|  |  |  |
| --- | --- | --- |
| 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. | Beskytte sensitive opplysninger  Klikk på fremoverpilen for å starte. |
| [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. | Hos Abbott støtter vi oss på opplysninger for å ta avgjørelser – ofte inneholder disse opplysningene sensitiv informasjon.  For at vi skal kunne oppfylle oppdraget vårt om å hjelpe folk med å leve sine beste liv gjennom god helse er det vesentlig at vi holder disse opplysningene sikre og overholder lovene og de etiske standardene som Abbott opprettholder. Dette kurset er designet for å gi deg de nødvendige ferdighetene for å støtte denne oppgaven. |
| [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. | Etter å ha fullført kurset vil du ha en bedre forståelse av:   * Hva sensitive opplysninger er, * Hvordan vi beskytter disse opplysningene hos Abbott, * Din rolle i å beskytte sensitive opplysninger, og * Hva du skal gjøre hvis du tror at sensitive opplysninger kan ha blitt offentliggjort på en upassende måte eller kompromittert. |
| [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 | Personlige opplysninger  Her vil du lære hvordan myndigheter, forbrukere og allmennheten har blitt stadig mer bekymret for personvern og sikkerheten til personlige opplysninger.  12 minutter  Del 1 | Personlige opplysninger  Gjenkjenne personlige opplysninger  Juridiske, forskriftsmessige og kontraktsmessige krav  Abbotts prinsipper for innebygd personvern  Gjennomgang  2 | Konfidensielle forretningsopplysninger  Her vil du lære hvordan de fleste av forretningsopplysningene vi bruker i det daglige arbeidet vårt anses som konfidensielle.  5 minutter  Del 2 | Konfidensielle forretningsopplysninger  Gjenkjenne konfidensielle forretningsopplysninger  Kostnaden ved å ikke beskytte konfidensielle forretningsopplysninger  Innsideinformasjon  Gjennomgang  3 | Beskytte sensitive opplysninger  Her vil du lære hva du kan gjøre for å hjelpe med å beskytte sensitive opplysninger.  8 minutter  Del 3 | Din rolle i å beskytte sensitive opplysninger  Få tilgang til og bruk av sensitive opplysninger  Deling av sensitive opplysninger  Oppbevaring og sletting av sensitive opplysninger  Tilbakemelding på upassende offentliggjøringer  Gjennomgang  4 | Kunnskapssjekk  Vurder din forståelse av nøkkelkonsepter og -prinsipper i dette kurset.  5 minutter  Del 4 | Kunnskapssjekk  Vurdering  Klikk på panelet for å komme i gang.  Klikk på den gule spill av-knappen for å starte.  Dette innholdet er ikke tilgjengelig ennå. Du må fullføre del {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. | En vanlig type sensitive opplysninger vi bruker hos Abbott er personlige opplysninger.  De siste årene har myndigheter, forbrukere og allmennheten blitt stadig mer bekymret for personvern og sikkerheten til personlige opplysninger. |
| [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. | Personlige opplysninger er enhver opplysning som kan brukes til å kontakte, lokalisere eller identifisere et individ. |
| [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 | Markedsføringsleder  Kan du gi meg noen eksempler på personlige opplysninger?  Personlige opplysninger kan omfatte biografisk informasjon som navn, fødselsdato, e-postadresse og telefonnummer.  Det kan omfatte informasjon om en persons utseende, for eksempel hårfarge eller vekt.  Det kan også omfatte informasjon knyttet til individets privatliv, for eksempel bilder, informasjonskapsler i nettleseren eller informasjon om posisjonssporing. |
| [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 | Salgsrepresentant  Inkluderer personlige opplysninger også beskyttet helseinformasjon?  Ja, det gjør de.  Beskyttet helseinformasjon (PHI) er en spesielt sensitiv type personlige opplysninger som brukes i helseindustrien. Det inkluderer personlig identifiserbar informasjon i medisinske journaler, inkludert samtaler mellom medisinsk fagpersonell om behandling. |
| [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. | I de fleste land der Abbott driver virksomhet, finnes det lover og forskrifter for å beskytte personlige opplysninger, inkludert beskyttet helseinformasjon.  Lover knyttet til personvern og beskyttelse av personlige opplysninger varierer fra land til land, men inneholder ofte de samme kjernevilkårene.  KLIKK PÅ HVERT AV DE UTHEVEDE OMRÅDENE PÅ SKJERMEN FOR Å LÆRE OM ULIKE TYPER PERSONVERNREGLER OG KRAV SOM FINNES RUNDT OM I VERDEN. |
| [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  I Europa er personvernforordningen (GDPR) én av de mest omfattende personvernlovgivningene globalt, og siden implementeringen i 2018 har den satt standarden for personvernbeskyttelse som andre land forsøker å etterligne. GDPR gjelder for organisasjoner i Europa, samt organisasjoner utenfor Europa som tilbyr varer og tjenester til, eller som overvåker atferden til, europeiske borgere.  Ett av nøkkelkonseptene i GDPR er retten til sletting, også kjent som retten til å bli glemt. Denne retten gir enkeltpersoner evnen til å be om at deres personopplysninger blir slettet fra en organisasjons registre. Hvis en enkeltperson foretar en slik forespørsel, må organisasjonen iverksette tiltak for å slette opplysningene fra systemene sine og forhindre at de blir brukt eller offentliggjort videre. Det kan være unntak for forespørsler fra registrerte. Uansett, Abbott vil for hver enkelt forespørsel informere om hvilke tiltak som blir gjort. Brudd på GDPR kan føre til store bøter for selskaper, opptil 4 % av deres årlige globale omsetning eller 20 millioner euro (avhengig av hva som er størst), for de mest alvorlige overtredelsene. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11)  [11\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11) | United States  In the United States, there is no single law that protects all personal information. Instead, there are privacy laws and regulations that apply to specific industries and types of data. For example, HIPAA protects the privacy of healthcare data, while the Fair Credit Reporting Act protects credit information.  However, some states have begun enacting their own comprehensive data privacy laws. For instance, California has the California Consumer Privacy Act (CCPA), which gives Californians certain rights to their data, such as the right to know what personal information is being collected about them and the right to delete any personal information collected. The CCPA will be amended by the California Privacy Rights Act (CPRA) in 2023, which will give people even more rights to their data.  Other states that have passed their own data privacy laws include Virginia, Colorado, Utah, and Connecticut. While each state's law is different, they all generally give people rights to their data and require companies to provide certain disclosures about their data processing activities.  Fines for violating state privacy laws can be significant. For example, California can fine companies up to $7,500 USD per violation of the CCPA.  Canada  There are laws at both the federal and provincial levels in Canada that are designed to protect an individual's personal information. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that applies to private sector organizations and is enforced by the Office of the Privacy Commissioner of Canada.  