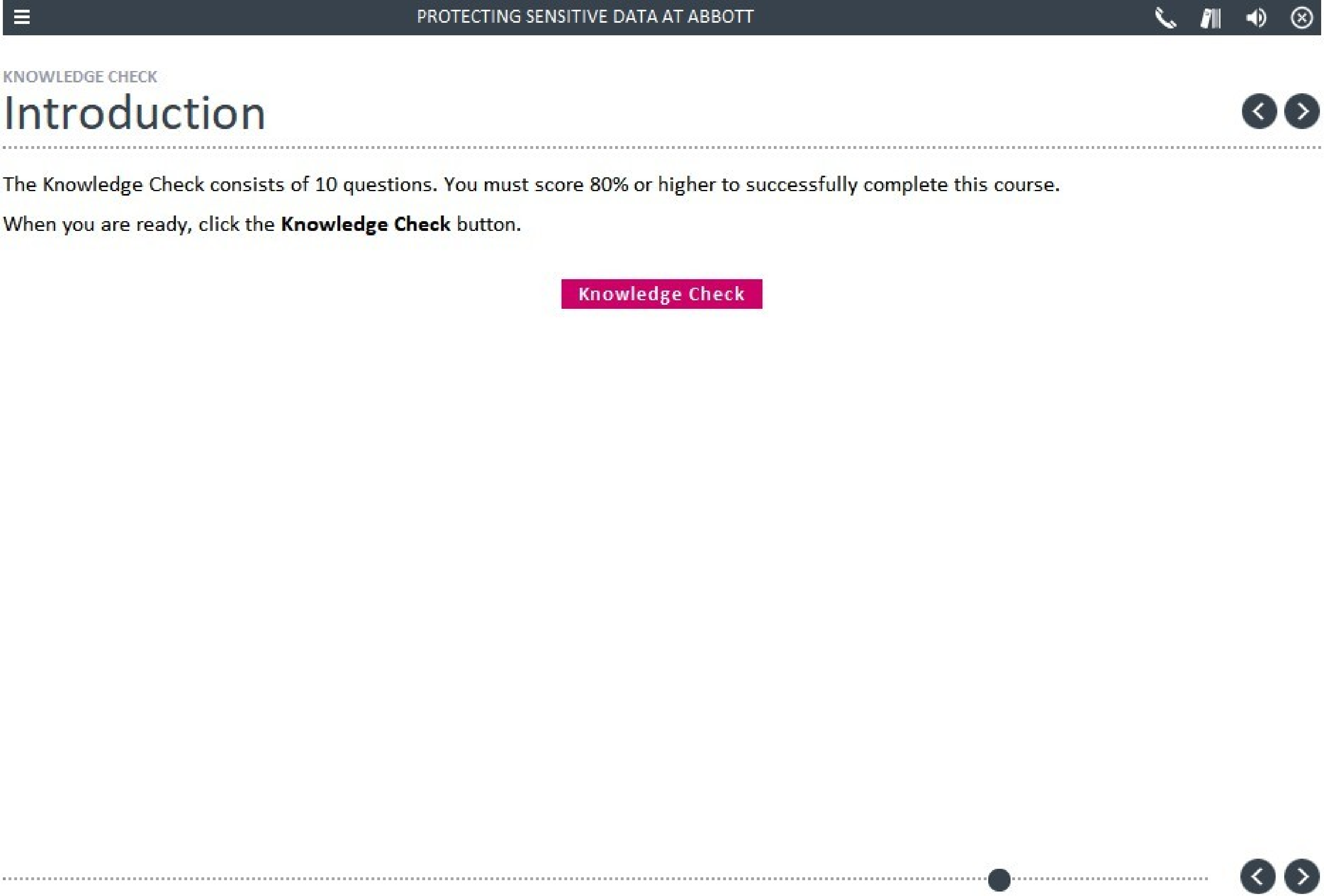


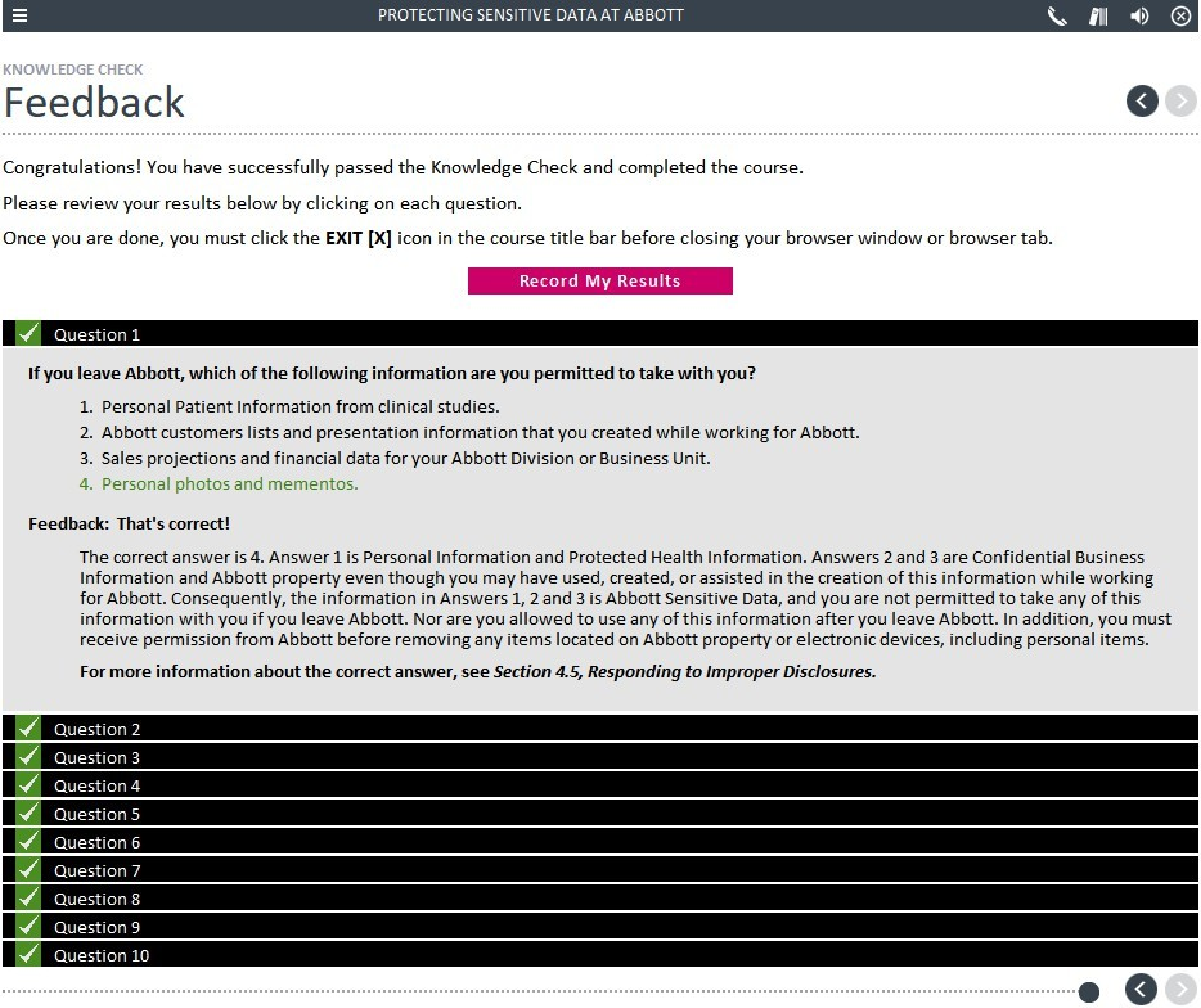
PROTECTING SENSITIVE DATA AT ABBOTT

KNOWLEDGE CHECK

Introduction

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.



KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

If you leave Abbott, which of the following information are you permitted to take with you?

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.

Feedback: That's correct!

The correct answer is 4. Answer 1 is Personal Information and Protected Health Information. Answers 2 and 3 are Confidential Business Information and Abbott property even though you may have used, created, or assisted in the creation of this information while working for Abbott. Consequently, the information in Answers 1, 2 and 3 is Abbott Sensitive Data, and you are not permitted to take any of