USER GUIDE – REGISTRATION

PROVIDER RELIEF FUND REPORTING PORTAL

Date: June 30, 2023

Table of Contents

Tables of Figures

1 BACKGROUND INFORMATION, PURPOSE, AND GETTING STARTED

1.1 BACKGROUND INFORMATION

The Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136), the Paycheck Protection Program (PPP) and Health Care Enhancement Act (P.L. 116-139), and the Coronavirus Response and Relief Supplemental Appropriations (CRRSA) Act (Division M of P.L. 116-260), and American Rescue Plan Act of 2021 (P.L. 117-2) appropriated funds to reimburse eligible healthcare providers for healthcare-related expenses or lost revenues attributable to COVID-19. These funds were, or will be, distributed by the Health Resources and Services Administration (HRSA) through the Provider Relief Fund (PRF) program. Recipients of these funds agreed to Terms and Conditions, which require compliance with reporting requirements as specified by the Secretary of Health and Human Services (HHS)in program instructions.

1.2 PURPOSE

HRSA developed the PRF Reporting Portal to enable PRF and American Rescue Plan (ARP) Rural[1] (referred to as "reporting entities" throughout this document) to comply with mandatory reporting requirements. Reporting entities must complete a two-step process in the PRF Reporting Portal (also referred to as "the portal" throughout this document) in order to submit their reports to HRSA. In order to complete the two-step process, reporting entities must 1) register as users and 2) complete reporting on the use of funds. The purpose of the ***PRF Reporting Portal User Guide – Registration*** is to assist reporting entities in the completion of the first step of the process. Reporting entities will be notified when they should complete the second step of the process and report on the use of funds.

1.3 POST-PAYMENT REPORTING REQUIREMENTS

Reporting entities should review the most recently published *Post-Payment Notice of Reporting Requirements* available on the PRF Reporting Requirements & Auditing website for information about reporting requirements. Recipients who received one or more General and Targeted Distributions, which includes the Nursing Home Infection Control (NHIC) Distribution[2] (formally known as the Skilled Nursing Facility and Nursing Home Infection Control Distribution), and/or ARP Rural Distribution payments exceeding $10,000 in the aggregate during a Payment Received Period are required to report in each applicable Reporting Time Period as shown in *Table 1 Reporting Periods.* **Reporting must be completed and submitted**

---

[1] Previous documentation did not include information regarding the ARP Rural Distribution payment(s). ARP Rural payments are funded separately from the PRF General and Target Distribution payments.
[2] The NHIC Distribution is a Targeted Distribution payment. The Distribution includes payments made in August 2020 and Nursing Home Quality Incentive Payment Program (QIP) payments.

to HRSA by 11:59 PM Eastern Time on the last date of the Reporting Time Period. Only electronic submissions through the PRF Reporting Portal are permitted.

Reporting entities that do not report within the respective Reporting Time Period are out of compliance with payment Terms and Conditions and may be subject to repayment and/or debt collection.

If a reporting entity received payments meeting the established monetary threshold during multiple Payment Received Periods, the recipient is required to report during each of the corresponding Reporting Time Periods as shown below.

Period	Payment Received Period	Period of Availability for Eligible Expenses	Period of Availability for Lost Revenues	Reporting Time Period
1	April 10, 2020, to June 30, 2020	January 1, 2020, to June 30, 2021	January 1, 2020, to June 30, 2021	July 1, 2021, to September 30, 2021
2	July 1, 2020, to December 31, 2020	January 1, 2020, to December 31, 2021	January 1, 2020, to December 31, 2021	January 1, 2022, to March 31, 2022
3	January 1, 2021, to June 30, 2021	January 1, 2020, to June 30, 2022	January 1, 2020, to June 30, 2022	July 1, 2022, to September 30, 2022
4	July 1, 2021, to December 31, 2021	January 1, 2020, to December 31, 2022	January 1, 2020, to December 31, 2022	January 1, 2023, to March 31, 2023
5	January 1, 2022, to June 30, 2022	January 1, 2020, to June 30, 2023	January 1, 2020, to June 30, 2023	July 1, 2023, to September 30, 2023
6	July 1, 2022, to December 31, 2022	January 1, 2020, to December 31, 2023	January 1, 2020, to June 30, 2023	January 1, 2024, to March 31, 2024
7	January 1, 2023, to June 30, 2023	January 1, 2020, to June 30, 2024	January 1, 2020, to June 30, 2023	July 1, 2024, to September 30, 2024
8	July 1, 2023, to December 31, 2023	January 1, 2020, to December 31, 2024	January 1, 2020, to June 30, 2023	January 1, 2025, to March 31, 2025
9	January 1, 2024, to June 30, 2024	January 1, 2020, to June 30, 2025	January 1, 2020, to June 30, 2023	July 1, 2025, to September 30, 2025

Grace period ended November 30, 2021

Table 1 Reporting Periods

1.4   RESPONSIBILITY FOR REPORTING

Reporting entities will complete and submit required reports for PRF and ARP Rural payments in the PRF Reporting Portal. The reporting entity may differ by type of payment, but generally HRSA defines this as the entity that registers its Tax Identification Number (TIN) and reports on payments received by that TIN and/or its subsidiary TINs.