At the provincial level, Quebec, Alberta, and British Columbia have enacted privacy laws that are similar to PIPEDA. Some other provinces also have rules in place that provide similar protections for personal information, including the provinces of Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia, which have enacted health information privacy laws.  These laws are in place to help prevent personal information from being mishandled or collected without the individual's knowledge, and give people the right to access their own information and correct any errors.  Violating these laws can result in significant fines. For example, violating PIPEDA can lead to a fine of up to $100,000. In Alberta, the Personal Information Protection Act (PIPA) allows for fines of up to $10,000 for individuals and $500,000 for organizations. | USA  I USA finnes det ingen enkeltstående lov som beskytter alle personlige opplysninger. Det er i stedet personvernlovgivning og forskrifter som gjelder for spesifikke industrier og typer av opplysninger. HIPAA (Health Insurance Portability and Accountability Act) beskytter for eksempel personvernet i helseomsorgsopplysninger, mens Fair Credit Reporting Act beskytter kredittinformasjon.  Enkelte stater har imidlertid begynt å innføre sine egne omfattende personvernlovgivninger. California har for eksempel California Consumer Privacy Act (CCPA), som gir californiere visse rettigheter til opplysningene sine, så som retten til å vite hvilke personlige opplysninger som blir innhentet om dem og retten til å slette de innhentede personlige opplysningene. CCPA vil bli endret av California Privacy Rights Act (CPRA) i 2023, noe som vil gi personer enda flere rettigheter til opplysningene sine.  Andre stater som har vedtatt sine egne personvernlovgivninger inkluderer Virginia, Colorado, Utah og Connecticut. Selv om hver stat er forskjellig, gir de alle generelt personer rettigheter til opplysningene sine og krever at selskaper oppgir visse offentliggjøringer om deres behandlingsaktiviteter for opplysninger.  Bøter for å bryte statlige personvernlover kan være vesentlige. California kan for eksempel gi selskaper bøter på opptil USD 7500 per brudd på CCPA.  Canada  Det finnes lover på både føderale og provinsielle nivåer i Canada som er designet for å beskytte en enkeltpersons personlige opplysninger. Personal Information Protection and Electronic Documents Act (PIPEDA) er for eksempel en føderal lov som gjelder for organisasjoner innen privat sektor og håndheves av Office of the Privacy Commissioner i Canada.  På provinsnivå har Quebec, Alberta og British Columbia vedtatt personvernlovgivninger lignende PIPEDA. Enkelte andre provinser har også regler på plass som gir lignende beskyttelser for personlige opplysninger, inkludert provinsene Ontario, New Brunswick, Newfoundland og Labrador og Nova Scotia, som har vedtatt personvernlovgivning om helseopplysninger.  Disse lovene er på plass for å bidra til å forhindre at personlige opplysninger blir misbrukt eller innhentet uten enkeltpersonens kunnskap og gir personer retten til å få tilgang til sine egne opplysninger og korrigere feil.  Brudd på disse lovene kan resultere i vesentlige bøter. Brudd på PIPEDA kan for eksempel føre til en bot på opptil USD 100 000. I Alberta tillater Personal Information Protection Act (PIPA) bøter på opptil USD 10 000 for enkeltpersoner og USD 500 000 for organisasjoner. |
| [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. | Den asiatiske stillehavsregionen  Personvernlovgivningen i den asiatiske stillehavsregionen utvides kontinuerlig og blir mer omfattende. Enkelte land, så som Kina, har implementert lokaliseringstiltak for opplysninger som krever at selskaper lagrer enkelte personopplysninger på servere innenfor deres grenser. I tillegg har Kina personvern- og sikkerhetseffektvurderingskrav for grensekryssende overføring av personlige opplysninger.  Andre, som Australia og Singapore, har vedtatt en mer forbrukerfokusert tilnærming mot personvern som gir enkeltpersoner større kontroll over sine opplysninger, inkludert retten til å vite hvordan selskaper bruker dem og evnen til å få tilgang til og korrigere dem ved behov.  Straffene for selskaper som bryter personvernlover varierer også svært mye på tvers av regionen. I Kina kan selskaper for eksempel bli bøtelagt opptil 500 000 RMB (omtrent USD 72 000) for brudd på personvernlover.  I Singapore kan selskaper derimot bli bøtelagt opptil 1 million (Singapore) dollar (omtrent USD 737 000) for brudd på landets personvernlovgivning. |
| [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. | Russland  Russland har også lover for å beskytte sine statsborgeres opplysninger, inkludert lovgivning for lokalisering av opplysninger, som krever at selskaper lagrer russiske statsborgeres personopplysninger på servere plassert i Russland.  Loven gjelder for selskaper som behandler opplysningene til russiske statsborgere, uavhengig av om disse selskapene er basert i Russland eller ikke. Så, et amerikansk selskap som behandler opplysningene til russiske statsborgere vil for eksempel måtte overholde loven.  Som i mange land krever loven også at selskaper iverksetter tiltak for å beskytte personopplysningene de behandler. Selskaper må for eksempel sikre at opplysningene er nøyaktige og oppdaterte, og iverksette tiltak for å forhindre at de blir misbrukt, tapt eller stjålet.  Bøtene for å bryte loven kan være fra USD 12 000 til USD 72 000 for den første overtredelsen og opptil USD 216 000 for den andre overtredelsen. |
| [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. | Latin-Amerika  De fleste latin-amerikanske land har lovgivning på plass som beskytter enkeltpersoners personvern. Flere land i regionen, så som Ecuador, Argentina og Brasil har imidlertid nylig revidert sine eksisterende personvernforskrifter for å holde seg oppdatert med internasjonale standarder.  Ecuador vedtok for eksempel nylig Organic Law on the Protection of Personal Data (LPPD) som vil tre i kraft i 2023. Denne loven gjelder for ethvert selskap rundt i verden som behandler personopplysningene til enkeltpersoner i Ecuador.  Som andre i regionen krever LPPD at selskaper varsler og innhenter samtykke fra enkeltpersoner før de bruker opplysningene deres, sletter dem når de ikke lenger er nødvendige og oppfyller visse restriksjoner før opplysninger deles med andre land. Disse tiltakene bidrar til å beskytte personvernet til enkeltpersoner på tvers av Latin-Amerika og sikre at selskaper håndterer personopplysninger ansvarlig.  Brudd på LPPD kan resultere i vesentlige bøter, fra 3 % til 17 % av en organisasjons årlige omsetning fra året før, noe som gir selskaper et sterkt insentiv for å overholde loven. |
| [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. | I tillegg til lover og forskrifter som regulerer hvordan Abbott driver virksomhet, kan det være ytterligere forpliktelser i spesifikke kontrakter vi har med kunder.  For eksempel er den amerikanske regjeringen en kunde hos Abbott. I henhold til vilkårene i en slik avtale, er vi pålagt å oppfylle forpliktelsene angitt i USAs Privacy Act of 1974.  KLIKK PÅ «PRIVACY ACT»-KNAPPEN FOR Å FINNE UT MER. |
| [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. | Privacy Act  Privacy Act of 1974 (5 U.S.C. 552a) er en viktig føderal forskrift. Den gir en kodeks for rettferdig informasjonspraksis som styrer innhenting, vedlikehold, bruk og formidling av personlig identifiserbar informasjon om enkeltpersoner som oppbevares i registersystemer av føderale etater. Abbott kan for enkelte transaksjoner få tilgang til offentlige etaters registre. I slike tilfeller må Abbott oppfylle flere forpliktelser, inkludert å bevise at personvernopplæring om å beskytte personlig identifiserbar informasjon har blitt gjennomført.  Ansatte bør kontakte juridisk avdeling før de inngår avtaler med kunder som har personvernforpliktelser. |
