CSR Readiness® Pro Edition

Frequently Asked Questions

June 2016

Confidential and Proprietary

CSR Readiness® Pro Edition
Frequently Asked Questions

READINESS PROGRAM TECHNICAL

SECURING PERSONAL DATA AND PREPARING FOR A BREACH ARE CRITICAL

DEFINITIONS

REQUIREMENTS TO PROTECT DATA

ABOUT CSR

TECHNICAL

How do I begin?

To begin, simply go to https://bio-haz.csrreadiness.com/ to register and create credentials to begin the process. You will have 24/7 access to your account.

I forgot my username

Your 'username' is the email address you registered with when signing up for Readiness. If you change your original registration email address using My Account in Readiness, this updated email address is your 'username'.

I forgot my password

To retrieve your password, you will need the email address you entered during registration or the updated email address you associated with your account using My Account in Readiness. Click on the Forgot Password link on the Log In screen. Enter in your email address and click the Email Link button. A reset password link will be sent to that email address. Click on that link to reset your password. If you do not receive that email or have any problems resetting your password, please contact **support@csrps.com** for further assistance.

I skipped some questions and want to go back to them, how do I do that?

To navigate back to questions previously skipped, you can use the Next and/or Back buttons located at the bottom of your questionnaire. You can also click on the Show Progress tab and click directly onto the domain of the question you would like to go back to. Before submitting your questionnaire, you will also be prompted to complete any required questions that have not been answered.

I don't know an answer to a question – can I just skip it?

You can skip questions and come back to them later. You will want to ensure all questions are answered prior to submitting your questionnaire, as not answering a question will affect your score, generate suggested remediation tasks and associated policy and procedure offerings.

How long will it take to complete this assessment?

It is estimated that it will take one hour to complete the assessment. The entire evaluation and remediation process may take longer should consultation or research be required to answer to some of the questions. Progress within the assessment is saved as questions are answered. You can leave the assessment and come back to it at a later time to finish. Your answers up to that point will be saved.

What is the ID Stay Safe seal?

This digital seal is a stamp that you can place on your website, which informs your customers, affiliates, potential clients, corporate insurers, etc., that your organization has performed a thorough self-assessment of your organization's processes to protect personally identifiable information, indicating that you have policies in place to maintain a high level of vigilance, audit, and association education with regards to the protection of personally identifiable information within your organization.

How do I put the completion seal on my website?

Once the self-assessment has been taken and the recommended remediation tasks have been completed, an email will be sent to the associated account's registered email address with the certification seal with instructions for its publication and directions to embed it on your web page. If there are any issues regarding the implementation of the completion seal, please contact **support@csrps.com** for further assistance.

SECURING PERSONAL DATA AND PREPARING FOR A BREACH ARE CRITICAL

What is CSR Readiness® Pro Edition?

The Readiness Pro Edition comprises the patent-pending risk assessment program CSR Readiness® and the *award winning* CSR Breach Reporting Service™.

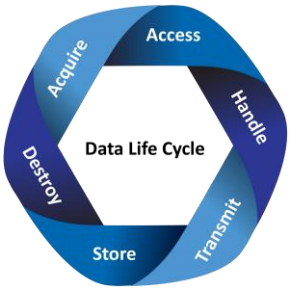
How does the CSR Readiness® Program work?

CSR Readiness® Program is an online self-assessment tool that helps you review, revise and revisit your business processes for handling the personally identifiable information (PII) of your customers, employees and vendors as required by a host of legislation and regulations.

CSR Readiness® 3 Step Process:

1) Review – Take a Self-Assessment Evaluation

- Detect location of personally identifiable information (PII) in an organization
- Determine how PII is:
  - ✓ Acquired
  - ✓ Accessed
  - ✓ Handled
  - ✓ Transmitted
  - ✓ Stored
  - ✓ Destroyed



2) Revise – Implement Readiness Policies and Remediation Instructions

- Remediate weaknesses and train employees on system-generated policies and procedures

3) Revisit – Continually Improve Risk Score

- Routinely monitor and audit performance to meet legal, regulatory and other compliance requirements

A dashboard will show progress and generate tasks to improve compliance. You can improve your business risk scores by remediation and implementation of further program offerings. Upon successful completion of the analysis and remediation, your business will earn a Certificate of Completion and the ID Stay Safe Digital Seal that you can use on your website and advertising.

What does the Certificate of Completion signify?

Once you have completed in the self-assessment evaluation and implemented the remediation tasks, you will be awarded the Certificate of Completion. This can be placed on your website and is valid for one year from date of issue. By annually revisiting your self-assessment, you can maintain this Certificate of Completion.

What does CSR Breach Reporting Service do for me?

In the event of the actual or suspected breach of PII, the CSR Breach Reporting Service reports to authorities and notifies consumers, as required.

Your call to the in-house CSR team of privacy professionals initiates a custom evaluation of your incident to determine if authorities and consumers must be notified. CSR files the necessary breach reports on your behalf, and consumer notification can be prepared with your input.

Why do businesses need this Pro Edition?

Various state, federal and international laws require businesses to protect the personally identifiable information of employees, vendors and customers. Penalties for noncompliance can include fines, prosecution and even jail time. Massachusetts and Connecticut are just two examples of many jurisdictions that require businesses that deal with their residents maintain comprehensive risk assessment, remediation and monitoring programs related to their handling of legally protected personal information, known as PII.

If organizations don't have this program, what could happen?