this information with you if you leave Abbott. Nor are you allowed to use any of this information after you leave Abbott. In addition, you must receive permission from Abbott before removing any items located on Abbott property or electronic devices, including personal items.

For more information about the correct answer, see *Section 4.5, Responding to Improper Disclosures.*

✓ Question 2

✓ Question 3

✓ Question 4

✓ Question 5

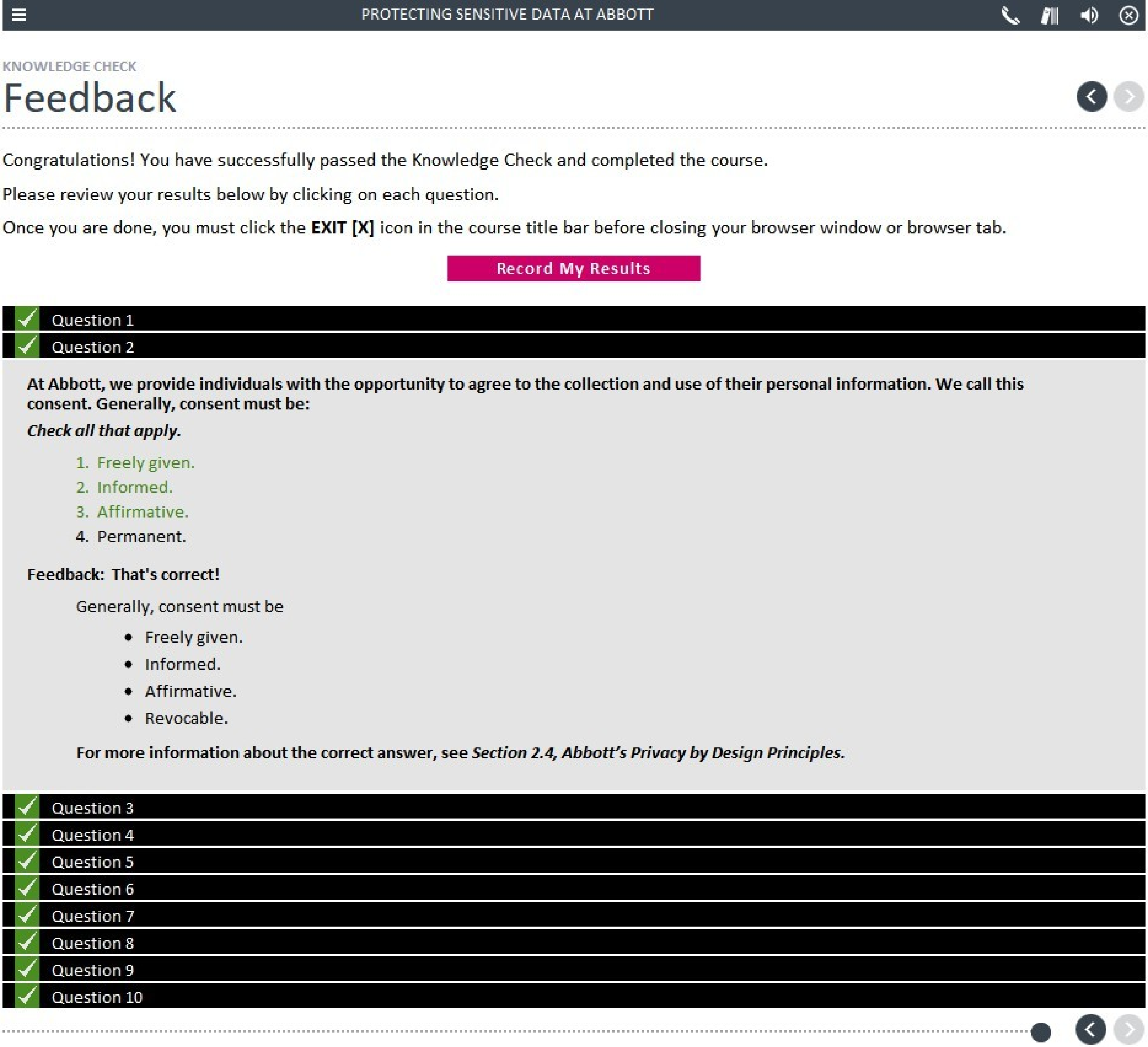
✓ Question 6

✓ Question 7

✓ Question 8

✓ Question 9

✓ Question 10



PROTECTING SENSITIVE DATA AT ABBOTT

KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

At Abbott, we provide individuals with the opportunity to agree to the collection and use of their personal information. We call this consent. Generally, consent must be:

Check all that apply.