| [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. | Lovene, forskriftene og kontraktkravene vi nettopp har gjennomgått, er ofte kompliserte og kan endres raskt.  Abbott har retningslinjer og prosedyrer på plass for å sikre at ansatte overholder disse lovene og forskriftene. Hvis du har spørsmål eller ønsker å lære mer, kan du kontakte OEC eller et medlem av det globale personvernsteamet.  For kontakter og ytterligere informasjon, klikk på Ressurser-ikonet. |
| [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 | Innhenting   * Varsel * Samtykke   FORVALTNING   * Dataintegritet * Tilgang og korrigering   Bruk   * Offentliggjøring og bruk   Disponering   * Oppbevaring og avhending sletting   Abbotts retningslinjer og prosedyrer for personvern og beskyttelse er organisert etter et enkelt sett med prinsipper. Vi kaller dette innebygd personvern.  Disse prinsippene er utformet for å hjelpe ansatte med å beskytte sensitive opplysninger i hver fase av opplysningenes livssyklus. For å illustrere, la oss se spesifikt på personlige opplysninger.  Den første fasen av opplysningenes livssyklus er innhenting.  I løpet av denne fasen bruker Abbott en rekke metoder for å innhente personlige opplysninger. For eksempel kan vi be forbrukerne om å oppgi kontaktinformasjon på et Abbott-nettsted, eller vi kan fange opp personlige opplysninger som er generert fra én av enhetene våre.  For å beskytte personvernrettighetene til enkeltpersonene i denne fasen, opprettholder vi prosesser for å sikre at vi overholder prinsippene for innebygd personvern for merknad og samtykke.  Varsling handler om å informere enkeltpersoner om hvilke personlige opplysninger som innhentes, og å forklare med et klart og tydelig språk hvordan vi har tenkt å bruke opplysningene.  Når du for eksempel sender inn en forespørsel på abbott.com, brukes de personlige opplysningene vi innhenter kun til å svare på henvendelsen.  Samtykke handler om å gi enkeltpersoner muligheten til å godta innhenting og bruk av deres personlige opplysninger.  Når vi søker samtykke, forsikrer vi oss generelt om at det er:   * Frivillig gitt. Enkeltpersonen blir aldri tvunget eller fortalt at samtykke er et krav. * Informert. Enkeltpersonen får tilstrekkelig informasjon til å ta en rimelig beslutning som de samtykker til. * Bekreftende. Enkeltpersonen må gi bekreftende samtykke. Vi tildeler aldri samtykke, for eksempel gjennom en enkeltpersons taushet, og vi krever heller ikke at enkeltpersonen gjør noe, for eksempel å fjerne avmerkingen for en boks, for å velge bort noe. * Tilbakekalling. Enkeltpersonen får en klar forklaring på hvordan man kan tilbakekalle samtykke.   En forbruker som registrerer seg i fordelsprogrammet Abbott Nutrition Similac© Strong Moms©, kan for eksempel samtykke til innhenting og bruk av deres personlige opplysninger ved å velge (for eksempel å merke av i en rute) å motta ytterligere salgsinformasjon.  Den andre fasen av opplysningenes livssyklus er forvalting.  I løpet av denne fasen blir informasjon behandlet og lagret.  For å beskytte personlige opplysninger i denne fasen, opprettholder vi prosesser som sikrer at vi overholder prinsippene for:   * dataintegritet, og * tilgang og korrigering.   Dataintegritet handler om å gjøre rimelige tiltak for å sikre at de personlige opplysningene vi beholder er nøyaktige, komplette og aktuelle.  Én måte vi gjør dette på, er ved å spore og registrere alle aktiviteter som behandler personlige opplysninger. Dette sikrer at vi kan identifisere kilden til opplysningene, de spesifikke formålene opplysningene er behandlet for og hvor de lagres.  Tilgang og korrigering handler om å gi enkeltpersoner rimelig tilgang til sine opplysninger og muligheten til å utøve sine rettigheter i forbindelse med disse opplysningene.  Dette inkluderer å svare på en persons forespørsel om å få tilgang til, slette, overføre eller endre lagrede registre med personlige opplysninger.  Den tredje fasen av livssyklusen er bruk.  I løpet av denne fasen brukes personlige opplysninger til å støtte aktiviteter i hele organisasjonen.  For å beskytte personlige opplysninger i denne fasen, opprettholder vi prosesser som sikrer at vi overholder prinsippet om offentliggjøring og bruk.  Offentliggjøring og bruk handler om å kontrollere hvem som har tilgang til personlige opplysninger og å begrense bruken til spesifikke formål.  Vi klarer dette gjennom tilgangskontroller og andre prosesser. Disse kontrollene og prosessene begrenser tilgangen til enkeltpersoner med spesifikke jobbfunksjoner, og begrenser også bruken til de spesifikke formålene som er beskrevet i kunngjøringen som samtykket ble gitt for.  Den siste fasen av livssyklusen er disponering.  Disponering refererer til hva som skjer med opplysninger når de ikke lenger brukes aktivt. Handlinger kan omfatte sletting, arkivering eller oppbevaring for juridiske formål.  For å beskytte personlige opplysninger i denne fasen, opprettholder vi retningslinjer og prosesser som sikrer at vi overholder prinsippet om oppbevaring og avhending.  Oppbevaring og avhending av personlige opplysninger handler om å oppbevare personlige opplysninger bare for den tiden som er nødvendig for å oppnå de formålene de var nødvendige og ble behandlet for.  Når personlige opplysninger ikke lenger er påkrevd i et aktivt produksjonsmiljø, har Abbott på plass prosesser for å enten arkivere eller slette dem på en måte som er i samsvar med Abbotts krav til forvaltning, oppbevaring og sletting av opplysninger. Våre krav til oppbevaring og sletting er også underlagt eventuell oppbevaring knyttet til juridiske forhold.  For ytterligere informasjon relatert til krav til oppbevaring eller sletting, se Abbotts globale retningslinjer for registre og informasjon (l1-02) eller kontakt Legal Information Governance and Records. Detaljer finner du i ressurser-delen av denne opplæringen.  For kontakter og ytterligere informasjon, klikk på Ressurser-ikonet.  Som vi nettopp har sett, er våre retningslinjer og prosedyrer utformet for å beskytte personlige opplysninger gjennom hele livssyklusen.  Vi gjør dette ved å følge prinsippene om:   * varsel, * samtykke, * dataintegritet, * tilgang og korrigering, * offentliggjøring og bruk, og * oppbevaring og sletting.   INNHENTING  Varsel  Samtykke  FORVALTNING  Dataintegritet  Tilgang og korrigering  BRUK  Offentliggjøring og bruk  DISPONERING  Oppbevaring og sletting |
