Coventry Privacy and Security

Protecting Everyone’s Privacy
Module Purpose

Consider this scenario:

A large hospital intended to have outdated patient files securely destroyed. An employee decided to save money by simply placing them in a dumpster outside the hospital.

A few days later, a man working nearby found confidential medical files that had blown into his business' parking lot. Concerned with the finding, he contacted a local news station that aired the story on television.

When individuals provide us their private information, they trust that we will maintain the privacy and security of that information.

Although this scenario seems unlikely, it has happened time and time again. As a result, the hospital spent years trying to rebuild their reputation with their patients, contractors, and the community.

This course will help you understand our commitment to members' privacy and what each of us can do to help maintain privacy and security within Coventry.
Course Objectives

At the end of this course, participants should be able to:

• Understand HIPAA, HITECH and other regulatory requirements
• Explain the permitted uses and proper disclosures of protected health information
• Use the "Need to Know" test
• Identify your role in securing confidential information
• Identify your responsibilities in protecting Coventry's information, equipment, and employees
Introduction to Privacy

A Commitment to Protecting Information

Breaking the trust of our members is one consequence of not protecting their privacy. We are also required by multiple laws and regulations to maintain the privacy of their protected health information.

Some of the most important of those laws and regulations include:

- Health Insurance Portability and Accountability Act of 1996
- HITECH ACT
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley (SOX) Act
- State Privacy Laws
What are HIPAA and HITECH and Why are they Important?

Until Congress passed HIPAA in 1996, personal health information was protected by a patchwork of federal and state laws. Patients' health information may have been distributed without consent for reasons not related to their medical treatment or health care reimbursement.

HIPAA set the following guidelines for the entire health care industry:
• Health care records must be kept private and secure
• Continued access to health care coverage through portability for those who change jobs
• Simplification through standard health care transaction formats
• Effective electronic transactions

HIPAA, along with other state and federal laws, requires that Coventry protect the confidentiality, integrity, and availability of an individual's health information.
HIPAA and HITECH Act

The HITECH Act includes a series of privacy and security provisions that expand the current requirements under the Health Insurance Portability and Accountability Act (HIPAA).

Among other things, the legislation strengthens enforcement of the HIPAA privacy rule, clarifies the definition of a Breach, extends HIPAA to include business associates, increases accountability for logging and reporting accountings of disclosures, and creates a right to be notified in the event of a breach of personally identifiable health information.

In addition to new breach notification requirements and penalty increases, enhancements to current systems and changes to policies and procedures must be made to accommodate statutory changes.

*If you become aware of a breach or potential breach, you must report the event immediately to your supervisor, Business Unit Privacy/Security Leader, or the Privacy Office.*
## HIPAA vs HITECH ACT

Let's take a look at a comparison between HIPAA and the HITECH Act.

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>HITECH</th>
<th>Changes</th>
<th>More Info – see full description in NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Security Incidents reporting</td>
<td>Duty to Notify as a Covered Entity and PHR vendor</td>
<td>HITECH adds very specific reporting duties to the member and HHS immediately in some cases and annually. Previously, only the HIPAA Security rule required notification to the member.</td>
<td>Breach Notification</td>
</tr>
<tr>
<td>Business Associates Agreements</td>
<td>HIPAA Rules apply to Business Associates</td>
<td>HIPAA required Business Associate Agreements to be executed, however HITECH now extends HIPAA regulations to Business Associates.</td>
<td>Business Associates Requirements</td>
</tr>
<tr>
<td>Right to Restrict</td>
<td>Right to Restrict</td>
<td>HIPAA permits disclosures for Treatment, Payment and Health Care Operations without member authorization, however HITECH now allows individuals to restrict disclosures when services are paid for out of pocket.</td>
<td>Right to Restrictions</td>
</tr>
<tr>
<td>Minimum Necessary</td>
<td>Minimum Necessary</td>
<td>Stronger focus on Minimum Necessary standard.</td>
<td>Preferences &amp; Disclosures</td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>Accounting of Disclosures</td>
<td>HITECH adds accounting requirements for disclosures of Treatment, Payment and Operations from an Electronic Health Record. These were formerly carved out of the Privacy Rule Accounting requirements.</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>Remuneration for PHI</td>
<td>Remuneration for PHI</td>
<td>HITECH further protects PHI from sale without member authorization.</td>
<td>No Sale of PHI</td>
</tr>
<tr>
<td>Access to ePHI</td>
<td>Access to ePHI</td>
<td>Must allow members to request Access to PHI in electronic format.</td>
<td>Access to PHI</td>
</tr>
<tr>
<td>Marketing / Fundraising</td>
<td>Marketing / Fundraising</td>
<td>HITECH further protects PHI from being used for Marketing/Fundraising without member authorization.</td>
<td>Marketing</td>
</tr>
<tr>
<td>Penalties / Enforcement</td>
<td>Penalties / Enforcement</td>
<td>Penalties under the HIPAA Enforcement rule have nearly doubled. HIPAA oversight has also been increased by allowing State Attorney General’s to enforcement HIPAA in addition to federal government agencies.</td>
<td>Rule Changes</td>
</tr>
</tbody>
</table>
## Definition of Terms