1. Freely given.
2. Informed.
3. Affirmative.
4. Permanent.

Feedback: That's correct!

Generally, consent must be

- Freely given.
- Informed.
- Affirmative.
- Revocable.

For more information about the correct answer, see *Section 2.4, Abbott's Privacy by Design Principles.*

✓ Question 3

✓ Question 4

✓ Question 5

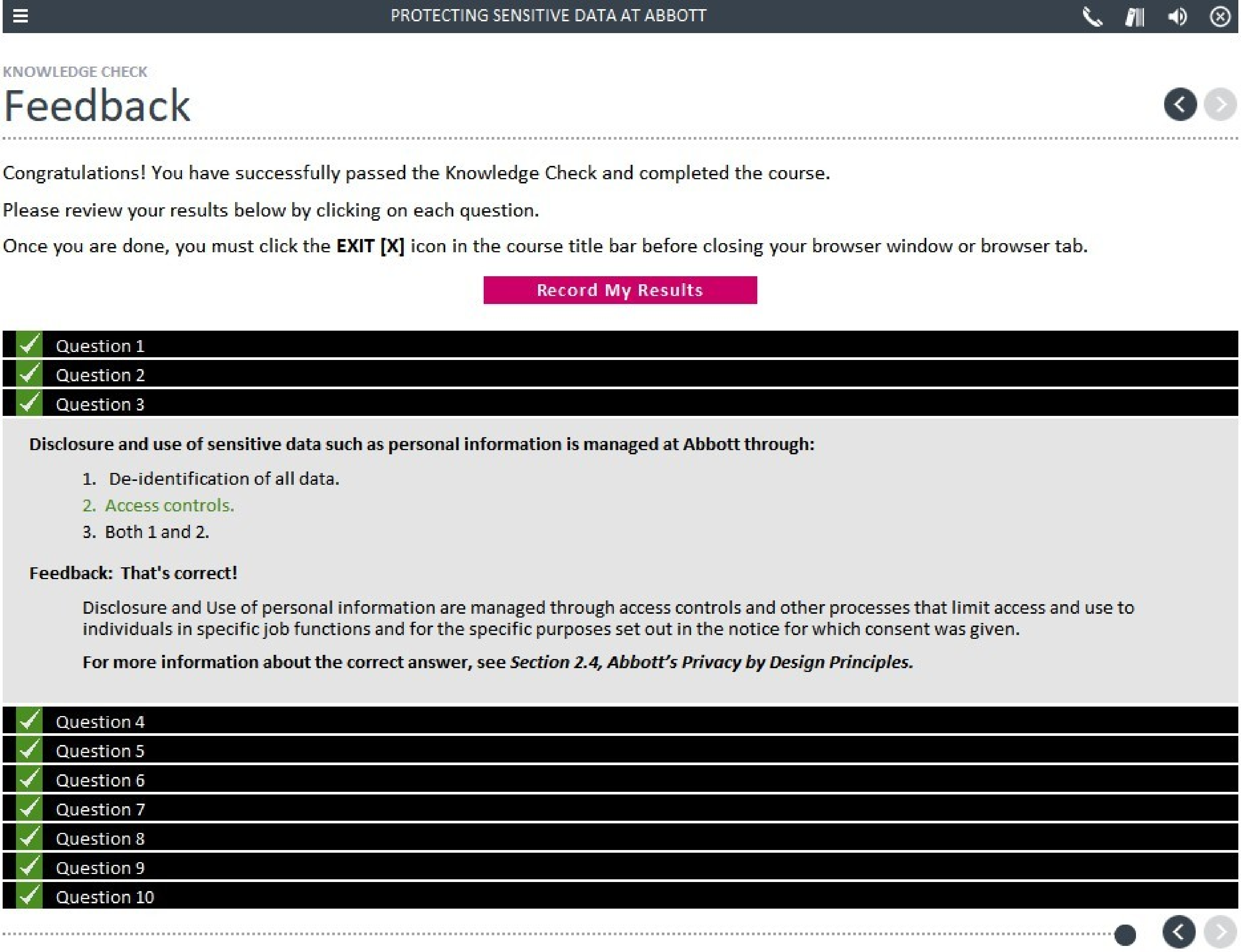
✓ Question 6

✓ Question 7

✓ Question 8

✓ Question 9

✓ Question 10



KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

✓ Question 3

Disclosure and use of sensitive data such as personal information is managed at Abbott through:

1. De-identification of all data.
2. Access controls.
3. Both 1 and 2.

Feedback: That's correct!

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 about the correct answer, see *Section 2.4, Abbott's Privacy by Design Principles.*

