% da receita anual de uma organização no ano anterior, servindo de grande incentivo para que as empresas cumpram a lei. |
| [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. | Além das leis e regulamentações que regem a forma como a Abbott conduz seus negócios, os contratos que firmamos com clientes podem estar sujeitos a regulamentações adicionais.  Por exemplo, o governo dos EUA é um cliente da Abbott. Nos termos desse contrato, somos obrigados a cumprir as exigências estabelecidas pela Lei de Privacidade dos EUA, promulgada em 1974.  CLIQUE NO BOTÃO “LEI DE PRIVACIDADE” PARA SABER MAIS. |
| [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. | Lei de Privacidade  A Lei de Privacidade de 1974 (5 U.S.C. 552a) é uma importante regulamentação federal. A lei estabelece um Código de práticas justas de informações que rege a coleta, manutenção, utilização e disseminação das informações de identificação pessoal de indivíduos que são armazenadas nos sistemas de registros das agências federais. Para determinadas transações, a Abbott pode receber acesso aos registros de agências governamentais. Nesses casos, a Abbott é obrigada a cumprir diversas exigências, incluindo a necessidade de comprovar a realização de um treinamento de privacidade sobre proteção de informações de identificação pessoal.  Antes de firmar qualquer acordo com clientes que têm obrigações de privacidade, os funcionários devem consultar o Departamento Jurídico. |
| [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. | As leis, regulamentações e exigências contratuais que acabamos de conhecer são, muitas vezes, complexas e podem mudar rapidamente.  A Abbott tem em vigor políticas e procedimentos que asseguram o cumprimento dessas leis e regulamentações pelos nossos funcionários. Se você tiver dúvidas ou quiser saber mais, fale com o OEC [*Office of Ethics and Compliance* (Escritório de Ética e Conformidade)] ou com um membro da equipe de Privacidade Global.  Para contatos e informações adicionais, clique no ícone Recursos. |
| [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 | Coleta   * Aviso * Consentimento   GERENCIAMENTO   * Integridade dos Dados * Acesso e Correção   Uso   * Divulgação e Uso   Descarte   * Retenção e Descarte   Os procedimentos e as políticas de privacidade e proteção de dados da Abbott são baseados em um conjunto simples de princípios. Chamamos esse conjunto de princípios de Privacidade por Design.  Esses princípios têm a finalidade de ajudar os funcionários a proteger dados sigilosos em cada estágio do ciclo de vida desses dados. Para ilustrar, vamos tratar especificamente as informações pessoais.  O primeiro estágio do ciclo de vida dos dados é a coleta.  Durante esse estágio, a Abbott utiliza diversos métodos para coletar informações pessoais. Por exemplo, podemos solicitar que os consumidores forneçam dados de contato em um site da Abbott, ou podemos capturar dados pessoais gerados por um de nossos dispositivos.  No intuito de proteger os direitos de privacidade dos indivíduos durante esse estágio, adotamos processos que garantem nosso cumprimento dos princípios Privacidade por Design relacionados a Avisos e Consentimento.  O princípio do aviso de privacidade se refere a informar às pessoas quais informações pessoais estão sendo coletadas e explicar, utilizando uma linguagem clara, precisa e não ambígua, como pretendemos usar essas informações.  Por exemplo, quando o cliente envia uma consulta pelo site abbott.com, as informações pessoais que coletamos são utilizadas com o único intuito de responder a essa consulta.  O princípio de consentimento se refere a oferecer aos indivíduos a oportunidade de concordar com a coleta e utilização de suas informações pessoais.  De modo geral, quando solicitamos consentimento, garantimos que ele seja:   * Fornecido livremente. O indivíduo nunca é coagido nem informado de que o consentimento é obrigatório. * Informado. O indivíduo recebe informações suficientes para tomar uma decisão fundamentada sobre o que está consentindo. * Afirmativo. O indivíduo deve fornecer seu consentimento de maneira afirmativa. Nunca consideramos que houve consentimento, por exemplo, com base no silêncio de um indivíduo, nem exigimos que o indivíduo realize alguma ação para negar seu consentimento, como desmarcar uma caixa de seleção. * Revogável. O indivíduo recebe uma clara explicação sobre como revogar o consentimento.   Por exemplo, ao se cadastrar no programa de Recompensas Nutrition Similac© Strong Moms© da Abbott, um consumidor pode consentir com a coleta e utilização de suas informações pessoais quando aceita (por ex., marcando uma caixa de seleção) receber outras informações promocionais.  O segundo estágio do ciclo de vida dos dados é o gerenciamento.  Durante esse estágio, as informações são processadas e armazenadas.  No intuito de proteger as informações pessoais durante esse estágio, adotamos processos que garantam nosso cumprimento dos seguintes princípios:   * Integridade de dados; e * Acesso e correção.   A integridade dos dados trata da adoção de medidas razoáveis para assegurar que as informações pessoais que retemos são precisas, completas e atualizadas.  Uma das formas pelas quais fazemos isso é monitorando e registrando todas as atividades que processam informações pessoais. Isso garante que possamos identificar a origem dos dados, as finalidades específicas para as quais foram processados e onde estão armazenados.  O princípio de acesso e correção trata de oferecer aos indivíduos acesso razoável aos próprios dados e a oportunidade de que exerçam os direitos relacionados a esses dados.  Isso inclui responder às solicitações, realizadas pelos indivíduos, de acesso, exclusão, transferência ou correção de registros armazenados de informações pessoais.  O terceiro estágio do ciclo de vida é o uso.  Durante esse estágio, informações pessoais são usadas em suporte às atividades realizadas em toda a organização.  No intuito de proteger as informações pessoais durante esse estágio, adotamos processos que garantam o cumprimento do princípio de Divulgação e Uso.  O princípio de Divulgação e Uso trata de controlar quem tem acesso às informações pessoais e de limitar o uso delas para fins específicos.  Gerenciamos esse princípio por meio de controles de acesso e outros processos. Esses controles e processos limitam o acesso a indivíduos de determinados cargos, além de restringir o uso às finalidades específicas descritas no aviso para o qual o consentimento foi dado.  