Before we get into the details of privacy and security, it is important to review some key definitions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>PII is known as personally identifiable information. It can be any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. One example of PII would be an individual's social security number.</td>
</tr>
<tr>
<td>PHI</td>
<td>PHI is known as protected health information. It is information that relates to the past, present, or future physical, mental, or medical condition of an individual. It can also include information related to the provision or payment of health care that can potentially identify an individual. Some examples include health care treatment and diagnoses.</td>
</tr>
<tr>
<td>EPHI</td>
<td>EPHI is known as electronic protected health information. EPHI is the same as PHI but is electronic in nature. Some examples include procedure and diagnosis codes.</td>
</tr>
<tr>
<td>NPPI</td>
<td>NPPI is non-public protected information and is defined as personally identifiable financial information provided by a consumer to a financial institution, including insurance organizations; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution, including insurance organizations. This term does not include publicly available information. One example of NPPI could include financial records or emails.</td>
</tr>
</tbody>
</table>
Who is Covered by HIPAA/HITECH?

Who must comply with HIPAA regulations? Some of the covered areas include:

- Health plans such as Coventry Health Care or self-funded plan sponsors
- Clearinghouses of information, such as Emdeon (formerly WebMD)
- Health care providers
- Business Associates such as persons or organizations that are not part of Coventry's workforce, but perform functions for or provide services to our company, and either create or receive PHI in connection with those functions or services
- Coventry acting as a Business Associate
Individual Rights under HIPAA

Each individual has the following rights under HIPAA:

• Right to request restrictions of disclosures
• Right to request confidential communications
• Right to request an Accounting of Disclosures (AOD) report
• Right to request a copy of his/her Designated Record Set (DRS)
• Right to request amendments to inaccurate information contained in his/her DRS
• Right to file a complaint with Coventry and/or Health and Human Services (HHS) if an individual feels that his/her privacy rights have been violated
Permitted Use and Disclosure of PHI

There are certain circumstances where the Privacy Rule permits Coventry to use or disclose protected health information without a member's consent.

<table>
<thead>
<tr>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
<th>Example 4</th>
<th>Example 5</th>
<th>Example 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>The coordination and management of health care</td>
<td>The administration of benefits including:</td>
<td>Credentialing of providers</td>
<td>Engaging in quality improvement activities</td>
<td>Satisfying National Committee for Quality Assurance (NCQA)/Utilization Review Accreditation Commission (URAC) accreditation requirements</td>
<td>Administering cases and disease management programs</td>
</tr>
<tr>
<td></td>
<td>• Determining member eligibility under a plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reviewing health care services for medical necessity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Responding to grievances and appeals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The "Need to Know" Test

While it may seem difficult at first to determine if it is acceptable to use or disclose protected health information, it is really as simple as taking a quick three-question test.

Question #1: Is PHI/PII really needed to complete the task at hand?

Question #2: Is the PHI/PII required for a particular task?

Question #3: Does the person requesting the PHI/PII really need it to do their job function?

If the answer to any of these questions is NO, then:
STOP!
DO NOT GIVE OUT THE INFORMATION! This could be a HIPAA violation!

If the answer is yes, then take the steps indicated on the next page.
The "Need to Know" Test

Let's assume that you have gone through the "Need to Know" test and you can honestly answer "YES" to all the questions.

Does this mean that you can use the data or provide it to the requestor? Not just yet.

At this point we need to consider the concept called "minimum necessary."

Minimum Necessary

Even if you determine that you or another individual has a need for PHI/PII, you should consider the concept of "minimum necessary."