✓ Question 4

✓ Question 5

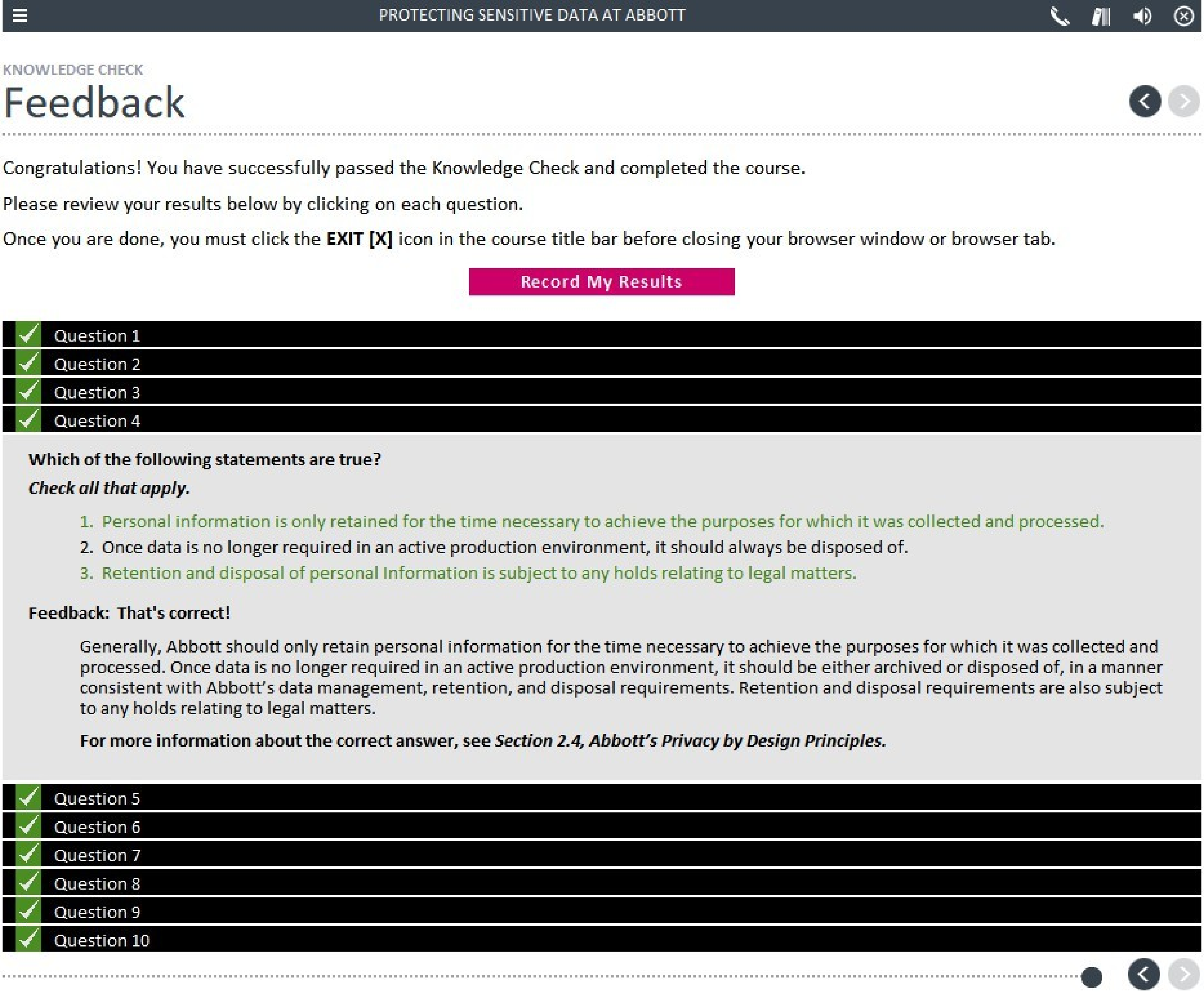
✓ Question 6

✓ Question 7

✓ Question 8

✓ Question 9

✓ Question 10



PROTECTING SENSITIVE DATA AT ABBOTT

KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

✓ Question 3

✓ Question 4

Which of the following statements are true?

Check all that apply.

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.

Feedback: That's correct!

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, see *Section 2.4, Abbott's Privacy by Design Principles.*

✓ Question 5

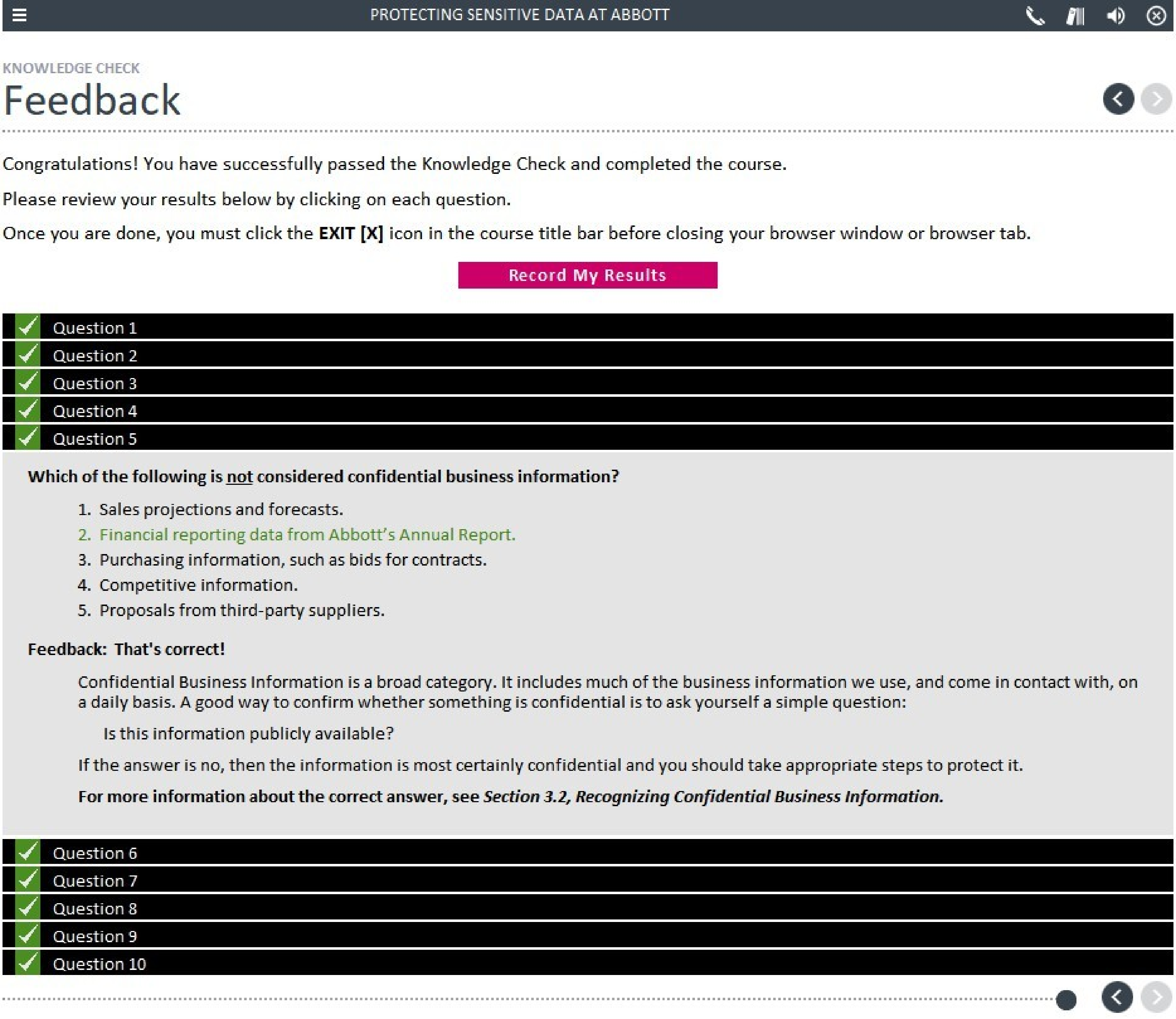
✓ Question 6

✓ Question 7

✓ Question 8

✓ Question 9

✓ Question 10



PROTECTING SENSITIVE DATA AT ABBOTT

KNOWLEDGE CHECK

Feedback

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.