O estágio final do ciclo de vida é o descarte.  O descarte refere-se ao que acontece com os dados depois que eles deixam de ser usados ativamente. As atividades podem incluir exclusão, arquivamento ou retenção para fins de custódia legal.  No intuito de proteger as informações pessoais durante esse estágio, adotamos políticas e processos que garantam o cumprimento do princípio de Retenção e Descarte.  O princípio de Retenção e Descarte diz respeito ao armazenamento de informações pessoais apenas durante o período necessário para alcançar os objetivos pelos quais foram necessárias e processadas.  Quando as informações pessoais não são mais necessárias em um ambiente de produção ativa, a Abbott implementa processos para arquivá-las ou descartá-las conforme os requisitos de gerenciamento, retenção e descarte de dados da empresa. Nossos requisitos de retenção e descarte também estão sujeitos a quaisquer requisitos de retenção legal relacionados a questões jurídicas.  Para obter mais informações sobre os requisitos de retenção ou descarte, consulte a Política Global de Registros e Informações (I1-02) da Abbott ou entre em contato com o Departamento de Registro e Governança de Informações. A seção Recursos deste treinamento traz mais detalhes.  Para contatos e informações adicionais, clique no ícone Recursos.  Como acabamos de ver, nossos procedimentos e políticas visam proteger as informações pessoais ao longo de todo o seu ciclo de vida.  Para isso, aderimos aos princípios de:   * Aviso; * Consentimento; * Integridade dos dados; * Acesso e correção; * Divulgação e uso; e * Retenção e descarte.   COLETA  Aviso  Consentimento  GERENCIAMENTO  Integridade dos Dados  Acesso e Correção  USO  Divulgação e Uso  DESCARTE  Retenção e Descarte |
| [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 | Clique na seta para começar sua revisão.  Revisão  Reserve um tempo para rever alguns dos principais conceitos abordados nesta seção.  Informações Pessoais (IP)  IP são qualquer informação que possa ser usada para   * contatar; * localizar; ou * identificar um indivíduo.   Informações de saúde protegidas (PHI)  As PHI representam uma categoria de informação pessoal especialmente sigilosa que é utilizada na indústria de cuidados para saúde.  Leis de privacidade  As leis de privacidade diferem de um país para o outro, mas muitas vezes abrangem os mesmos princípios centrais.  Princípios de Privacidade por Design da Abbott  Os procedimentos e as políticas de privacidade e proteção de dados da Abbott são baseados em um conjunto simples de princípios denominado Privacidade por Design.  Aviso e Consentimento  O princípio de Aviso e Consentimento serve para informar as pessoas sobre quais IP estão sendo coletadas e dar a elas a oportunidade de concordar com a coleta.  Integridade dos Dados  A Integridade dos Dados trata da adoção de medidas razoáveis para assegurar que as IP que retemos são precisas, completas e atualizadas.  Acesso e Correção  O princípio de Acesso e Correção diz respeito a dar às pessoas o direito de acessar e corrigir os próprios dados.  Divulgação e Uso  O princípio de Divulgação e Uso diz respeito ao controle de acesso a IP.  Retenção e Descarte  O princípio de Retenção e Descarte diz respeito ao armazenamento de IP apenas durante o período necessário para alcançar os objetivos pelos quais foram necessárias e processadas.  Para ver o seu progresso, clique no botão Menu  Excelente trabalho!  Você concluiu a seção 1 de 4  Clique na seta para frente para continuar a aprender |
| [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. | Outro tipo de dados sigilosos que usamos frequentemente são as informações confidenciais de negócios.  Informações confidenciais de negócios são uma categoria ampla. Elas incluem grande parte das informações de negócios que usamos e com as quais temos contato diariamente. Informações confidenciais são informações que não estão publicamente disponíveis e que podem ser úteis para concorrentes da Abbott ou prejudiciais à empresa, se divulgadas. |
| [Screen 14](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=21_C_18)  [21\_C\_18](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=21_C_18) | Kandice | Marketing Manager  Can you give me some examples of confidential business information?  Confidential business information can include, but is not limited to: product designs and processes, compositions, organisms, computer software, research and development data, clinical and pharmacological data, patient data, technical data, customer and prospective customer lists, business practices, marketing plans and strategies, financial and operational data, and personnel data.  It can also include purchasing information, such as bids for contracts, supplier lists, and costing information. | Kandice | Gerente de marketing  Você poderia dar algum exemplo de informações confidenciais de negócios?  As informações confidenciais de negócios podem incluir, entre outras: projetos e processos de produtos, composições, organismos, software de computador, dados de pesquisa e desenvolvimento, dados clínicos e farmacológicos, dados de pacientes, dados técnicos, listas de clientes atuais e potenciais, práticas comerciais, planos e estratégias de marketing, dados financeiros e operacionais e dados pessoais.  Elas também abrangem informações de compras, como licitações para contratos, listas de fornecedores e informações de custo. |
| [Screen 15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19)  [22\_C\_19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19) | Jerry | Sales Representative  Are there certain types of confidential business information that are more sensitive than others?  Yes. Certain types of confidential business information require greater care than normal because improper disclosure or use of this information can cause serious harm to the company.  Examples include:   * Trade secrets, manufacturing formulas and processes; * Clinical and regulatory data, regulatory submissions, or pre-approval information; and * Financial data that has not been released to the public. | Jerry | Representante de vendas  Existem tipos de informações confidenciais de negócios que são mais sigilosos do que outros?  Sim. Alguns tipos de informações confidenciais de negócios requerem mais cuidado do que o normal, pois a divulgação ou utilização indevida dessas informações podem prejudicar gravemente a empresa.  Alguns exemplos:   * segredos comerciais, fórmulas e processos de fabricação; * dados clínicos e regulatórios, registros regulatórios ou informações de pré-aprovação; e * dados financeiros que não foram divulgados para o público. |