The Privacy Rule states that the least possible PHI/PII should be used or disclosed to accomplish a given task or process.

For example, if an individual needs a list of members who have terminated from a plan, we should only provide the names. It would not be appropriate to provide social security numbers and other PHI/PII from the members associated with that plan.

Remember: Use the minimum necessary PHI/PII to achieve a given task or process.
De-identification

In addition to providing only the minimum necessary information, another tool available to protect confidential information is de-identification.

De-identification is the removal of all PHI identifiers (PII) so the information may be used freely, and disclosed without the requirement for privacy and confidentiality protections.

If medical information is no longer linked to an individual, it is no longer considered PHI. Therefore, it no longer falls under HIPAA regulations.

De-identified information may be sufficient for many functions such as credentialing or meeting accreditation requirements.

Carefully consider whether the task may be accomplished with de-identified information. If so, use the de-identified information instead of using PHI/PII.

Personal identifiers can be easily overlooked. It is best to confirm with your supervisor/manager, Business Unit Privacy/Security Leader, or the Information Risk Management Team that the information has been fully de-identified.
The Privacy Rule requires that before a covered entity shares PHI/PII with, or receives PHI/PII from a Business Associate, they must contractually agree to take certain steps to protect against unauthorized use or disclosure of PHI/PII. This is called a "Business Associate Agreement."
# PII/PHI Used Internally

It is important to note that HIPAA applies to disclosures within Coventry.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Not Permitted</strong></td>
<td>PHI/PII collected as part of plan operations at HealthAmerica could not be shared with the Altius Health Plan unless there is a need (permitted by HIPAA) or the member has filed an exemption.</td>
</tr>
<tr>
<td><strong>Permitted</strong></td>
<td>HealthAmerica could share PII/PHI with the Customer Service Organization (CSO) as necessary for the CSO to provide services such as claims processing or customer service.</td>
</tr>
</tbody>
</table>
A plan sponsor is an employer, organization, or joint relationship between two or more employers that establishes and maintains an employee benefit plan.

Sometimes, Coventry administers a plan that is sponsored or underwritten by someone other than Coventry. In that case, Coventry is acting as a Business Associate of the plan, not as a Business Associate of the employer or plan sponsor.

So, in a situation like this, what impact does this have for PII/PHI?

**PHI/PII should not be shared with a plan sponsor unless:**

- Applicable requirements for protecting PHI/PII including receipt of the plans sponsor certification have been met.
- The member authorized in writing to make such a disclosure.
A Word about Social Security Numbers

Social security numbers were once used as a common identification tool by businesses and individuals. In recent years, however, federal and state governments have limited the use and disclosure of social security numbers.

The full social security number should not be used or disclosed. If it is necessary to use or disclose a social security number, use only the last four digits. Masking or removing of social security numbers is preferred.
Section 2 Knowledge Check

If you become aware of a breach or potential breach you must report the event immediately to:
- the Privacy Office
- your supervisor
- your Business Unit Privacy/Security

any of the above is a correct action

Which of the following questions are part of the "Need to Know" test? (Select the three that apply and click "Submit")

- Would the member consider this data private?
- Does the person requesting the PHI/PII really need it to do their job?
- Is there medical information contained in the data set?
- Is PHI/PII really needed to complete the task at hand?
- Is the PHI/PII required for a particular task?

Correct – That is right! The three questions of the "Need to Know" test are: 1) Is PHI/PII really needed to complete a task at hand? 2) Is the PHI/PII required for a particular task? and 3) Does the person requesting the PHI/PII really need it to do their job?

Match the definition with the appropriate word at the bottom.

These should not be used as federal and state governments have limited their use. Masking or using only the last four digits is preferred.

Social Security Numbers | PHI | Minimum Necessary

Information that relates to the past, present, or future physical, mental, or medical condition of an individual. It can also include information related to the provision or payment of health care that can potentially identify an individual.

Social Security Numbers | PHI | Minimum Necessary

The least possible PHI/PII that can be used or disclosed to accomplish a given task.