| [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 | Klikk på pilen for å starte gjennomgangen din.  Gjennomgang  Ta deg tid til å gjennomgå noen av nøkkelkonseptene dekket i denne delen.  Personlige opplysninger (PO)  PO er all informasjon som kan brukes til å   * kontakte * lokalisere eller * identifisere en enkeltperson.   Beskyttet helseinformasjon (PHI – Personal Health Information)  Beskyttet helseinformasjon er en spesielt sensitiv type personlige opplysninger som brukes i helseindustrien.  Personvernlover  Personvernlover er forskjellige fra land til land, men omfavner ofte de samme kjerneprinsippene.  Abbotts prinsipper for innebygd personvern  Abbotts retningslinjer og prosedyrer for personvern og beskyttelse er organisert etter et enkelt sett med prinsipper, kalt innebygd personvern.  Varsling og samtykke  Varsling og samtykke handler om å la personer få vite hvilke PO som innhentes og gi dem muligheten til å samtykke til denne innhentingen.  Dataintegritet  Dataintegritet handler om å gjøre rimelige tiltak for å sikre at PO er nøyaktige, komplette og aktuelle.  Tilgang og korrigering  Tilgang og korrigering handler om å gi enkeltpersoner retten til å få tilgang til å korrigere opplysningene sine.  Offentliggjøring og bruk  Offentliggjøring og bruk handler om å kontrollere hvem som har tilgang til PO.  Oppbevaring og sletting  Oppbevaring og sletting av PO handler om å oppbevare personlige opplysninger bare for den tiden som er nødvendig for å oppnå de formålene de var nødvendige og ble behandlet for.  For å sjekke fremgangen din, klikk på Meny-knappen  Flott gjort!  Du har fullført del 1 av 4  Klikk framover-pilen for å fortsette å lære |
| [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. | En annen type sensitive opplysninger som vi ofte bruker, er konfidensielle forretningsopplysninger.  Konfidensielle forretningsopplysninger er en bred kategori. Det inkluderer mye av forretningsopplysningene vi daglig bruker og kommer i kontakt med. Konfidensielle opplysninger er informasjon som ikke er offentlig tilgjengelig og som kan være til nytte for Abbotts konkurrenter eller skadelig for Abbott hvis den offentliggjøres. |
| [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 | Markedsføringsleder  Kan du gi meg noen eksempler på konfidensielle forretningsopplysninger?  Konfidensielle forretningsopplysninger kan inkludere, men er ikke begrenset til: produktdesign og -prosesser, komposisjoner, organismer, programvare for datamaskiner, forskning og utviklingsdata, kliniske og farmakologiske opplysninger, pasientopplysninger, tekniske data, kundelister og lister over potensielle kunder, forretningspraksiser, markedsføringsplaner og -strategier, økonomiske og driftsmessige opplysninger og opplysninger om personale.  Det kan også inkludere innkjøpsinformasjon, for eksempel anbud på kontrakter, leverandørlister og kostnadsinformasjon. |
| [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 | Salgsrepresentant  Er det visse typer konfidensielle forretningsopplysninger som er mer sensitive enn andre?  Ja. Visse typer konfidensielle forretningsopplysninger krever større aktsomhet enn normalt, fordi upassende offentliggjøring eller bruk av denne informasjonen kan forårsake alvorlig skade for selskapet.  Eksempler inkluderer:   * forretningshemmeligheter, så som produksjonsformler og -prosesser, * kliniske og regulatoriske opplysninger, regulatoriske innsendelser eller forhåndsgodkjenningsinformasjon, og * finansielle opplysninger som ikke er offentlig tilgjengelige. |
| [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. | Som du ser, anses det meste av forretningsopplysningene vi bruker i våre daglige arbeidsaktiviteter som konfidensielle.  En god måte å bekrefte om forretningsopplysningene du bruker er konfidensielle, er å stille deg selv et enkelt spørsmål:  Er denne informasjonen offentlig tilgjengelig?  Hvis svaret er nei, bør opplysningene betraktes som konfidensielle, og passende tiltak må iverksettes for å beskytte den. |
| [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. | Det er også viktig å huske på at eventuelle konfidensielle forretningsopplysninger du opprettet som del av jobbfunksjonen din hos Abbott tilhører Abbott.  Som et resultat må du beskytte denne informasjonen og du kan ikke beholde den hvis du slutter i jobben din hos 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. | Det er viktig å beskytte konfidensielle forretningsopplysninger.  Ikke overraskende kan upassende bruk eller offentliggjøring av denne informasjonen føre til betydelige skade for 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. | Upassende bruk eller offentliggjøring av konfidensiell informasjon kan skade Abbotts relasjoner med kunder og klienter, føre til pinlig presse- og mediedekning og føre til tap av konkurransemessige fordeler for Abbott. Det kan også resultere i sivile søksmål og kriminelle straffer, inkludert mot nåværende og tidligere ansatte.  KLIKK PÅ «NYLIGE SAKER»-KNAPPEN FOR MER INFORMASJON. |
| [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. | NYLIGE SAKER  De siste årene har selskaper blitt tilkjent store jurydommer og erstatninger mot tidligere ansatte som har tatt selskapsinformasjon på urettmessig måte. Ett selskap ble for eksempel tilkjent en erstatning på USD 240 millioner for en tidligere ansatt som urettmessig fremla selskapets konfidensielle informasjon til en konkurrent. Et annet selskap ble tildelt en erstatning på USD 854 millioner dollar fra en lagrett mot en tidligere ansatt og vedkommendes nye arbeidsgiver, da den tidligere ansatte misbrukte selskapets konfidensielle informasjon og deretter brukte selskapets konfidensielle informasjon på vegne av sin nye arbeidsgiver.  Studier indikerer at tyveri av konfidensiell informasjon forårsaker tap på mellom USD 209 og USD 625 milliarder for børsnoterte selskaper. |
| [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. | Det burde ikke være overraskende at myndigheter tar tyveri av konfidensiell informasjon svært alvorlig.  Under føderale straffebestemmelser kan en enkeltperson for eksempel få opptil ti års fengsel og en bot på USD 5 millioner for å stjele konfidensiell informasjon. I tillegg kan et selskap som blir funnet skyldig i å stjele konfidensiell informasjon ilegges en bot på USD 10 millioner eller tre ganger verdien av den konfidensielle informasjonen.  KLIKK PÅ «BØTER OG SANKSJONER»-KNAPPEN FOR MER INFORMASJON. |
| [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. | BØTER OG SANKSJONER  De siste årene har flere personer og selskaper blitt bøtelagt eller fått fengselsstraffer for tyveri av konfidensiell informasjon. For eksempel:   * En konkurrent fikk en bot på USD 60 millioner for å ha stjålet et annet selskaps konfidensiell informasjon, * En tidligere IT-ansatt ble dømt til 97 måneder i fengsel for å ha stjålet konfidensiell informasjon, * En tidligere selger ble dømt til 12 måneder i fengsel for å ha stjålet konfidensiell informasjon, * En toppleder ble dømt til 24 måneder i fengsel for å ha stjålet konfidensiell informasjon, og * En forsker ble dømt til fengsel i 18 måneder for å ha stjålet konfidensiell informasjon. |
| [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. | En annen type konfidensielle forretningsopplysninger som er viktige å gjenkjenne og beskytte, refereres ofte til som *innsideinformasjon.*  Innsideinformasjon er vesentlig ikke-offentlig informasjon som med rimelighet kan forventes å påvirke markedsverdien av verdipapirene til selskapet eller påvirke investorers beslutninger om å kjøpe eller selge verdipapirer om den blir offentliggjort. |
| [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. | Eksempler på innsideinformasjon inkluderer:   * nyheter om et potensielt oppkjøp, * en forsinkelse i en produktlansering, * nyheter om brudd på interne IT-systemer, * uventede endringer i inntjening eller utbyttesatser, * foreslåtte anbud eller aksjesplitt, * informasjon om viktige nye produkter, * kontraktstildelinger, * utvidelsesplaner, * vesentlige tvistemål eller regulatoriske forhandlinger osv. |