| [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. | Como você pode ver, muitas das informações que usamos em nossas atividades profissionais cotidianas são consideradas confidenciais.  Uma forma de confirmar se as informações de negócios que você está usando são confidenciais é se fazer uma pergunta simples:  Essas informações estão disponíveis publicamente?  Se a resposta for “não”, as informações devem ser consideradas confidenciais, e será necessário adotar medidas apropriadas para protegê-las. |
| [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. | Também é importante lembrar que qualquer informação confidencial de negócios criada como parte de sua função na Abbott é propriedade da Abbott.  Consequentemente, você precisa proteger essas informações e não pode retê-las em caso de término do vínculo de trabalho com a 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. | Proteger as informações confidenciais de negócios é essencial.  Não surpreendentemente, o uso indevido ou divulgação dessas informações pode resultar em danos significativos para a Abbott. |
| [Screen 19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=26_C_20d)  [26\_C\_20d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=26_C_20d) | The improper use or disclosure of confidential information can significantly harm Abbott’s relationship with its customers and clients, lead to embarrassing press and media coverage, and result in the loss of competitive advantages for Abbott. It can also result in civil lawsuits and criminal penalties, including against current and former employees.  CLICK THE ‘RECENT CASES’ BUTTON FOR MORE INFORMATION. | O uso indevido ou divulgação de informações confidenciais pode prejudicar significativamente o relacionamento da Abbott com seus consumidores e clientes, gerar uma cobertura constrangedora da imprensa e da mídia, e causar a perda de vantagens competitivas para a Abbott. Também pode resultar em ações civis e penalidades criminais contra funcionários atuais e ex-funcionários.  CLIQUE NO BOTÃO “CASOS RECENTES” PARA MAIS INFORMAÇÕES. |
| [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 $625 billion to publicly traded companies. | CASOS RECENTES  Nos anos recentes, as empresas receberam vereditos positivos e indenizações de antigos funcionários por apropriação indevida de informações da empresa. Por exemplo, uma empresa obteve uma indenização de US$ 240 milhões de um ex-funcionário que indevidamente divulgou informações confidenciais a um concorrente. Outra empresa obteve uma sentença favorável de US$ 854 milhões contra um ex-funcionário e seu novo empregador quando esse ex-funcionário se apropriou indevidamente das informações confidenciais da empresa e, em seguida, as utilizou em nome do novo empregador.  Segundo estudos, o roubo de informações confidenciais causa prejuízos entre US$ 209 e 625 bilhões a empresas de capital aberto. |
| [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 $10 million or three times the value of the confidential information.  CLICK THE ‘FINES AND PENALTIES’ BUTTON FOR MORE INFORMATION. | Não é de se surpreender que as autoridades levam o roubo de informações confidenciais muito a sério.  Por exemplo, segundo as leis criminais federais, uma pessoa pode pegar até dez anos de prisão e receber uma multa de US$ 5 milhões por roubar informações confidenciais. Além disso, se uma empresa for considerada culpada de roubar informações confidenciais, ela pode ser multada em US$ 10 milhões ou 3 vezes o valor das informações confidenciais.  CLIQUE NO BOTÃO “MULTAS E PENALIDADES” PARA MAIS INFORMAÇÕES. |
| [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 $60 Million for stealing another company’s confidential information; * A former IT employee was sentenced to 97 months in prison for stealing confidential information; * A former salesman was sentenced to 12 months in prison for stealing confidential information; * A senior executive was sentenced to 24 months in prison for stealing confidential information; and * A research scientist was sentenced to 18 months in prison for stealing confidential information. | MULTAS E PENALIDADES  Nos últimos anos, muitas pessoas e empresas foram multadas e sentenciadas à prisão pelo roubo de informações confidenciais. Por exemplo:   * um concorrente foi multado em US$ 60 milhões por roubar informações confidenciais de outra empresa; * um ex-funcionário de TI foi condenado a 97 meses de prisão por roubo de informações confidenciais; * um ex-vendedor foi condenado a 12 meses de prisão por roubo de informações confidenciais; * um executivo sênior foi condenado a 24 meses de prisão por roubo de informações confidenciais; e * um cientista pesquisador foi condenado a 18 meses de prisão por roubo de informações confidenciais. |
| [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. | Outro tipo de informações confidenciais de negócios que são importantes reconhecer e proteger são as *informações privilegiadas*.  Informações privilegiadas são informações materiais não públicas que, se divulgadas publicamente, possivelmente comprometeriam o valor de mercado das ações de uma empresa ou influenciariam as decisões dos investidores quanto à compra ou à venda de ações. |
| [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. | Os exemplos de informações privilegiadas incluem:   * notícia sobre uma possível aquisição; * atraso no lançamento de um produto; * notícia de uma violação dos sistemas internos de TI; * mudanças não previstas nas taxas de lucros ou dividendos; * ofertas de compra ou propostas de divisões de ações; * informações sobre produtos novos importantes; * concessões de contratos; * planos de expansão; e * litígios ou processos regulatórios significativos, etc. |