Social Security Numbers | PHI | Minimum Necessary
Summary

Protecting individuals' privacy is a commitment that is not only good business but is required by federal and many state privacy laws. Some of the most important details of this section were:

- The HIPAA and HITECH regulations require protection of personal information.
- Under HIPAA, individuals have the right to restrict data disclosures, receive notice of data disclosures, amend their data, request to see their data, amend their data, request to see their data, or file a complaint with Coventry or the Health and Human Services Department.
- All business lines within Coventry are covered by privacy rules.
- The types of confidential data that must be protected include Protected Health Information (PHI) and Personally Identifiable Information (PII).
- PII is information that can be potentially used to identify an individual.
- PHI is known as Protected Health Information. PHI is a subset of PII and includes information that relates to the past, present, or future physical, mental, or medical condition of an individual. It can also include information related to the provision or payment of health care that can potentially identify an individual.
- Protected health information can be contained in any format including electronic (E PHI) or paper (PHI).
- Use the "Need to Know" test to determine if PHI/PII should be used or given out.
- Another tool to protect private information is "minimum necessary." "Minimum necessary" is when the least possible PHI/PII is used or given out to achieve a given task.
Protecting Information

Information Security
Coventry Security Requirements

As mentioned in the previous section, Coventry has an obligation to protect our members' information. Federal and state laws require us to ensure the confidentiality, integrity, and availability of confidential information including PHI.

Ensuring the confidentiality of our members' information is everyone's responsibility. It only requires a failure of one person for our data and systems to be compromised.

Remember: Security is everyone's business. You are the first line of defense and an important link in maintaining information security.
Maintaining Appropriate Access

To maintain security of information, Coventry and its employees operate under the concept of "least privilege access."

"Least privilege access" means that we provide access to the least possible amount of information to complete a required task or job function.

All requests for information access must be carefully evaluated using the concept of "least privilege."
Password Management

Two of Coventry's most important links in information security defense are your user account and password.

Employees are responsible for taking appropriate steps to secure their passwords including:

• Never sharing your account with ANYONE including your manager and co-workers

• Always creating a strong password

• Never saving your user names and passwords where they can be accessed by others such as in a file or on local or network drives

Remember:
You are responsible for anything that happens under your USER ID and password.

You should Never compromise your password!
Strong Passwords

Your password is what keeps your user account safe. Having a strong password helps keep intruders from accessing our systems and confidential information.

Coventry requires that passwords be:

- A minimum of eight (8) characters in length, mixing letters (both upper and lower case), numbers, and symbols
- Complex enough they should not be easily guessed

Avoid using:

- Any part of your user or logon name
- Pets or relatives names
- Part of an old password
- Consecutive numbers or letters, either backwards or forwards, such as "56789" or "ZYXWVU"
Removable Media Devices

Removable media devices such as flash drives or CDs pose significant disclosure risk of confidential information.

In order to mitigate this risk, encryption standards must be utilized when saving confidential data to removable media. Coventry's encryption standards can be found in InfoSecPolicy 07.01.01 - ENCRYPTION.

Coventry approved methods for transferring of information includes secure FTP's and Zix Secure Messaging. For internal transmissions, use SharePoint or company shared drives.
# Data Classification

Coventry now requires that documents or emails be assigned classifications.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
</table>
| Trade Secret/Competitive Advantage Documents | Information that may be used by Coventry to establish a strategic advantage. Possession, use, or disclosure of this information may be restricted by laws or regulation. This information must also be stored in a secure location at all times and minimum access allowed based upon business need. Documents of this nature should be noted with a footer similar to the one below:  
  Data Classification: Trade Secret/Competitive Advantage. |
| Public Domain Documents               | Disclosure of Public Domain information outside of Coventry would have no adverse impact on the company, its operations, or liability. Documents of this nature should be noted with a footer similar to the one below:  
  Data Classification: Public Domain                                                              |
| Internal Use Only Documents           | Consists of information that is intended to be used within Coventry. This information may be sensitive to personnel, technical, or business operations, but unauthorized disclosure would not significantly impact Coventry, its employees, member, or clients. Documents of this nature should be noted with a footer similar to the one below:  
  Data Classification: Internal Use Only                                                              |
| Confidential Documents                | Disclosure of this information would likely impact Coventry’s operational effectiveness, cause an important financial loss, provide significant gain to a competitor, or cause a major drop in client confidence. Information in this class must be protected. Data integrity is vital. Documents of this nature should be noted with a footer similar to the one below:  
  Data Classification: Coventry Confidential                                                              |
Storage of Confidential Information

Coventry Health Care prohibits employees from storing confidential information locally on any equipment. This includes desktops, laptops, personal home computers, PDAs, or smart devices.