| [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. | Hvis du er kjent med eller har innsideinformasjon, er det ulovlig å handle med, eller anbefale andre å handle med, Abbott-verdipapirer.  Dette gjelder også kjøp og salg av verdipapirer fra andre selskaper, inkludert de som for tiden gjør eller som forventes å gjøre forretninger med Abbott.  For å lære mer om Abbots forventninger med hensyn til bruk og beskyttelse av ikke-offentliggjort informasjon, kan du gjennomgå Abbotts retningslinjer om innsidehandel. Detaljer finner du i ressurser-delen av denne opplæringen. |
| [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 | Klikk på pilen for å starte gjennomgangen din.  Gjennomgang  Ta deg tid til å gjennomgå noen av nøkkelkonseptene dekket i denne delen.  Konfidensielle forretningsopplysninger  Alle forretningsopplysninger som ikke er offentlig tilgjengelige skal regnes som konfidensielle. Dette inkluderer mye av forretningsopplysningene vi bruker i våre daglige arbeidsaktiviteter.  Upassende bruk av konfidensielle forretningsopplysninger  Den upassende bruken eller offentliggjøringen av konfidensielle forretningsopplysninger kan resultere i vesentlig skade på selskapet, kundene våre og våre ansatte.  Innsideinformasjon  Innsideinformasjon er vesentlig ikke-offentlig informasjon som med rimelighet kan forventes å påvirke markedsverdien av verdipapirene til selskapet eller påvirke investorers beslutninger om å kjøpe eller selge verdipapirer om den blir offentliggjort.  For å sjekke fremgangen din, klikk på Meny-knappen  Flott gjort!  Du har fullført del 2 av 4  Klikk på framover-pilen for å fortsette å lære |
| [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. | Nå som du har god forståelse av de ulike typene opplysningene du sannsynligvis møter i løpet av arbeidsdagen din, her er det du kan gjøre for å bidra til å beskytte dem. |
| [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. | Før du får tilgang til sensitive opplysninger, må du alltid sørge for at arbeidsrollen og ansvaret ditt påkrever at du får tilgang til opplysningene.  Hvis du har et spørsmål om hvorvidt du bør få tilgang til opplysningene, spesielt med hensyn til personlige opplysninger, kontakt lederen din, OEC eller et medlem av det globale personvernsteamet.  KLIKK PÅ «VISSTE DU»-KNAPPEN FOR MER INFORMASJON. |
| [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. | VISSTE DU  Abbott engasjerer seg i forskjellige former for lovlig overvåkning for å redusere risikoen for upassende bruk av opplysninger.  Dette inkluderer å overvåke nedlastning av opplysninger eller sending av opplysninger til e-postadresser utenfor 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. | Hvis du har tillatelse til å få tilgang til sensitive opplysninger, må du bare bruke disse opplysningene til det spesifikke formålet du er gitt tilgang for.  Når det gjelder personlige opplysninger, må du kun bruke opplysningene i henhold til gitt samtykke eller gitt varsel. |
| [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. | Før du deler sensitive opplysninger, må du sørge for at personen du planlegger å dele med har riktig autorisasjon.  Hvis du har spørsmål om hvorvidt du bør få tilgang til opplysningene, spesielt med hensyn til personlige opplysninger, snakk med lederen din eller et medlem av Abbotts personvernsteam. |
| [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. | Forespørsler fra ditt eget land  Hvis en Abbott-ansatt i samme land ber om sensitive opplysninger, må du alltid:   * bekrefte identiteten til den personen som fremmer forespørselen, * bekrefte personens behov for å få tilgang til informasjonen, * kontrollere for å sikre at personen er autorisert til å motta informasjonen, * verifisere at informasjonen kan brukes til det forespurte formålet og * kun dele den mengden informasjon som kreves for å dekke behovet, ikke mer.   Hvis du er i tvil, kontakt OEC eller det globale personvernteamet før du deler de sensitive opplysningene. |
| [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. | Forespørsler fra andre land  Mange land og regioner har regelverk for å beskytte sine borgeres rettigheter, og har begrensninger på overføring av personlige opplysninger over landegrensene.  Hvis du mottar en forespørsel om informasjon som inneholder sensitive opplysninger fra en kollega i et annet land enn ditt eget, må du undersøke retningslinjene for personvern for din avdeling eller funksjon, eller rådføre deg med OEC eller det globale personvernteamet før du fortsetter. Følg deretter de samme trinnene som om du skulle ha svart på en forespørsel fra en kollega i ditt eget land. |
| [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. | Forespørsler fra tredjeparter  Hvis forespørselen om sensitive opplysninger kommer fra en tredjepart, må du forsikre deg om at det er en gyldig og passende kontraktavtale på plass. Hvis du er usikker, kontakt OEC, det globale personvernsteamet eller juridisk avdeling før du deler. |
| [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. | Arkiver eller slett alltid sensitive opplysninger på en måte som er i samsvar med Abbotts krav til forvaltning, lagring og sletting av opplysninger. |
| [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. | Hvis du mottar en juridisk oppbevaringsordre, må du aldri forkaste, ødelegge eller slette informasjon som dekkes av ordren.  Hvis du har spørsmål relatert til juridiske oppbevaringsordren eller oppbevaring og sletting, kontakt advokaten/advokatassistenten oppført i varselet om oppbevaringsordren eller ring prosedyreavdelingen på (224) 667-5701. |
| [Screen 34](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37)  [44\_C\_37](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37) | Always take special care with sensitive data when someone leaves Abbott.  Managers must ensure the departing employee is terminated in the appropriate system (e.g., Workday for Employees or Fieldglass for Contingent Workers) as soon as they are notified the employee is leaving. This will ensure access to Abbott data, physical access to buildings, and final pay will be properly managed. | Vær alltid forsiktig med sensitive opplysninger når noen forlater Abbott.  Ledere må sikre at medarbeideren som skal slutte avsluttes i det riktige systemet (f.eks. Workday for medarbeidere eller Fieldglass for innleide arbeidere) så snart de får beskjed om at medarbeideren skal slutte. Dette vil sikre at tilgang til Abbott-opplysninger, fysisk tilgang til bygninger og endelig betaling vil bli administrert riktig. |
| [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. | Sikre at ingen sensitive opplysninger blir tatt med av medarbeideren som skal slutte. Overfør alle filer til Abbott-medarbeideren som vil påta seg rollen eller ansvaret til den som forlater virksomheten.  Påminn medarbeideren som skal slutte om forpliktelsen til å ikke beholde eller offentliggjøre sensitive opplysninger. Medarbeidere kan ikke ta sine arbeidsprodukter eller noe annen Abbott-eiendom (f.eks. mobile enheter) med seg når de forlater Abbott. Hvis du har spørsmål om de lokale avslutningsprosessene dine, kontakt personalavdelingen. |
| [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. | Utilsiktede offentliggjøringer av beskyttet helseinformasjon kan skje til enhver tid.  Du kan for eksempel overhøre en sykepleier diskutere detaljer om en pasients helsestatus, eller du kan ved et uhell bli lagt til som mottaker på en e-post som inneholder detaljer om en pasients journal. |
| [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. | I respons på eventuell utilsiktet eller upassende offentliggjøring av en pasients beskyttede helseinformasjon (PHI), bør du umiddelbart rapportere hendelsen til OEC eller et medlem av det globale personvernteamet. |