Record My Results

✓ Question 1

✓ Question 2

✓ Question 3

✓ Question 4

✓ Question 5

Which of the following is <u>not</u> considered confidential business information?

1. Sales projections and forecasts.
2. Financial reporting data from Abbott's Annual Report.
3. Purchasing information, such as bids for contracts.
4. Competitive information.
5. Proposals from third-party suppliers.

Feedback: That's correct!

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 about the correct answer, see *Section 3.2, Recognizing Confidential Business Information.*

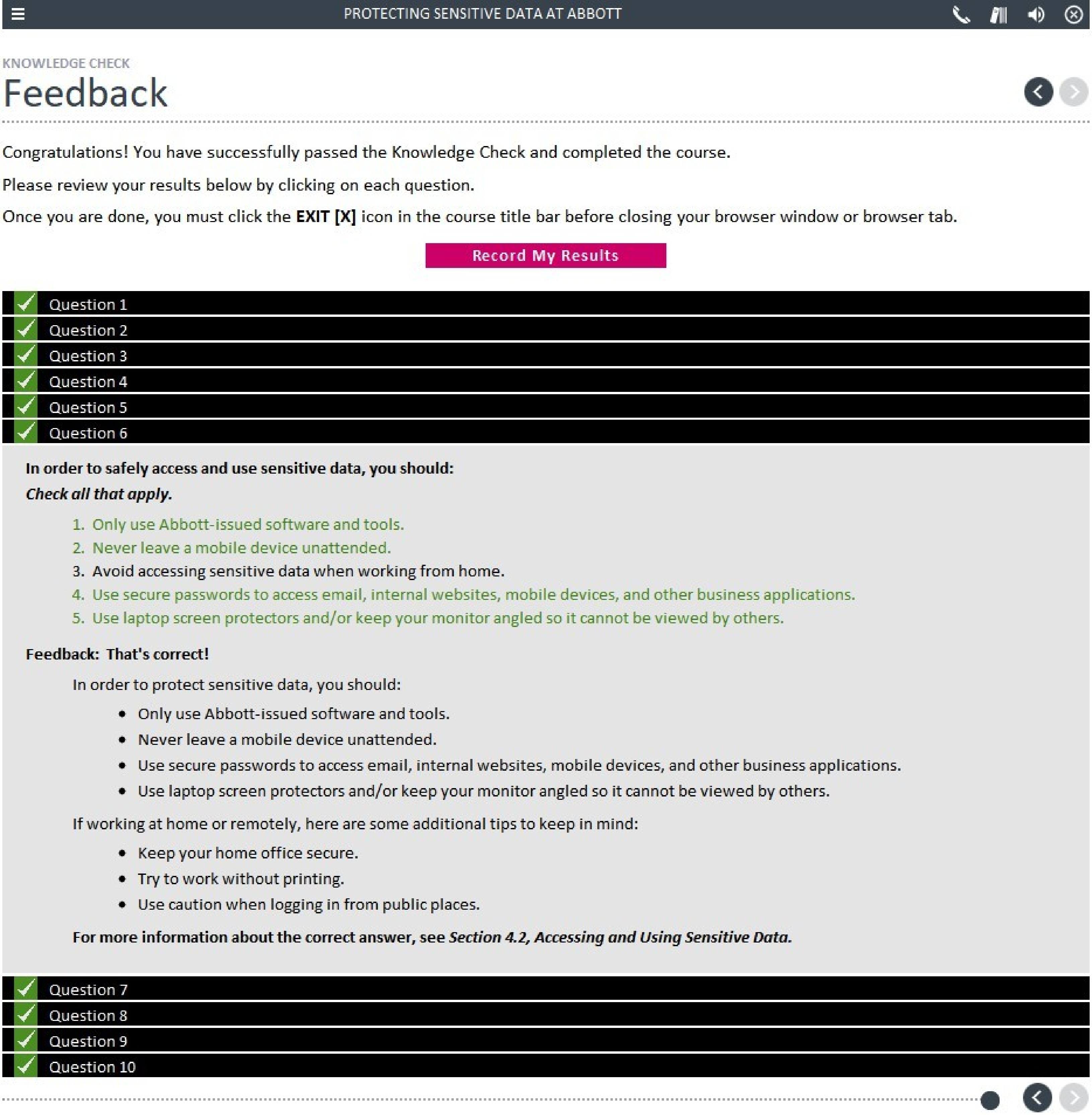
✓ Question 6

✓ Question 7

✓ Question 8

✓ Question 9

✓ Question 10



KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

✓ Question 3

✓ Question 4

✓ Question 5

✓ Question 6

In order to safely access and use sensitive data, you should:

Check all that apply.

1. Only use Abbott-issued software and tools.
2. Never leave a mobile device unattended.
3. Avoid accessing sensitive data when working from home.
4. Use secure passwords to access email, internal websites, mobile devices, and other business applications.
5. Use laptop screen protectors and/or keep your monitor angled so it cannot be viewed by others.

Feedback: That's correct!

In order to protect sensitive data, you should:

- Only use Abbott-issued software and tools.
- Never leave a mobile device unattended.
- Use secure passwords to access email, internal websites, mobile devices, and other business applications.
- Use laptop screen protectors and/or keep your monitor angled so it cannot be viewed by others.

If working at home or remotely, here are some additional tips to keep in mind:

- Keep your home office secure.
- Try to work without printing.
- Use caution when logging in from public places.