| [Screen 23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23)  [32\_C\_23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23) | If you are aware or in possession of insider information, it is illegal to trade in, or recommend others to trade in, Abbott securities.  This also applies to the buying and selling of securities of other companies, including those currently doing or expected to do business with Abbott.  To learn more about Abbott’s expectations with regard to the use and protection of unpublicized information, review Abbott’s policy on Insider Trading. Details can be found in the Resources section of this training. | Se você tem conhecimento ou posse de informações privilegiadas, é ilegal comercializar ou recomendar que outros comercializem os títulos da Abbott.  Isso também se aplica à compra e venda de títulos de outras empresas, incluindo aquelas que atualmente fazem ou que potencialmente farão negócios com a Abbott.  Para saber mais sobre as expectativas da Abbott com relação ao uso e à proteção de informações não divulgadas publicamente, analise a Política sobre Informações Privilegiadas da Abbott. A seção Recursos deste treinamento traz mais detalhes. |
| [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 | Clique na seta para começar sua revisão.  Revisão  Reserve um tempo para rever alguns dos principais conceitos abordados nesta seção.  Informações Confidenciais de Negócios  Qualquer informação de negócio que não esteja publicamente disponível deve ser considerada confidencial. Isso inclui grande parte das informações de negócio que usamos em nossas atividades de trabalho diárias.  Uso indevido de informações confidenciais de negócios  O uso indevido ou divulgação de informações confidenciais de negócios pode resultar em danos significativos à Empresa, seus clientes e funcionários.  Informações privilegiadas  Informações privilegiadas são informações materiais não públicas que, se divulgadas publicamente, possivelmente comprometeriam o valor de mercado das ações de uma empresa ou influenciariam as decisões dos investidores quanto à compra ou à venda de ações.  Para ver o seu progresso, clique no botão Menu  Excelente trabalho!  Você concluiu a seção 2 de 4  Clique na seta para frente para continuar a aprender |
| [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. | Agora que você tem um bom entendimento dos diferentes tipos de dados que provavelmente vai encontrar durante seu dia de trabalho, veja o que você pode fazer para ajudar a proteger esses dados. |
| [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. | Antes de acessar quaisquer dados sigilosos, certifique-se de que sua função e suas responsabilidades exigem o acesso aos dados.  Se você tiver alguma dúvida sobre se deve acessar os dados, principalmente no que diz respeito às informações pessoais, entre em contato com seu gerente, o time de OEC ou um membro da equipe de Privacidade Global.  CLIQUE NO BOTÃO “VOCÊ SABIA?” PARA MAIS INFORMAÇÕES. |
| [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. | VOCÊ SABIA?  A Abbott pratica várias formas de monitoramento legal para reduzir o risco de uso indevido de dados.  Isso inclui o monitoramento de download de dados ou o envio de dados para endereços de e-mail que não pertencem à Abbott. |
| [Screen 27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27)  [37\_C\_27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27) | If you have permission to access sensitive data, only use it for the specific purpose for which you have been granted access.  In the case of personal information, only use the data according to the consent given or notice provided. | Se você tiver permissão para acessar dados sigilosos, utilize-os somente no intuito específico para o qual você recebeu acesso.  No caso das informações pessoais, utilize os dados apenas de acordo com o consentimento dado ou o aviso fornecido. |
| [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. | Antes de compartilhar dados sigilosos, certifique-se de que a pessoa com quem você planeja compartilhar tenha a devida autorização.  Se você não tiver certeza se deve acessar os dados, especialmente no que diz respeito às informações pessoais, fale com o seu gerente ou um membro da equipe de Privacidade da 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. | Solicitações do seu próprio país  Caso um funcionário da Abbott localizado no mesmo país que você solicite dados sigilosos, sempre:   * Confirme a identidade da pessoa que está fazendo a solicitação; * Confirme que a pessoa tem necessidade de acessar as informações; * Verifique se a pessoa está autorizada a receber as informações; * Verifique se as informações podem ser usadas para a finalidade solicitada; e * Compartilhe apenas o volume de informações necessário para atender à necessidade em questão, nunca mais do que isso.   Em caso de dúvida, entre em contato com o OEC ou a equipe de Privacidade Global antes de compartilhar dados sigilosos. |
| [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. | Solicitações de outros países  Muitos países e regiões têm leis elaboradas para proteger os direitos de seus cidadãos, e impõem restrições para a transferência internacional de informações pessoais.  Se um colega em um país diferente do seu solicitar informações que contêm dados sigilosos, antes de prosseguir, consulte as políticas de privacidade de dados da sua região ou função ou consulte o time de OEC ou a equipe de Privacidade Global. Em seguida, siga as mesmas etapas caso você estivesse atendendo a uma solicitação de um colega no seu próprio país. |
| [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. | Solicitações de terceiros  Se a solicitação de dados sigilosos partir de um terceiro, certifique-se de que haja um acordo contratual válido e apropriado em vigor. Em caso de dúvida, entre em contato com o time de OEC, a equipe de Privacidade Global ou o departamento Jurídico antes de compartilhar esses dados. |
| [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. | Sempre arquive ou descarte dados sigilosos de acordo com os requisitos de gerenciamento, retenção e descarte de dados da Abbott. |
| [Screen 33](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=43_C_36)  [43\_C\_36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=43_C_36) | If you receive a legal hold order, you are prohibited from discarding, destroying, or deleting any information covered by the hold.  If you have questions related to legal hold orders or retention and disposal, contact the attorney/paralegal listed in the Legal Hold notification, or call the Litigation Department at (224) 667-5701. | Se receber uma ordem judicial para retenção de dados, você está proibido de descartar, destruir ou excluir qualquer informação abrangida pela determinação judicial .  Em caso de dúvidas quanto a ordens ou processos judiciais para retenção e descarte de dados, entre em contato com o advogado indicado na notificação judicial ou com o Departamento Jurídico da Abbott. |