| [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. | Hvis du blir klar over upassende eller utilsiktet offentliggjøring av konfidensielle forretningsopplysninger, må du umiddelbart rapportere offentliggjøringen til både:   * Din direkte overordnede, og * OEC eller et medlem av det globale personvernsteamet.   Din umiddelbare rapportering av offentliggjøringen vil hjelpe Abbott med umiddelbart å få tilbake informasjonen, hindre ytterligere upassende bruk eller misbruk av informasjonen og, hvis aktuelt, hjelpe selskapet med søksmål eller strafferettslige tiltak. |
| [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. | Du må aldri fremlegge sensitive Abbott-opplysninger til noen som ikke er autorisert til å motta de sensitive opplysningene.  Du bør likeledes kun bruke sensitive Abbott-opplysninger på vegne av Abbott og mens du utfører dine Abbott-forretningsfunksjoner.  Hvis du offentliggjør sensitive opplysninger på en upassende måte, kan du stå ovenfor disiplinærtiltak, inkludert avslutning av ansettelse. |
| [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. | Du har ikke lov til, både under og etter arbeidsforholdet ditt hos Abbott, å dele sensitive Abbott-opplysninger med noen Abbott-konkurrent. |
| [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. | Manglende evne til å returnere sensitive opplysninger til Abbott, overføring av sensitive opplysninger til en ikke-godkjent enhet, konto eller server, eller å gi sensitive opplysninger til noen person eller enhet som ikke er autorisert til å være i besittelse av informasjonen, kan føre til at Abbott tar rettslige tiltak mot deg.  KLIKK PÅ «JURIDISKE TILTAK»-KNAPPEN FOR MER INFORMASJON. |
| [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. | JURIDISKE TILTAK  Juridiske tiltak kan inkludere at Abbott sender inn et søksmål mot deg som ville:   * Hindre deg i å jobbe for en ny arbeidsgiver inntil sensitive Abbott-opplysninger er blitt returnert og beskyttet; * Kreve at du gir alle elektroniske enheter til Abbott for gjennomgang og inspeksjon; * Føre til at du må betale økonomisk erstatning for ulovlig bevaring og/eller bruk av sensitive Abbott-opplysninger, og føre til at du overtrer pliktene og forpliktelsene du skylder Abbott under din arbeidsavtale med Abbott; og * Forplikte deg til å betale saksomkostninger Abbott pådrar seg som følge av et søksmål Abbott legger frem for å beskytte sine sensitive opplysninger.   Om nødvendig vil Abbott også jobbe med lokale, statlige og føderale myndigheter for å beskytte og beholde sensitive Abbott-opplysninger. I dette scenarioet kan du også bli gjenstand for strafferettslige reaksjoner. |
| [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. | Enhver hendelse som involverer et potensielt brudd på informasjonssikkerhet, inkludert en mistet eller stjålet mobil enhet, skal rapporteres umiddelbart til din lokale globale servicedesk.  Hvis du er bekymret for et potensielt brudd eller ønsker å rapportere en potensiell personvernhendelse, kontakt globalt personvern. |
| [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 | Klikk på pilen for å starte gjennomgangen din.  Gjennomgang  Ta deg tid til å gjennomgå noen av nøkkelkonseptene dekket i denne delen.  Få tilgang til og bruk av sensitive opplysninger  Få kun tilgang til og bruk sensitive opplysninger for det spesifikke formålet du er gitt tilgang for.  Deling av sensitive opplysninger  Deling av sensitive opplysninger:   * bekreft identiteten til den som forespør, * bekreft deres behov for å få tilgang til informasjonen, * verifiser at informasjonen kan brukes til de(t) forespurte formålet(ene) og * del kun mengden informasjon som kreves for å dekke behovet.   Oppbevaring og sletting av sensitive opplysninger  Arkiver eller slett alltid sensitive opplysninger på en måte som er i samsvar med Abbotts krav til forvaltning, lagring og sletting av opplysninger.  Respons på utilsiktet offentliggjøring av beskyttet helseinformasjon  I respons på eventuell utilsiktet eller upassende offentliggjøring av en pasients beskyttede helseinformasjon, rapporter offentliggjøringen umiddelbart til OEC eller et medlem av det globale personvernteamet.  Rapportering av en personvernhendelse  Kontakt det globale personvernteamet for å rapportere en potensiell personvernhendelse.  For å sjekke fremgangen din, klikk på Meny-knappen  Flott gjort!  Du har fullført del 3 av 4  Klikk framover-pilen for å fortsette å lære |
| [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. | Hvor du kan få hjelp  Kontoret for etikk og samsvar (OEC)  Globalt personvern – kontakt Globalt personvern via e-post på [privacy@abbott.com](mailto:privacy@abbott.com). Du finner ytterligere kontaktdetaljer og viktig informasjon om personvern på Globalt personvern-portalen [her](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) på Abbott World og her på Abbott World.  OEC-kontakter – Du oppfordres til å kontakte OEC til enhver tid med eventuelle etikk- eller samsvarsspørsmål, eller for å diskutere bekymringer om mulig overtredelse av våre skriftlige standarder, lover eller forskrifter.   * Gå til [Kontakt OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx)-siden på [OEC-nettstedet](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) på Abbott World eller [OEC@abbott.com](mailto:OEC@abbott.com).   ENTERPRISE CYBERSECURITY – NETTSIKKERHET FOR VIRKSOMHETEN  Gå til nettstedet for Enterprise Cybersecurity [her](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) på Abbott World.  Gå til nettstedet for [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) for å lære om sikre måter å dele informasjon på.  Juridisk avdeling  Kontakt [juridisk avdeling](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) med spørsmål eller bekymringer angående tredjeparts kontraktsforpliktelser angående personvern og databeskyttelse.  Kontakt teamet for informasjonsstyring på [information.governance@abbott.com](mailto:information.governance@abbott.com) med spørsmål eller bekymringer angående oppbevaringskrav eller for veiledning om akseptabel bruk av teknologiløsninger.  REFERANSERETNINGSLINJER:   * Klikk [her](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) for å gå gjennom retningslinjene for konfidensiell informasjon * Klikk [her](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) for å gå gjennom Abbotts retningslinjer for innsidehandel * Klikk [her](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) for å gå gjennom retningslinjene for akseptabel teknologibruk. * Klikk [her](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) for å gå gjennom retningslinjene for oppføringer og informasjon på M-Files.   OEC-retningslinjer og prosedyrer  For vårt selskaps globale og landsspesifikke OEC-retningslinjer og prosedyrer:   * Abbott-ansatte bør besøke [iComply](https://icomply.abbott.com/Default.aspx).   Human Resources Service Center   * Klikk [her](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) for en liste over kontaktnumre for HR-støtte.   Kursressurser  Utskrift  Klikk [her](file:///D:/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) for en full utskrift av dette kurset. |
| [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. | Kunnskapssjekken består av 10 spørsmål. Du må score 80 % eller høyere for å fullføre kurset.  Når du er klar, klikker du på knappen **Kunnskapssjekk**. |