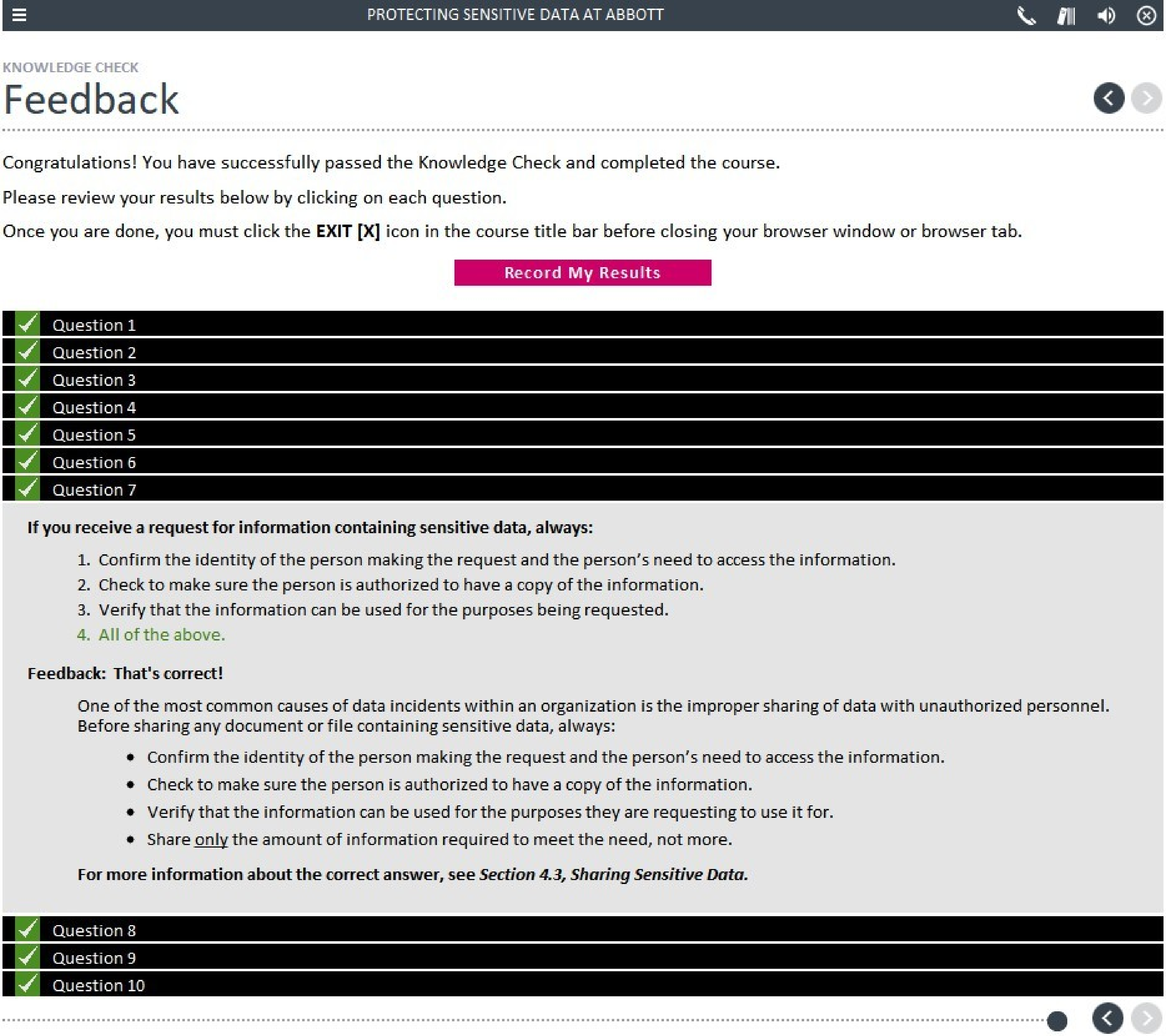
For more information about the correct answer, see *Section 4.2, Accessing and Using Sensitive Data.*

✓ Question 7

✓ Question 8

✓ Question 9

✓ Question 10



KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

✓ Question 3

✓ Question 4

✓ Question 5

✓ Question 6

✓ Question 7

If you receive a request for information containing sensitive data, always:

1. Confirm the identity of the person making the request and the person's need to access the information.
2. Check to make sure the person is authorized to have a copy of the information.
3. Verify that the information can be used for the purposes being requested.
4. All of the above.

Feedback: That's correct!

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:

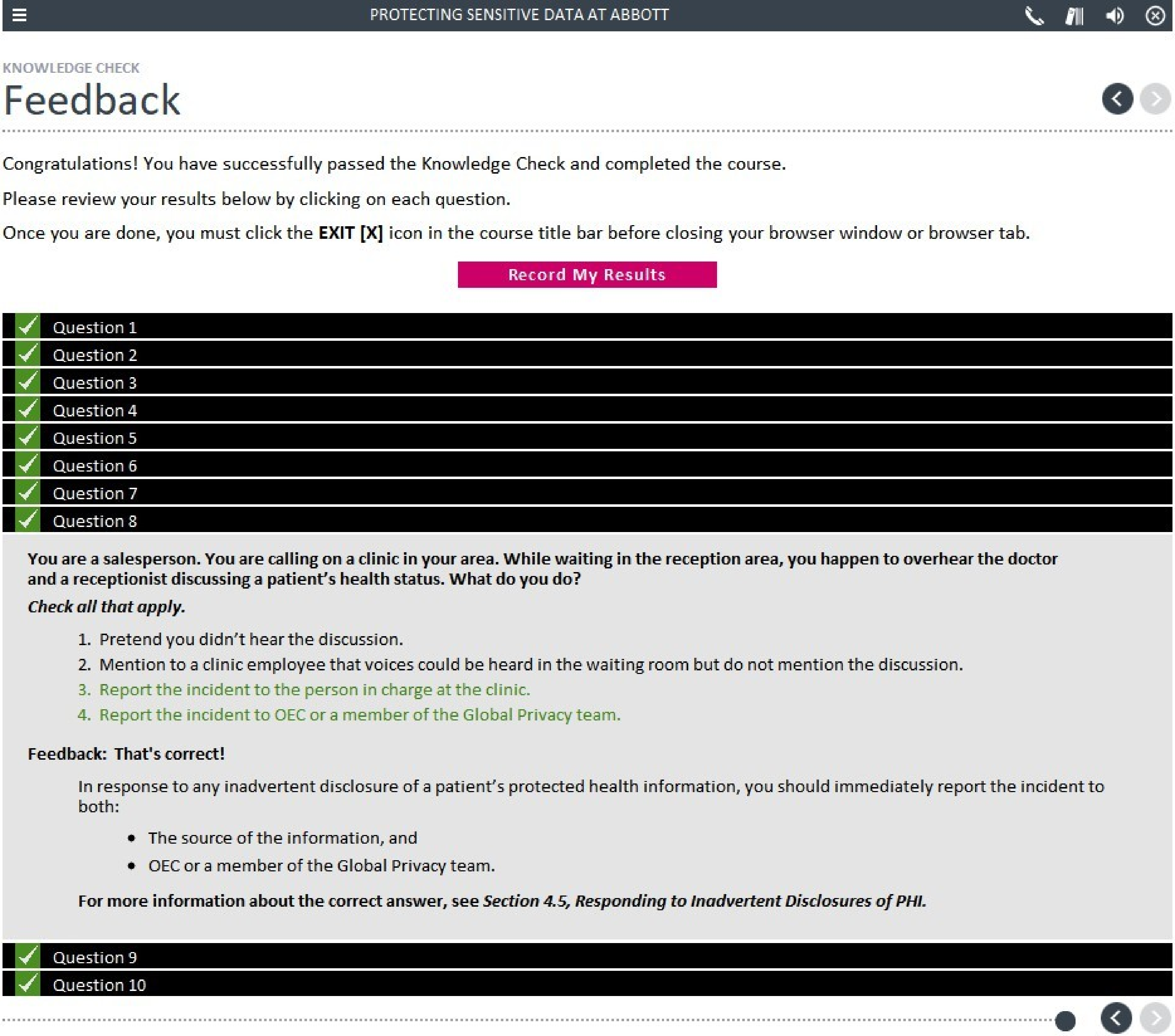
- Confirm the identity of the person making the request and the person's need to access the information.
- Check to make sure the person is authorized to have a copy of the information.
- Verify that the information can be used for the purposes they are requesting to use it for.
- Share only the amount of information required to meet the need, not more.