| [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. | Tenha cuidado especial com dados sigilosos sempre que alguém sair da Abbott.  Os gerentes precisam se certificar de que o(a) funcionário(a) em processo rescisório tenha seu acesso cancelado no respectivo sistema (por ex., Workday para funcionários ou Fieldglass para temporários) assim que ele(a) receber a notificação de que ele(a) está deixando a empresa. Isso garantirá que o acesso aos dados da Abbott, o acesso físico aos edifícios e o pagamento final sejam gerenciados de maneira adequada. |
| [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. | Certifique-se para que o funcionário não saia da empresa levando consigo dados sigilosos. Transfira todos os arquivos para o funcionário da Abbott que assumirá a função ou as responsabilidades da pessoa que está se desligando da empresa.  Lembre o funcionário que sairá da empresa da obrigação de não reter nem divulgar informações sigilosas. Os funcionários não podem levar o produto de seu trabalho nem qualquer outra propriedade da Abbott (por exemplo, dispositivos móveis) ao saírem da Abbott. Se você tiver dúvidas sobre seus processos de rescisão locais, entre em contato com o departamento de Recursos Humanos. |
| [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. | As divulgações inadvertidas de PHI podem acontecer a qualquer momento.  Por exemplo, você pode escutar uma enfermeira falando sobre o estado de saúde de um paciente, ou receber por acidente a cópia de um e-mail que contém dados do prontuário de um paciente. |
| [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. | Caso ocorra a divulgação acidental de dados protegidos de saúde (PHI) de um paciente, você deve comunicar o incidente imediatamente para o time de OEC ou um membro da equipe de Privacidade Global. |
| [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. | Se você tomar conhecimento da divulgação indevida ou acidental de informações confidenciais de negócios, relate imediatamente o incidente a essas duas partes:   * seu supervisor direto, e * o time de OEC ou um membro da equipe de Privacidade Global.   O relato imediato da divulgação ajudará a Abbott a recuperar rapidamente as informações, evitar seu uso indevido ou incorreto e, se pertinente, ajudar a empresa a instaurar uma ação civil ou criminal. |
| [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. | Você nunca deve divulgar dados confidenciais da Abbott a ninguém que não seja autorizado a recebê-los.  Da mesma forma, você só deve usar dados confidenciais da Abbott em nome da Abbott e durante o desempenho de sua função de negócios na Abbott.  Se você divulgar indevidamente dados sigilosos, estará sujeito a ação disciplinar, incluindo encerramento do contrato de trabalho. |
| [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. | Você não tem permissão para, durante e depois de trabalhar na Abbott, compartilhar dados da empresa com nenhum de seus concorrentes. |
| [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. | A não devolução dos dados confidenciais à Abbott, a transmissão de dados confidenciais a um dispositivo, armazenamento, conta ou servidor não aprovado, ou o fornecimento de dados confidenciais da empresa a qualquer pessoa ou entidade não autorizada pode levar a Abbott a entrar com uma ação judicial contra você.  CLIQUE NO BOTÃO “AÇÃO JUDICIAL” PARA MAIS INFORMAÇÕES. |
| [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. | AÇÃO JUDICIAL  A ação judicial pode incluir um processo civil da Abbott contra você para:   * impedir que você trabalhe para um novo empregador até que os dados confidenciais da Abbott sejam devolvidos e protegidos; * exigir que você entregue todos os dispositivos eletrônicos à Abbott para revisão e inspeção; * fazer com que você pague pelos prejuízos financeiros decorrentes da retenção e/ou uso ilegal de dados confidenciais da Abbott e violação dos seus deveres e obrigações com a empresa à luz do seu contrato de trabalho com a Abbott; e * obrigar você a pagar os honorários e as despesas legais incorridas pela Abbott como resultado de uma ação judicial para proteger seus dados confidenciais.   Se necessário, a Abbott também trabalhará com as autoridades locais, estaduais e federais para proteger e reter os dados confidenciais da empresa. Nesse cenário, você também pode enfrentar penalidades criminais. |
| [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. | Qualquer evento que envolva um possível comprometimento da segurança das informações, incluindo a perda ou o roubo de um dispositivo móvel, deve ser comunicado imediatamente ao *Service Desk Global* local.  Caso você acredite que ocorreu uma violação em potencial ou deseje denunciar um possível incidente de privacidade, entre em contato com a equipe de Privacidade Global. |
| [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 | Clique na seta para começar sua revisão.  Revisão  Reserve um tempo para rever alguns dos principais conceitos abordados nesta seção.  Acesso e uso de dados sigilosos  Apenas acesse e use dados sigilosos para os fins específicos aos quais você recebeu acesso.  Compartilhamento de dados sigilosos  Antes de compartilhar dados sigilosos:   * Confirme a identidade do solicitante; * Confirme a necessidade de acessar as informações; * Verifique se as informações podem ser usadas para a(s) finalidade(s) solicitada(s); e * Compartilhe apenas o volume de informações requerido para atender à necessidade.   Retenção e descarte de dados sigilosos  Sempre arquive ou descarte dados sigilosos de acordo com os requisitos de gerenciamento, retenção e descarte de dados da Abbott.  Como responder a divulgações acidentais de PHI  Caso ocorra a divulgação acidental de dados protegidos de saúde (PHI) de um paciente, comunique imediatamente a divulgação para o time de OEC ou um membro da equipe de Privacidade Global.  Como denunciar um incidente de privacidade  Entre em contato com a equipe de Privacidade Global para relatar um incidente de privacidade potencial.  Para ver o seu progresso, clique no botão Menu  Excelente trabalho!  Você concluiu a seção 3 de 4  Clique na seta para frente para continuar a aprender |