All confidential data must be saved to a network drive and access controls implemented such as file permissions based on the principle of "least privilege access" and approved authorization.
Working Outside the Office Setting

Many Coventry employees have a need to work from remote locations. Employees who work remotely are responsible for protecting confidential information, regardless of the format (paper, electronic).

When in a public environment:

• Never leave portable media devices such as laptops or PDAs unattended in a public environment
• Be aware of your surroundings as others may be able to see confidential information
• When on the phone, be careful not to discuss confidential matters in public locations
Network Security

Employees also play an important role in protecting our networks from outside threats. Some of those threats include viruses, spyware, or hackers.

While Coventry maintains protection against viruses and hackers, there are steps employees can take to help prevent our network from being compromised.

Coventry prohibits the following:

• Connecting non-Coventry owned equipment to the Coventry network
• Downloading and installing software on Coventry computers without appropriate approvals
• Creating wireless hotspots on Coventry's network unless explicitly authorized by the Technical Risk Management Team
• Connect a personal PDA to the network
Security Incidents

As mentioned earlier, you play an important role in protecting our data security. Sometimes, an employee is the first to notice hints that could indicate a security incident.

Below you will find a list of security incident examples. If you notice any of these situations, you must report them to your supervisor/manager, Technical Risk Management Team, Information Security Governance Team, your assigned Business Unit Privacy/Security Leader, by emailing system-security@cvty.com, or the Coventry Comply Line at 1-877-CHC-LINE.

| Data that has been altered or destroyed outside of normal business practice |
| The inability to access data that you are authorized to access |
| Appearance or disappearance of files, or unexpected changes in file size |
| The editing of files when no changes should have occurred |
| Lost or stolen equipment containing Coventry data |
| Unexpected processes, such as email transmissions, which start without user input |

| The attempt to get an individual to disclose information, such as a user name or password, by using human interaction (social engineering) to trick people into disclosing information |
| Introduction of computer viruses that display strange messages or that mislabel files and directories |
| Employees/non-employees attempting to connect non-Coventry owned equipment to a Coventry network |
Electronic Transmission of Confidential Information

The Internet is an open channel and information transmitted is potentially available to unintended recipients.

Coventry and its employees must use approved communication channels with appropriate safeguards when sending PHI and other confidential information to external recipients.

PHI and other confidential information should not be sent outside of Coventry by email unless it is secured. Zix Secure Messaging protects data from being compromised while in transit. Zix Secure Messaging can be used by simply typing cvtysecure in the subject line.
Section 3 Knowledge Check

Based on the guidelines mentioned in the course, which one of the following passwords would be considered "strongest?"

<table>
<thead>
<tr>
<th>Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bertha86!3</td>
<td>While this password contains numbers, letters, and symbols, it DOES NOT contain both upper and lower case letters.</td>
</tr>
<tr>
<td>123bertha45</td>
<td>This password is incorrect because it uses sequential numbers and DOES NOT contain both upper and lower case letters.</td>
</tr>
<tr>
<td>Ber14a1*2x</td>
<td>You are correct. This is the strongest possible password. It contains both upper and lower case letters, numbers, and symbols. Notice how some of the letters in the name have been replaced by numbers. This further helps to strengthen the password.</td>
</tr>
<tr>
<td>4321Bertha*</td>
<td>While this password has upper and lower case letters, numbers, and symbols, it uses a sequential number pattern.</td>
</tr>
</tbody>
</table>

Which of the following MUST be considered when working from outside the office setting? (Select all that apply and click "Submit.")

- Never leave portable media devices such as laptops or PDAs unattended in a public environment.
- Be aware of your surroundings as others may be able to see confidential information.
- Never use a hotel or airport connection. They are not secure.
- When on the phone, be careful not to discuss confidential matters in public locations.

That is correct. You should: never leave portable media devices such as laptops or PDAs unattended in a public environment; be aware of your surroundings as others may be able to see confidential information; and when on the phone, be careful not to discuss confidential matters in public locations.

You need to send some PHI outside of Coventry via email. You have already conducted the "Need to Know" test and are only providing the "minimum necessary" information. What must be typed in the "subject" line of the email message to use Zix Secure Messaging?