For more information about the correct answer, see *Section 4.3, Sharing Sensitive Data.*

✓ Question 8

✓ Question 9

✓ Question 10



PROTECTING SENSITIVE DATA AT ABBOTT

KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

✓ Question 3

✓ Question 4

✓ Question 5

✓ Question 6

✓ Question 7

✓ Question 8

You are a salesperson. You are calling on a clinic in your area. While waiting in the reception area, you happen to overhear the doctor and a receptionist discussing a patient's health status. What do you do?

Check all that apply.

1. Pretend you didn't hear the discussion.
2. Mention to a clinic employee that voices could be heard in the waiting room but do not mention the discussion.
3. Report the incident to the person in charge at the clinic.
4. Report the incident to OEC or a member of the Global Privacy team.

Feedback: That's correct!

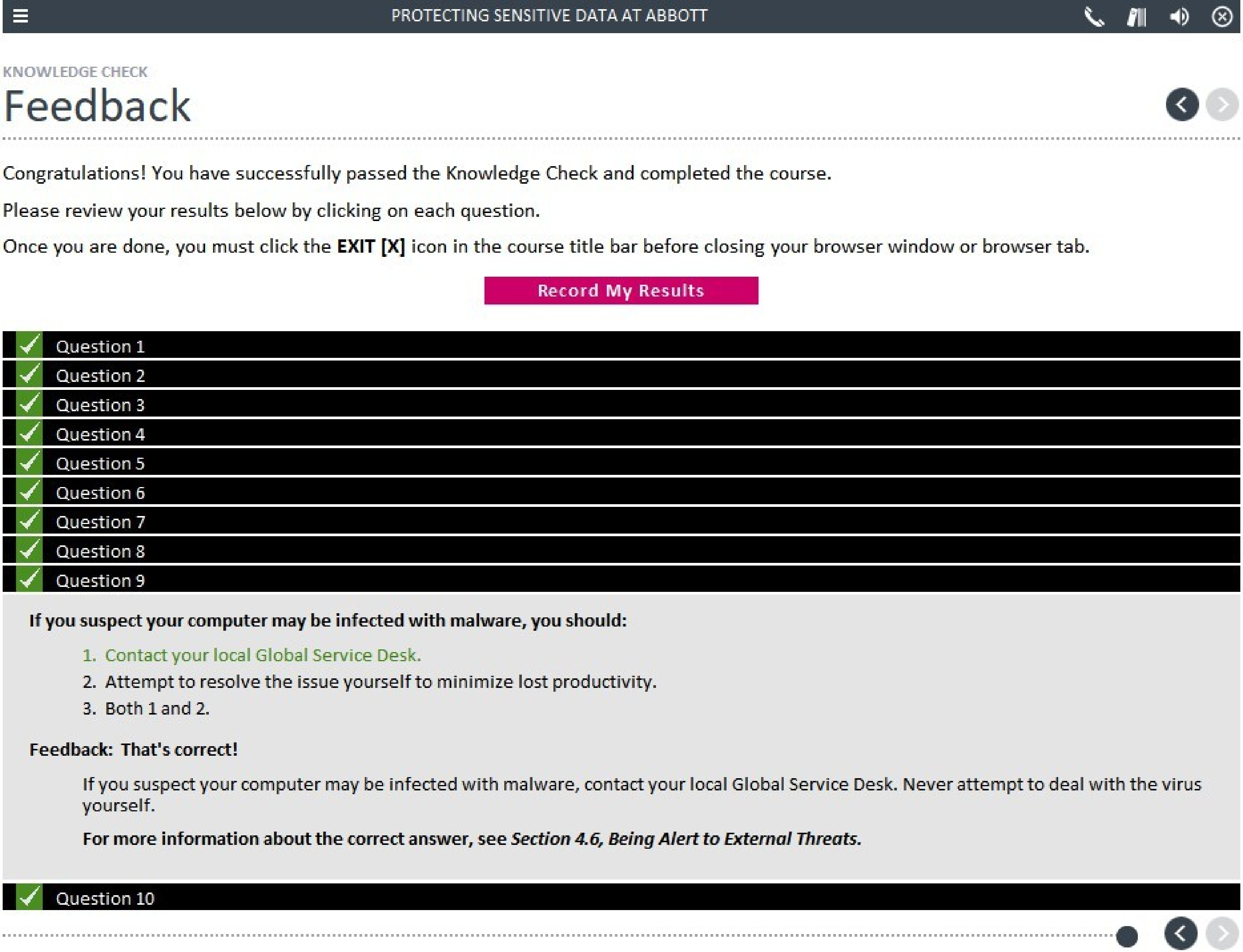
In response to any inadvertent disclosure of a patient's protected health information, you should immediately report the incident to both:

- The source of the information, and
- OEC or a member of the Global Privacy team.