| [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. | Onde obter ajuda  Escritório de Ética e Conformidade *(Office of Ethics and Compliance, OEC)*  Departamento de Privacidade Global– Entre em contato com o Departamento de Privacidade Global pelo e-mail [privacy@abbott.com](mailto:privacy@abbott.com). Você pode encontrar dados de contato adicionais e importantes informações sobre privacidade no Portal de Privacidade Global [aqui](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) na Abbott World.  Contatos de OEC – Você é incentivado a entrar em contato com o time de OEC sempre que tiver dúvidas sobre ética e *compliance*, ou para discutir as preocupações sobre possíveis violações de nossas normas, leis ou regulamentos escritos.   * Acesse a página [Contatar o OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) no [site do OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) na Abbott World ou [OEC@abbott.com](mailto:OEC@abbott.com).   SEGURANÇA CIBERNÉTICA EMPRESARIAL  Visite o site de Segurança Cibernética Corporativa [aqui](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) na Abbott World.  Visite o site [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) para aprender sobre formas seguras de compartilhar informações.  Departamento Jurídico  Em caso de dúvidas ou preocupações sobre as obrigações contratuais de terceiros com relação a privacidade e proteção de dados, entre em contato com o [Departamento Jurídico](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal).  Em caso de dúvidas ou preocupações sobre as exigências de retenção, ou se você desejar obter orientações sobre o uso aceitável de soluções tecnológicas, entre em contato com a equipe de Governança da Informação pelo e-mail [information.governance@abbott.com](mailto:information.governance@abbott.com).  POLÍTICAS DE REFERÊNCIA:   * Clique [aqui](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) para consultar a Política de Informações Confidenciais * Clique [aqui](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) para consultar a política da Abbott sobre Informações Privilegiadas * Clique [aqui](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) para consultar a Política de Uso Aceitável de Tecnologias. * Clique [aqui](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) para consultar a Política de Registros e Informações nos M-Files.   Políticas e procedimentos de OEC  Para acessar as políticas e procedimentos globais e específicos do time de OEC de cada país:   * Funcionários da Abbott devem visitar o [iComply](https://icomply.abbott.com/Default.aspx).   Centro de serviços de recursos humanos   * Clique [aqui](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) para obter uma lista dos números de contato do suporte de RH.   Recursos do curso  Transcrição  Clique [aqui](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) para acessar a transcrição completa do curso. |
| [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. | O Teste de Conhecimentos consiste em 10 perguntas. Você precisa acertar 80% ou mais para concluir este curso com sucesso.  Quando estiver pronto, clique no botão **Teste de Conhecimentos**. |
| 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? | Suponha que você trabalhou na Abbott por muitos anos e recentemente aceitou uma oferta de trabalho em outra empresa, qual dos seguintes dados seria legalmente permitido que você leve consigo ao sair? |
| 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] Informações pessoais de pacientes de estudos clínicos  [2] Lista de clientes e informações de apresentações que você criou enquanto trabalhava para a Abbott  [3] Projeções de vendas e dados financeiros da sua divisão ou unidade de negócios na Abbott  [4] Fotos e lembranças pessoais |
| 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. | A resposta correta é a 4. Informações pessoais, informações confidenciais de negócios e informações de saúde protegidas são consideradas dados sigilosos que você não pode levar consigo ou usar depois que sair da Abbott. Além disso, todos os dispositivos eletrônicos da Abbott e outras propriedades da Abbott devem ser devolvidos antes de sair da empresa.  Para obter mais informações, consulte a Seção 3.4, Respondendo a divulgações indevidas. |
| 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. | Um gerente de marketing está trabalhando no lançamento de um novo produto e precisa criar um formulário de consentimento para clientes potenciais. O formulário permitirá a coleta e uso de informações pessoais. Para alinhar às práticas de consentimento da Abbott, qual das seguintes afirmações sobre o formulário de consentimento precisam ser verdadeiras?  Marque todas as alternativas que se aplicam. |
| 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] O formulário não deve pressionar os clientes a dar consentimento.  [2] O formulário deve dar aos clientes todas as informações sobre como suas informações pessoais serão usadas.  [3] O formulário deve solicitar aos clientes que concordem expressamente com a coleta e uso de suas informações pessoais.  [4] O formulário não deve permitir que os clientes retirem o consentimento depois de dá-lo. |
| 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. | As práticas de consentimento da Abbott exigem que o formulário:   * Seja claro e conciso; * Não pressione as pessoas a dar consentimento; * Forneça todas as informações sobre como as informações pessoais serão usadas; * Exige que as pessoas concordem expressamente com a coleta e uso de suas informações pessoais; e * Permitir a retirada do consentimento, se desejar.   Para obter mais informações, consulte a Seção 1.3, Princípios de Privacidade por Design da Abbott. |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | A Abbott gerencia a divulgação e o uso de dados sigilosos, como informações pessoais, por meio de: |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] Anonimização de todos os dados.  [2] Controles de acesso.  [3] Ambas as alternativas 1 e 2. |