| 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? | Med antagelse om at du har jobbet for Abbott i flere år og nylig har akseptert et tilbud om å jobbe for et annet selskap, hvilke av følgende ville du legalt ha tillatelse til å ta med deg når du slutter? |
| 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] Personlig pasientinformasjon fra kliniske studier  [2] Abbott-kundelister og presentasjonsinformasjon som du laget mens du jobbet for Abbott  [3] Salgsprognoser og økonomiske data for din Abbott-avdeling eller -forretningsenhet  [4] Personlige bilder og suvenirer |
| 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. | Det riktige svaret er 4. Personlige opplysninger, konfidensielle forretningsopplysninger og beskyttet helseinformasjon regnes alle som sensitive opplysninger som du ikke kan ta med deg eller bruke etter at du har sluttet hos Abbott. I tillegg må alle Abbotts elektroniske enheter og annen Abbott-eiendom returneres før du slutter.  For mer informasjon, se del 3.4, Respons på upassende offentliggjøringer. |
| 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. | En markedsføringsleder jobber på en ny prosjektlansering og må opprette et samtykkeskjema for potensielle kunder. Skjemaet vil muliggjøre innhentingen og bruken av personlige opplysninger. For å være på linje med Abbotts praksis for samtykke, hvilke av følgende må være sanne for samtykkeskjemaet?  Kryss av for alle riktige svar. |
| 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] Skjemaet må ikke presse kunder til å gi sitt samtykke.  [2] Skjemaet må gi kunder all informasjon om hvordan deres personlige opplysninger vil brukes.  [3] Skjemaet må kreve at kunder aktivt samtykker til innhentingen og bruken av deres personlige opplysninger.  [4] Skjemaet må ikke tillate kunder å trekke tilbake sitt samtykke når de har gitt det. |
| 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. | Abbotts praksis for samtykke krever at skjemaet:   * Er klart og konsist. * Ikke presser personer til å gi sitt samtykke. * Oppgir all informasjon om hvordan personlige opplysninger vil brukes. * Krever at personer aktivt samtykker til innhentingen og bruken av deres personlige opplysninger. * Tillater tilbaketrekking av samtykke hvis dette er ønskelig.   For mer informasjon, se del 1.3, Abbotts prinsipper for innebygd personvern. |
| Screen 46  Question 3: Scenario  63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Offentliggjøring og bruk av sensitive opplysninger, som for eksempel personlige opplysninger, administreres hos Abbott gjennom: |
| Screen 46  Question 3: Options  64\_C\_48 | [1] De-identification of all data.  [2] Access controls.  [3] Both 1 and 2. | [1] Avidentifisering av alle opplysninger.  [2] Tilgangskontroller.  [3] Både 1 og 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. | Offentliggjøring og bruk av personlige opplysninger administreres gjennom tilgangskontroller og andre prosesser som begrenser tilgang og bruk til enkeltpersoner i spesifikke jobbfunksjoner, og for de spesifikke formålene som er angitt i varselet som samtykket ble gitt for.  For mer informasjon, se del 1.3, Abbotts prinsipper for innebygd personvern. |
| 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. | Hvilke av følgende er sanne med hensyn til oppbevaring og sletting av personlige opplysninger?  Kryss av for alle riktige svar. |
| 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] Personlige opplysninger oppbevares bare i den tiden som er nødvendig for å utføre det de ble innhentet og behandlet for.  [2] Når opplysninger ikke lenger er påkrevd i et aktivt produksjonsmiljø, bør de alltid slettes.  [3] Oppbevaring og sletting av personlige opplysninger er underlagt eventuelle oppbevaringsordre knyttet til juridiske forhold. |
| 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. | Generelt sett bør Abbott kun oppbevare personlige opplysninger så lenge det er nødvendig for å utføre det de ble innhentet og behandlet for. Når opplysninger ikke lenger er påkrevd i et aktivt produksjonsmiljø, bør de enten arkiveres eller slettes, på en måte som er i samsvar med Abbotts krav til forvaltning, oppbevaring og sletting av opplysninger. Krav til oppbevaring og sletting er også underlagt eventuelle oppbevaringsordre knyttet til juridiske forhold.  For mer informasjon om riktig svar, del 1.3, Abbotts prinsipper for innebygd personvern. |
| 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. | En ingeniør jobber med å utvikle et nytt produkt. Hvilke av følgende skal regnes som konfidensielle forretningsopplysninger som må holdes sikre?  Kryss av for alle riktige svar. |
| 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] Salgsprognoser og prognoser for det nye produktet.  [2] Finansielle rapporteringsopplysninger fra Abbots årsrapport.  [3] Innkjøpsinformasjon, så som anbud på kontrakter for det nye produktet.  [4] Konkurranseinformasjon om lignende produkter.  [5] Forslag fra tredjepartsleverandører relatert til det nye produkter. |
| 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. | Konfidensielle forretningsopplysninger er en bred kategori. Det inkluderer mye av forretningsopplysningene vi daglig bruker og kommer i kontakt med. En god måte å bekrefte om noe er konfidensielt på, er å stille deg selv et enkelt spørsmål:  Er denne informasjonen offentlig tilgjengelig?  Hvis svaret er nei, er informasjonen med all sannsynlighet konfidensiell, og du bør iverksette passende tiltak for å beskytte den.  For mer informasjon, se del 2.1, Gjenkjenne konfidensielle forretningsopplysninger. |
| 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: | Personvernforordningen (GDPR) er én av de mest omfattende personvernlovgivningene i verden. Den ble implementert i 2018 og er standarden for personvernbeskyttelse. Denne forskriften ble designet i: |
| Screen 46  Question 6: Options  73\_C\_48 | [1] Canada  [2] Asia  [3] Europe  [4] Russia  [5] United States  [6] Latin America | [1] Canada  [2] Asia  [3] Europa  [4] Russland  [5] USA  [6] Latin-Amerika |
| Screen 46  Question 6: Feedback  74\_C\_48 | The correct answer is Europe. In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate.  For more information, see Section 1.2, Legal, Regulatory and Contractual Agreements. | Det riktige svaret er Europa. I Europa er personvernforordningen (GDPR) én av de mest omfattende personvernlovgivningene globalt, og siden implementeringen i 2018 har den satt standarden for personvernbeskyttelse som andre land forsøker å etterligne.  For mer informasjon, se del 1.2, Juridiske, forskriftsmessige og kontraktsmessige avtaler. |
| 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: | Kollegaen din har nettopp fullført et prosjekt som involverte innhenting og bruk av personopplysninger. Han har siden mottatt en forespørsel fra en annen avdeling om å få tilgang til disse opplysninger. Du gir kollegaen din råd om å: |
| 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] Bekrefte identiteten til den som forespør, og deres behov for å få tilgang til informasjonen.  [2] Verifisere at den som forespør er autorisert til å ha en kopi av informasjonen.  [3] Sørge for at opplysningene kan brukes for de forespurte formålene.  [4] Alle de ovennevnte. |