While it's impossible to completely avoid a breach due to uncontrollable circumstances, 97% could have been prevented. Accidents, errors and theft are just a few ways that information is compromised. Smart devices and wireless services compound the problem. Proactive detection and correction can go a long way to prevent loss and further fallout due to reputational damage, lost sales, fines, lawsuits and prosecution.

The Department of Homeland Security, the FTC, Visa and the BBB encourage businesses to protect consumer data and plan ahead to reduce risk. All states have laws that protect their residents who might be your customers, employees or vendors. Many laws specifically require creation and maintenance of information security programs. These laws include penalties for noncompliance.

For example, the civil penalty for violating the Connecticut Act No. 08-167, which requires the safeguarding of personal data, is $500 per violation, up to $500,000 for a single event.

Lost trust means lost sales. The fallout of data breaches has caused businesses to close their doors. According to Visa, businesses should "Consider a breach likely and plan accordingly."

Does Breach Reporting Service only cover items stored with Bio-Haz Solutions?

No, the Breach Reporting Service covers the location contracted with Bio-Haz Solutions and handles reporting and notification as needed for the breach of ALL PII data your business may have, whether it is stored in your office, an employee takes a file home, or your business laptop is stolen while you are away on vacation.

DEFINITIONS

What is personally identifiable information or PII?

The simple answer is that it's anything that can be used to identify you. The loss of this information leads to identity theft.

Types of personal information include: name, address, phone, email, birthdates, Social Security numbers, driver's license, bank account and credit card information. The list continues to grow with new and revised legislation and court rulings.

Other personal information includes health information, medical records, Vehicle Identification Numbers, license plate numbers, login credentials and passwords, school records as well as voice recognition files. Fingerprints, retina scans, and handprints are also considered personal information.

What is the difference between PCI and PII?

PCI data is just one type of personally identifiable information. The PCI Data Security Standard protects credit cardholder data such as debit or credit card number, expiration date and card security code.

What is a breach of personally identifiable information?

The unauthorized access, loss, use or disclosure of information by either accident or criminal intent which can identify an individual.

What is data breach reporting?
When a breach occurs, the clock starts ticking to comply with federal, state and other laws. Reporting involves the where, when and how of the incident.

What is consumer notification?
Almost every state has enacted a data breach notification statute. These laws generally require businesses that have personal information about residents within a state to notify those residents when that data is compromised.

Is this Insurance?
No. The CSR Breach Reporting Service reports to authorities and notifies consumers, as required In the event of the actual or suspected breach of PII.

What are some examples of a breach?
A breach can occur in many ways, including through lost laptops or smart phones, loss or improper disposal of paper records, intrusion into your network or PC by hackers and theft. The definition continues to expand.

REQUIREMENTS TO PROTECT DATA

Who do I need to report a breach to?
Who you need to report to in the event of a particular breach may depend on multiple factors including where you are located, what kind of PII was involved in the breach, and the location of the individuals that may have compromised PII. Over 100 countries have data protection laws, as well as 300+ federal, state and local authorities in the U.S. and Canada.

Does CSR determine whether a breach occurred?
No. Based upon our interview with you, our Privacy Professionals determine whether reporting to authorities or notification to consumers is necessary. If reporting is required, our Privacy Professionals will do so on your behalf. If consumer notification is necessary, we will work with you to do so.

What laws govern personally identifiable information?
Here are a few examples of the hundreds of laws and regulations that relate to the protection of personally identifiable information (PII) and requirements to report suspected or real loss.

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Drivers Privacy Protection Act (DPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI-DSS)
- Family Educational Rights and Privacy Act (FERPA)
- 47 state data breach laws
- Data security laws requiring comprehensive information security programs to safeguard personal information, i.e. Massachusetts' 201 CMR 17.00

Who are the enforcement agencies and others who might be involved after a breach?
Enforcement officials include various federal and state agencies as well as attorneys general, commissioners and others. Here are a few examples:

- Federal Trade Commission (FTC)

- Consumer Financial Protection Bureau (CFPB)
- Card brands like Visa, MasterCard, etc.
- State Attorneys General
- Federal Bureau of Investigation (FBI)
- US Secret Service
- Dept. of Health and Human Services/Office of Civil Rights

What if personally Identifiable information shared and/or received from another organization is compromised?

If your business is a third-party provider with personally identifiable information of customers, employees, or vendors of another business, then, depending upon circumstances, you very likely are required to protect that data.

What if personally Identifiable information under my care is encrypted, redacted, or masked?

Even if the material is encrypted, redacted or masked, various regulations still require your protection. For example, encryption keys must be secured.

How can I limit the threat of a data breach?

Almost everyone can do more to protect personally identifiable information. CSR Readiness® helps you assess your risk in handling PII, remediate your processes, implement policies, train staff and continue to monitor and audit, as required by laws and regulations.

ABOUT CSR

Who is CSR?

CSR Professional Services, Inc. is a leading provider of award-winning data life cycle management and expert services for businesses domestically and around the globe, including the patented, award-winning CSR Breach Reporting Service™.

CSR enables compliance with personally identifiable information requirements, while facilitating best practices to reduce the business risk and financial liability associated with the acquisition, handling, storage, sharing and disposal of data.

How many companies use this service?

Hundreds of thousands of businesses have enrolled in CSR data management and breach services.

Can you help me with other privacy services?

Other services include personally identifiable information business analysis, remediation, audit, forensic, education, certification, special projects and Stand-In Privacy Officer provision. For further information, email biohaz@ptd.net .

Can you send me some information?

Go to www.bio-haz.com to read more about protecting personal information.