| Screen 46  Question 3: Feedback  65\_C\_48 | Disclosure and Use of personal information are managed through access controls and other processes that limit access and use to individuals in specific job functions and for the specific purposes set out in the notice for which consent was given.  For more information, see  Section 1.3, Abbott’s Privacy by Design Principles. | O gerenciamento de divulgação e uso de informações pessoais é feito por meio de controles de acesso e outros processos que, por sua vez, limitam o acesso e o uso dos dados a indivíduos que ocupam determinados cargos e aos fins específicos descritos no aviso para o qual o consentimento foi fornecido.  Para obter mais informações, consulte a Seção 1.3, Princípios de Privacidade por Design da 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. | Qual das seguintes afirmações é verdadeira em relação à retenção e descarte de informações pessoais?  Marque todas as alternativas que se aplicam. |
| 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] As informações pessoais são retidas apenas durante o período necessário para alcançar os objetivos que motivaram a coleta e o processamento dos dados.  [2] Assim que os dados deixam de ser necessários em um ambiente de produção ativa, eles sempre devem ser descartados.  [3] A retenção e o descarte de informações pessoais estão sujeitos a todas as retenções determinadas por questões legais. |
| 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. | De modo geral, a Abbott deve reter informações pessoais apenas durante o período necessário para alcançar os objetivos que motivaram a coleta e o processamento dos dados. Quando os dados não são mais necessários em um ambiente de produção ativa, eles devem ser arquivados ou descartados conforme os requisitos de gerenciamento, retenção e descarte de dados da Abbott. Os requisitos de retenção e descarte também estão sujeitos a quaisquer retenções relacionadas a questões jurídicas.  Para obter mais informações sobre a resposta correta, consulte a Seção 1.3, Princípios de Privacidade por Design da 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. | Um engenheiro está trabalhando no desenvolvimento de um novo produto. Qual das seguintes alternativas seria considerada informações confidenciais de negócios que precisam ser protegidas?  Marque todas as alternativas que se aplicam. |
| 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] Projeções de vendas e previsões de novos produtos.  [2] Dados financeiros do Informe Anual da Abbott.  [3] Informações de compras, como ofertas para contratos para novos produtos.  [4] Informações competitivas sobre produtos similares.  [5] Propostas de fornecedores terceirizados relacionadas ao novo produto. |
| 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. | Informações confidenciais de negócios são uma categoria ampla. Elas incluem grande parte das informações de negócios que usamos e com as quais temos contato diariamente. Uma boa forma de confirmar se algo é confidencial é se fazer uma pergunta simples:  Essas informações estão disponíveis publicamente?  Se a resposta for “não”, as informações certamente são confidenciais e será necessário adotar medidas apropriadas para protegê-las.  Para obter mais informações, consulte a Seção 2.1, Como reconhecer informações confidenciais de negócios. |
| 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: | O Regulamento Geral sobre a Proteção de Dados (GDPR) é uma das leis de privacidade mais abrangentes do mundo. Implementada em 2018, é o padrão para proteção da privacidade. Este regulamento foi criado no: |
| Screen 46  Question 6: Options  73\_C\_48 | [1] Canada  [2] Asia  [3] Europe  [4] Russia  [5] United States  [6] Latin America | [1] Canadá  [2] Ásia  [3] Europa  [4] Rússia  [5] Estados Unidos  [6] América Latina |
| 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. | A resposta correta é Europa. Na Europa, o Regulamento Geral sobre a Proteção dos Dados (GDPR) é uma das leis de privacidade mais abrangentes em âmbito global, e desde sua implementação em 2018, determinou o padrão de proteção de privacidade que outros países tentam seguir.  Para mais informações, consulte a Seção 1.2, Acordos Legais, Regulatórios e Contratuais. |
| 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: | Seu colega acabou de concluir um projeto que envolveu a coleta e uso de dados pessoais. Desde então, ele recebeu um pedido de outro departamento para acessar tais dados. Você orienta seu colega a: |
| 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] Confirmar a identidade do solicitante e a legítima necessidade dele ter acesso às informações.  [2] Verifique se o solicitante tem autorização para ter uma cópia das informações.  [3] Certifique-se de que os dados podem ser usados para as finalidades solicitadas.  [4] Todas as opções anteriores. |
| 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. | Uma das causas mais comuns de incidentes de dados dentro de uma organização é o compartilhamento indevido de dados com pessoas não autorizadas. Antes de compartilhar qualquer documento ou arquivo contendo dados sigilosos, sempre:   * Confirme a identidade do solicitante e a legítima necessidade dele ter acesso às informações. * Verifique se a pessoa está autorizada a ter uma cópia das informações. * Verifique se as informações podem ser usadas com as finalidades de utilização que estão sendo solicitadas. * Compartilhe apenas o volume de informações necessário para atender à necessidade em questão, nunca mais do que isso.   Para obter mais informações, consulte a Seção 3.2, Compartilhamento de dados sigilosos. |
| 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? | Você é um representante de vendas visitando uma clínica em sua área. Enquanto aguarda na área da recepção, você perde documentos sigilosos que contêm informações de saúde protegidas de um paciente. O que você faz? |
| 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] Notifica o diretor de privacidade da clínica.  [2] Entra em contato com seu supervisor.  [3] Denuncia o incidente ao time de OEC ou a um membro da equipe de Privacidade Global. |
| 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. | Caso ocorra a divulgação acidental de informações de saúde protegidas de um paciente, você deve comunicar o incidente imediatamente para:   * o time de OEC ou um membro da equipe de Privacidade Global.   Para obter mais informações, consulte a Seção 3.4, Respondendo a divulgações indevidas. |