| 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. | Én av de vanligste årsakene til hendelser som angår opplysninger i en organisasjon er deling av opplysninger med uautorisert personell. Før du deler et dokument eller en fil som inneholder sensitive opplysninger, må du alltid:   * bekrefte identiteten til personen som fremmer forespørselen, og personens behov for å få tilgang til informasjonen. * kontrollere for å sikre at personen er autorisert til å ha en kopi av informasjonen. * verifisere at informasjonen kan brukes til de formålene den blir forespurt for. * kun dele den mengden informasjon som kreves for å dekke behovet, ikke mer.   For mer informasjon, se del 3.2, Deling av sensitive opplysninger. |
| 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? | Du er en salgsrepresentant som besøker en klinikk i ditt område. Mens du venter i resepsjonsområdet, legger du ved et uhell fra deg sensitive dokumenter som inneholder en pasients beskyttede helseinformasjon. Hva gjør du? |
| 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] Varsler klinikkens personvernombud.  [2] Kontakter din overordnede.  [3] Rapporterer hendelsen til OEC eller et medlem av det globale personvernsteamet. |
| 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. | I respons på utilsiktet offentliggjøring av en pasients beskyttede helseinformasjon, bør du umiddelbart rapportere hendelsen til både:   * OEC eller et medlem av det globale personvernsteamet.   For mer informasjon, se del 3.4, Respons på upassende offentliggjøringer. |
| 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? | Mens du er på vei til jobb på toget, etterlater du ved et uhell laptopen din som inneholder sensitive arbeidsdokumenter ved setet ditt og forlater toget. Du innser feilen din når du når kontoret ditt og leter etter laptopen din, men du kan ikke finne den noe sted. Hva bør du gjøre først? |
| 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] Ringe togselskapet og spørre om noen har innlevert laptopen din.  [2] Dra tilbake til togstasjonen og lete etter laptopen din.  [3] Kontakte din lokale globale servicedesk. |
| 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. | Hvis du tror at sensitive opplysninger kan ha blitt kompromittert, så som gjennom en mistet eller stjålet laptop, kontakt din lokale globale servicedesk umiddelbart.  For mer informasjon, se del 3.4, Rapportering av en datahendelse. |
| Screen 46  Question 10: Scenario  84\_C\_48 | You should only use personal information:  Check all that apply. | Du bør kun bruke personlige opplysninger:  Kryss av for alle riktige svar. |
| 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] For det spesifikke formålet du er gitt tilgang for.  [2] I henhold til varselet gitt til den registrerte.  [3] I henhold til samtykket gitt av den registrerte. |
| 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. | Hvis du har tillatelse til å få tilgang til personlige opplysninger, bruk dem kun:   * For det spesifikke formålet du er gitt tilgang for. * I henhold til varselet gitt til den registrerte. * I henhold til samtykket gitt av den registrerte.   For mer informasjon, se del 3.1 Få tilgang til og bruke sensitive opplysninger. |
| [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 | Alle spørsmålene er ubesvarte |
| [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. | Ingen resultater er tilgjengelige ettersom du ikke har fullført kunnskapssjekken.  Gratulerer! Du har bestått kunnskapssjekken og fullført kurset.  Se igjennom resultatene dine under ved å klikke på hvert spørsmål.  Når du er ferdig, må du klikke på ikonet **EXIT [X]** i emnetittellinjen før du lukker nettleservinduet eller nettleserfanen.  Beklager, du besto ikke kunnskapssjekken. Ta et par minutter for å se igjennom resultatene dine nedenfor ved å klikke på hvert spørsmål.  Trykk på **Ta kunnskapssjekken på nytt** når du er ferdig. |
| 89\_toc\_1 | Introduction | Introduksjon |
| 90\_toc\_2 | Welcome | Velkommen |
| 91\_toc\_3 | Objectives | Målsetninger |
| 92\_toc\_4 | Menu | Meny |
| 93\_toc\_5 | Personal Information | Personlige opplysninger |
| 94\_toc\_6 | Recognizing Personal Information | Gjenkjenne personlige opplysninger |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Juridiske, forskriftsmessige og kontraktsmessige krav |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Abbotts prinsipper for innebygd personvern |
| 97\_toc\_9 | Review | Gjennomgang |
| 98\_toc\_10 | Confidential Business Information | Konfidensielle forretningsopplysninger |
| 99\_toc\_11 | Recognizing Confidential Business Information | Gjenkjenne konfidensielle forretningsopplysninger |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Kostnaden ved å ikke beskytte konfidensielle forretningsopplysninger |
| 101\_toc\_13 | Insider Information | Innsideinformasjon |
| 102\_toc\_14 | Review | Gjennomgang |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Din rolle i å beskytte sensitive opplysninger |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Få tilgang til og bruk av sensitive opplysninger |
| 105\_toc\_17 | Sharing Sensitive Data | Deling av sensitive opplysninger |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Oppbevaring og sletting av sensitive opplysninger |
| 107\_toc\_19 | Responding to Improper Disclosures | Tilbakemelding på upassende offentliggjøringer |
| 108\_toc\_20 | Review | Gjennomgang |
| 109\_toc\_21 | Knowledge Check | Kunnskapssjekk |
| 110\_toc\_22 | Introduction | Introduksjon |
| 111\_toc\_23 | Assessment | Vurdering |
| 112\_toc\_24 | Question 1 | Spørsmål 1 |
| 113\_toc\_25 | Question 2 | Spørsmål 2 |
| 114\_toc\_26 | Question 3 | Spørsmål 3 |
| 115\_toc\_27 | Question 4 | Spørsmål 4 |
| 116\_toc\_28 | Question 5 | Spørsmål 5 |
| 117\_toc\_29 | Question 6 | Spørsmål 6 |
| 118\_toc\_30 | Question 7 | Spørsmål 7 |
| 119\_toc\_31 | Question 8 | Spørsmål 8 |
| 120\_toc\_32 | Question 9 | Spørsmål 9 |
| 121\_toc\_33 | Question 10 | Spørsmål 10 |
| 122\_toc\_34 | Feedback | Tilbakemelding |
| 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 | Kurset kan ikke kontakte LMS. Klikk på «OK» for å fortsette og gjennomgå kurset. Merk: Kurssertifisering er ikke tilgjengelig. Klikk på «Avbryt» for å avslutte |
| 124\_string\_2 | All questions remain unanswered | Alle spørsmålene er ubesvarte |
| 125\_string\_3 | Questions | Spørsmål |
| 126\_string\_4 | Question | Spørsmål |
| 127\_string\_5 | not answered | ikke besvart |
| 128\_string\_6 | That's correct! | Det er riktig! |
| 129\_string\_7 | That's not correct! | Det er feil! |
| 130\_string\_8 | Feedback: | Tilbakemelding: |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | BESKYTTE SENSITIVE OPPLYSNINGER |
| 132\_string\_10 | Knowledge Check | Kunnskapssjekk |
| 133\_string\_11 | Submit | Send inn |
| 134\_string\_12 | Retake Knowledge Check | Ta kunnskapssjekken på nytt |
| 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. | Beskrivelse av kurset: Hos Abbott bruker vi ofte sensitive opplysninger for å ta viktige forretningsbeslutninger. Fordi mange av våre interessenter har bekymringer i forbindelse med måten disse opplysningene innhentes og brukes på, har Abbott retningslinjer og prosedyrer for å sikre at disse opplysningene blir beskyttet. Dette kurset forklarer hva sensitive opplysninger er, hvorfor de er viktig for virksomheten vår og hvilke skritt vi kan ta for å sikre at vi behandler og håndterer denne informasjonen på en trygg og sikker måte. Det vil ta ca. 30 minutter å fullføre dette kurset. |
| 136\_string\_14 | Menu | Meny |
| 137\_string\_15 | Resources | Ressurser |
| 138\_string\_16 | Reference Material | Referansemateriell |
| 139\_string\_17 | Audio | Audio |
| 140\_string\_18 | Exit | Slutt |
| 141\_string\_19 | Record My Results | Registrer mine resultater |