- cvtysecure
- CVTYSECURE
- Cvtysecure

That's right! Adding cvtysecure to the subject line of the email will protect your email and make it secure.
Section Summary

By protecting our systems, we can prevent the release of confidential and protected information. Here are some key points from this section:

- System security is everyone's responsibility.
- Access to systems should be granted on the basis of "least privilege".
- Use of strong passwords helps to prevent unauthorized user account access.
- You should never compromise your password.
- Use Zix Secure Messaging when sending PHI/PII via email by typing "cvtysecure" in the subject field.

When working outside the office setting, be cautious of those around you and never leave portable media devices unattended. Be aware of your surroundings when having phone conversations outside of the office.

Removable media devices, such as USB flash drives and CDs, may not be used to store confidential information unless approved encryption technology is used.

Do not install software to your Coventry PC without the appropriate permissions.
Non-Coventry owned equipment should not be connected to the Coventry network.
Never connect a Personal Digital Assistant (PDA) to the Coventry network.
Physical Security

Protecting Coventry's Assets and Employees
Your Role in Physical Security

Every Coventry employee plays an important role in securing our facilities. There are steps we can take to help ensure the safety of our employees and the company's assets.

<table>
<thead>
<tr>
<th>Physical Security Incidents</th>
<th>ID Badges and Building Access</th>
<th>Visitor Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coventry relies on its employees to be the eyes and ears of our physical security. When an employee encounters a suspected security incident, they must report it.</td>
<td>Our building badge systems are the most effective way to prevent unauthorized access to Coventry facilities. Avoid tailgating others or letting others piggyback behind you.</td>
<td>Coventry identifies, monitors, and restricts access to its facilities by visitors. This is done with a visitor log.</td>
</tr>
</tbody>
</table>
| To report a security incident, you should contact your manager/supervisor/director, Business Unit Privacy/Security Leader, a local facility manager, or by emailing system-security@cvty.com. | Follow these tips:  
Be aware of individuals following closely behind you.  
If a Coventry ID badge is not visible, request to see it.  
If they are unable to present an ID, escort them to the individual responsible for signing in visitors. | All visitors (including visiting employees) are required to sign in with the receptionist, security guard, or other designated person who controls access to the facility. All visitors should be monitored or escorted, as reasonably necessary, during their visit to our facility. |
| | | Visitor log procedures vary from location to location. Check with HR or Facilities at your location. |
Section 4 Knowledge Check

If an employee attempts to follow you into a facility without swiping their badge and their ID is not visible, you should ask to see their Coventry ID. If they do not have their Coventry ID, you should take down their name and employee number, let them in, and contact HR or local security.

True / False

You are right! This is false. Instead of allowing the individual through the door, you should escort them to the person responsible for signing in visitors.
Summary

Protecting the physical facilities where our employees work and our data is stored is an important part of maintaining privacy and security. There are three important things an employee can do to help secure our facilities:

**Visitor Logs** - Visitor logs help us to control, identify, and monitor access to our facilities. All visitors must sign in and wear a visitor badge at all times. In addition, visitors should be escorted as reasonably necessary.

**Physical Security Incidents** - When an employee notices something that seems strange or out of place, it must be reported to a manager/supervisor/director, Business Unit Privacy/Security Leader, a local facility manager, or by emailing system-security@cvty.com.

**ID Badges and Building Access** - Our badge systems provide critical physical security to our facilities. Employees should wear their badges at all times and tailgating and piggybacking are not permitted.
Final Assessment

Instructions

For this quiz you will be given a series of 5 questions, Select the best choice for each question. You must pass the quiz with at least 80% in order to complete this module.
Policy Compliance

Our Privacy and Security Policies can be found on the Policy Center. You can access the Policy Center by typing "policycenter" into your Internet Explorer browser address bar.

All employees are required to adhere to Coventry policies including those pertaining to Privacy and Security.

Employees who fail to follow established Coventry policies will be subject to disciplinary action, up to and possibly including termination of employment.
Course Conclusion

Coventry has a responsibility to our members and business partners to safeguard confidential information entrusted to us. We do this by adhering to our privacy and security policies and standards. By following these privacy and security policies and standards, you can help us maintain the confidentiality of this information.

Once you have passed the quiz, you will have completed the course on Privacy and Security. There are two other modules that must be completed as part of the Coventry Compliance and Ethics Training Program. They are titled "Code of Business Conduct and Ethics" and "Fraud, Waste, and Abuse."

In addition, you must sign the Attestation of Completion and the Confidentiality Agreement.

To close this course, click on the close button (x) in the upper right hand corner.