| 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? | Ao se deslocar para o trabalho de trem, você acidentalmente esquece seu laptop com documentos sigilosos de trabalho no seu assento e sai do trem. Você percebe o erro ao chegar ao escritório e procura desesperadamente pelo laptop, mas não o encontra em nenhum lugar. O que você deve fazer primeiro? |
| 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] Ligar para a empresa de trem e perguntar se alguém encontrou o laptop.  [2] Voltar à estação de trem e procurar por seu laptop.  [3] Entrar em contato com seu *Service Desk Global* local. |
| Screen 46  Question 9: Feedback  83\_C\_48 | If you believe that sensitive information may have been compromised, such as through a lost or stolen laptop, please contact your local Global Service Desk immediately.  For more information, see Section 3.4, Reporting a Data Incident. | Se você acha que as informações sigilosas possam ter sido comprometidas, seja através de um laptop perdido ou roubado, entre em contato com o seu *Service Desk Global* imediatamente.  Para obter mais informações, consulte a Seção 3.4, Relatando um incidente de dados. |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | Você só deve usar informações pessoais:  Marque todas as alternativas que se aplicam. |
| 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] Para a finalidade específica para a qual você recebeu acesso.  [2] De acordo com o aviso fornecido ao titular dos dados.  [3] De acordo com o consentimento concedido pelo titular dos dados. |
| 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. | Caso tenha permissão para acessar informações pessoais, use apenas:   * Para a finalidade específica para a qual você recebeu acesso. * De acordo com o aviso fornecido ao titular dos dados. * De acordo com o consentimento concedido pelo titular dos dados.   Para obter mais informações, consulte a Seção 3.1, Acesso e uso de dados sigilosos. |
| [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 | Todas as perguntas continuam sem resposta |
| [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. | Nenhum resultado estará disponível até que você conclua o Teste de Conhecimentos.  Parabéns! Você passou com sucesso no Teste de Conhecimentos e concluiu o curso.  Analise os resultados abaixo, clicando em cada pergunta.  Assim que estiver pronto, você deve clicar no ícone **SAIR [X]** na barra principal do curso para fechar a janela do navegador ou a guia do navegador.  Sinto muito, você não passou no Teste de Conhecimentos. Dedique alguns minutos para analisar seus resultados abaixo, clicando em cada pergunta.  Quando estiver pronto, clique no botão **Refazer o Teste de Conhecimentos**. |
| 89\_toc\_1 | Introduction | Introdução |
| 90\_toc\_2 | Welcome | Bem-vindo |
| 91\_toc\_3 | Objectives | Objetivos |
| 92\_toc\_4 | Menu | Menu |
| 93\_toc\_5 | Personal Information | Informações pessoais |
| 94\_toc\_6 | Recognizing Personal Information | Como reconhecer informações pessoais |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Exigências legais, regulatórias e contratuais |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Princípios de Privacidade por Design da Abbott |
| 97\_toc\_9 | Review | Revisão |
| 98\_toc\_10 | Confidential Business Information | Informações Confidenciais de Negócios |
| 99\_toc\_11 | Recognizing Confidential Business Information | Como reconhecer informações confidenciais de negócios |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Custo de não proteger as informações confidenciais de negócios |
| 101\_toc\_13 | Insider Information | Informações privilegiadas |
| 102\_toc\_14 | Review | Revisão |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Seu papel na proteção de dados sigilosos |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Acesso e uso de dados sigilosos |
| 105\_toc\_17 | Sharing Sensitive Data | Compartilhamento de dados sigilosos |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Retenção e descarte de dados sigilosos |
| 107\_toc\_19 | Responding to Improper Disclosures | Respondendo a divulgações indevidas |
| 108\_toc\_20 | Review | Revisão |
| 109\_toc\_21 | Knowledge Check | Teste de Conhecimentos |
| 110\_toc\_22 | Introduction | Introdução |
| 111\_toc\_23 | Assessment | Avaliação |
| 112\_toc\_24 | Question 1 | Pergunta 1 |
| 113\_toc\_25 | Question 2 | Pergunta 2 |
| 114\_toc\_26 | Question 3 | Pergunta 3 |
| 115\_toc\_27 | Question 4 | Pergunta 4 |
| 116\_toc\_28 | Question 5 | Pergunta 5 |
| 117\_toc\_29 | Question 6 | Pergunta 6 |
| 118\_toc\_30 | Question 7 | Pergunta 7 |
| 119\_toc\_31 | Question 8 | Pergunta 8 |
| 120\_toc\_32 | Question 9 | Pergunta 9 |
| 121\_toc\_33 | Question 10 | Pergunta 10 |
| 122\_toc\_34 | Feedback | Feedback |
| 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 | O curso não consegue entrar em contato com o LMS. Clique em “OK” para continuar e revisar o curso. Observação: a Certificação do Curso poderá não estar disponível. Clique em “Cancelar” para sair |
| 124\_string\_2 | All questions remain unanswered | Todas as perguntas continuam sem resposta |
| 125\_string\_3 | Questions | Perguntas |
| 126\_string\_4 | Question | Pergunta |
| 127\_string\_5 | not answered | não respondida |
| 128\_string\_6 | That's correct! | Correto! |
| 129\_string\_7 | That's not correct! | Incorreto! |
| 130\_string\_8 | Feedback: | Feedback: |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | PROTEÇÃO DE DADOS SIGILOSOS |
| 132\_string\_10 | Knowledge Check | Teste de Conhecimentos |
| 133\_string\_11 | Submit | Enviar |
| 134\_string\_12 | Retake Knowledge Check | Refaça o Teste de Conhecimentos |
| 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. | Descrição do curso: Na Abbott, frequentemente usamos dados sigilosos para tomar importantes decisões de negócios. Como muitas das nossas partes interessadas se preocupam com a forma como esses dados são coletados e usados, a Abbott adota políticas e procedimentos que visam garantir a proteção desses dados. Este curso explica o que são dados sigilosos, porquê eles são vitais para a nossa empresa e quais medidas podemos adotar para assegurar que processamos e tratamos essas informações de maneira segura. Este curso leva aproximadamente 30 minutos para ser concluído. |
| 136\_string\_14 | Menu | Menu |
| 137\_string\_15 | Resources | Recursos |
| 138\_string\_16 | Reference Material | Material de referência |
| 139\_string\_17 | Audio | Áudio |
| 140\_string\_18 | Exit | Sair |
| 141\_string\_19 | Record My Results | Registrar meus resultados |