For more information about the correct answer, see *Section 4.5, Responding to Inadvertent Disclosures of PHI.*

✓ Question 9

✓ Question 10



KNOWLEDGE CHECK

Feedback

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.

✓ Question 1

✓ Question 2

✓ Question 3

✓ Question 4

✓ Question 5

✓ Question 6

✓ Question 7

✓ Question 8

✓ Question 9

If you suspect your computer may be infected with malware, you should:

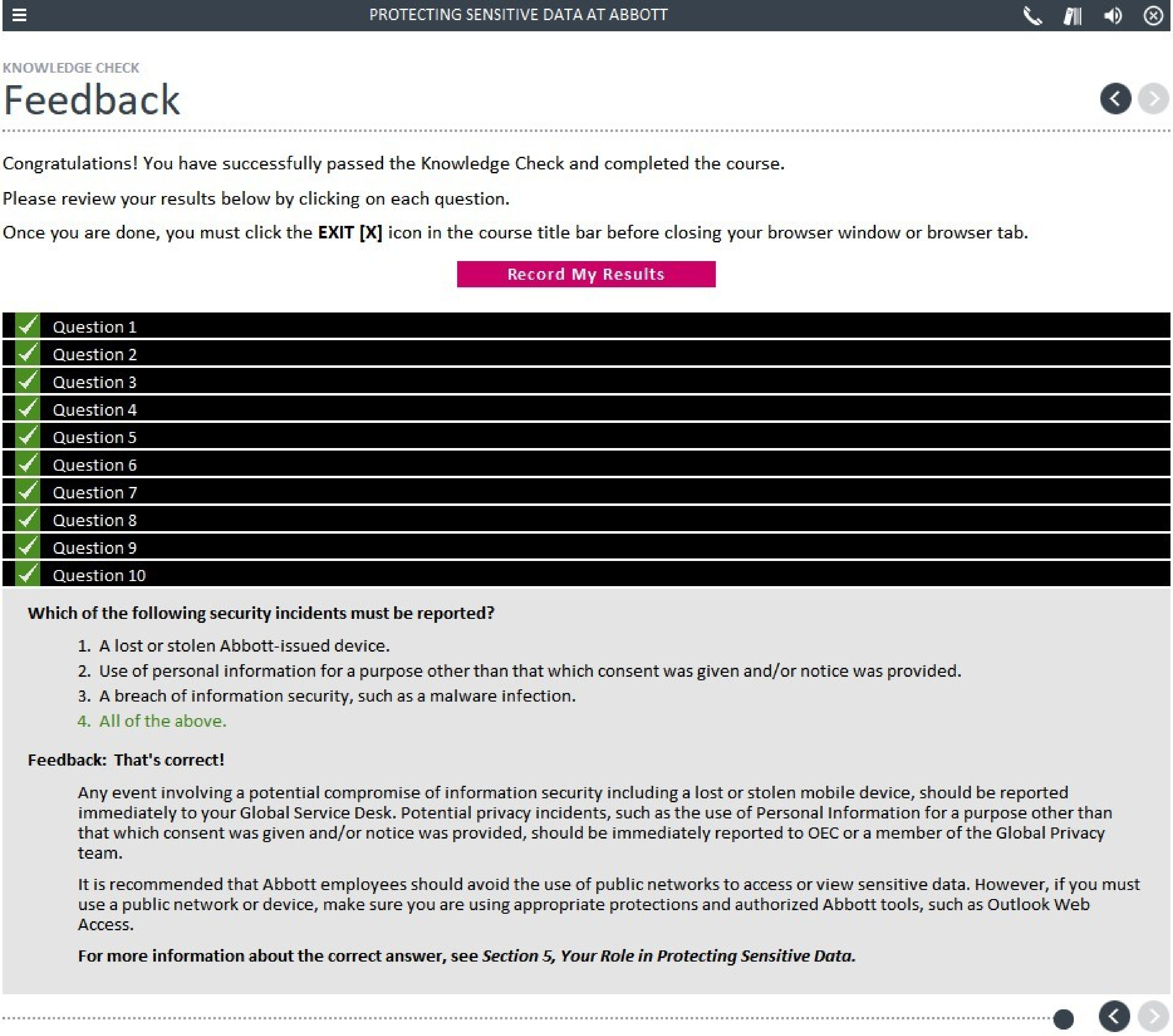
1. Contact your local Global Service Desk.
2. Attempt to resolve the issue yourself to minimize lost productivity.
3. Both 1 and 2.

Feedback: That's correct!

If you suspect your computer may be infected with malware, contact your local Global Service Desk. Never attempt to deal with the virus yourself.

For more information about the correct answer, see *Section 4.6, Being Alert to External Threats.*

✓ Question 10



KNOWLEDGE CHECK

Feedback

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.

- ✓ Question 1
- ✓ Question 2
- ✓ Question 3
- ✓ Question 4
- ✓ Question 5
- ✓ Question 6
- ✓ Question 7
- ✓ Question 8
- ✓ Question 9
- ✓ Question 10

Which of the following security incidents must be reported?

1. A lost or stolen Abbott-issued device.
2. Use of personal information for a purpose other than that which consent was given and/or notice was provided.
3. A breach of information security, such as a malware infection.
4. All of the above.

Feedback: That's correct!

Any event involving a potential compromise of information security including a lost or stolen mobile device, should be reported immediately to your Global Service Desk. Potential privacy incidents, such as the use of Personal Information for a purpose other than that which consent was given and/or notice was provided, should be immediately reported to OEC or a member of the Global Privacy team.

It is recommended that Abbott employees should avoid the use of public networks to access or view sensitive data. However, if you must use a public network or device, make sure you are using appropriate protections and authorized Abbott tools, such as Outlook Web Access.

For more information about the correct answer, see *Section 5, Your Role in Protecting Sensitive Data.*