A TIN is either an Employer Identification Number (EIN) or Social Security Number (SSN) and must be entered in nine-digit format with no special characters.

- A parent entity may report on its subsidiaries' General Distribution payments, regardless of whether the subsidiary TINs received the General Distribution payments directly from HRSA or whether General Distribution payments were transferred to them by the parent entity.

- The parent entity may report on these General Distribution payments regardless of whether the parent or the subsidiary attested to the Terms and Conditions.
- The original recipient of a Targeted Distribution payment is always the reporting entity in accordance with the CRRSA Act.
- A parent entity may not report on its subsidiaries' Targeted Distribution. The TIN that qualified for Targeted Distribution payments must report on the use of funds in accordance with the CRRSA Act. This is required regardless of whether the qualifying recipient or its parent subsequently transferred the payment. A reporting entity that is a subsidiary must indicate the payment amount of any of the Targeted Distributions it received that were transferred to/by the parent entity, if applicable.
- For ARP Rural payment recipients, regardless of whether or not a parent was obligated to distribute payments to its subsidiaries who qualified for ARP Rural payments, HRSA requires parent entities to report on ARP Rural payments they received from the agency.

1.5   BEFORE STARTING

Reporting entities must complete registration before beginning to report on the use of funds. A reporting TIN submitting reports in multiple reporting periods will only need to register once. Users will need approximately 20 minutes to complete the registration process. **The registration process must be completed in one session as it is not possible to save partially entered information.** Upon successful registration and at the end of the reporting process, portal users will receive an email notification from 'PRFReporting-NoReply@hrsa.gov.' Portal users should add this email address to their safe sender list before beginning. For instructions on adding 'PRFReporting-NoReply@hrsa.gov' as a safe email sender, users should follow the instructions of the email provider associated with the email account. As an example, instructions for Outlook users may be found at https://support.microsoft.com/en-us/office/block-or-allow-junk-email-settings-48c9f6f7-2309-4f95-9a4d-de987e880e46#bkmk_safesenders. Please note that the 'PRFReporting-NoReply@hrsa.gov' account is not monitored and should not be used to communicate with HRSA staff.

Reporting entities should ensure they have all of the information required to register available before they begin. Information required to register:

1. Tax Identification Number (TIN) or other number submitted during the application process [*e.g.,* Social Security Number (SSN), Employer Identification Number (EIN)]. The TIN may be the TIN of a parent entity if a parent is reporting on behalf of subsidiaries.
2. Business name (as it appears on the IRS Form W-9 of the reporting entity).
3. Contact information (First Name, Last Name, Phone number, Title[3], Mobile Number[4], Email[5], Username) of the person responsible for submitting the report. A username and password will be associated when initiating two-factor authentication preferences.

---

[3] Not a required data field.

[4] Mobile Number can be used if SMS is selected for two-factor authentication preference.

[5] Email Address can be used if Email is selected for two-factor authentication preference.

4. Address as it appears on the IRS Form W-9 (Street 1, Street 2, City, State, five-digit ZIP code) of the reporting entity.
5. TIN(s) of subsidiaries (if a reporting entity is reporting on behalf of subsidiary(ies), a list delimited by commas, *e.g.,*123456789,987654321,135791357).
6. Provider Relief Fund payment information (for any one of the payments received).
   - TIN of entity that received the payment. **The TIN must be a TIN that received a PRF and/or ARP Rural payment as it will be validated during the registration process.**
   - Mode of payment (check or direct deposit Automated Clearing House [ACH]) if Check is selected, Check Number is displayed. If Direct Deposit(ACH) is selected Settlement Date (ACH) is displayed.
   - Payment amount.

1.6   GETTING STARTED

The PRF Reporting Portal is only compatible with the most current version of Microsoft Edge, Google Chrome, and Mozilla Firefox.

Links to key PRF resources are available to reporting entities on the home screen and within the portal. They may be accessed on the home screen before beginning registration or by clicking on the blue 'Resources & FAQs' button in the upper right corner of the screen of the portal. Clicking the 'Resources & FAQs' button will open a new browser tab as shown in *Figure 1 Resources and Help Screen* which will avoid exiting the registration process early and inadvertently losing data already entered.

Figure 1 Resources and Help Screen

If at any point the user would like to exit the PRF Reporting Portal, they can click on the blue 'Return to Home' button in the upper left corner of any of the registration screens. If this button is clicked, the user will be prompted with a message informing them that all data entered will be lost and the user will be redirected to the home screen. *Figure 2 Return to Home Screen* displays both the 'Return to Home' button and the pop-up message that confirms that the user would like to return to home and lose all data previously entered.
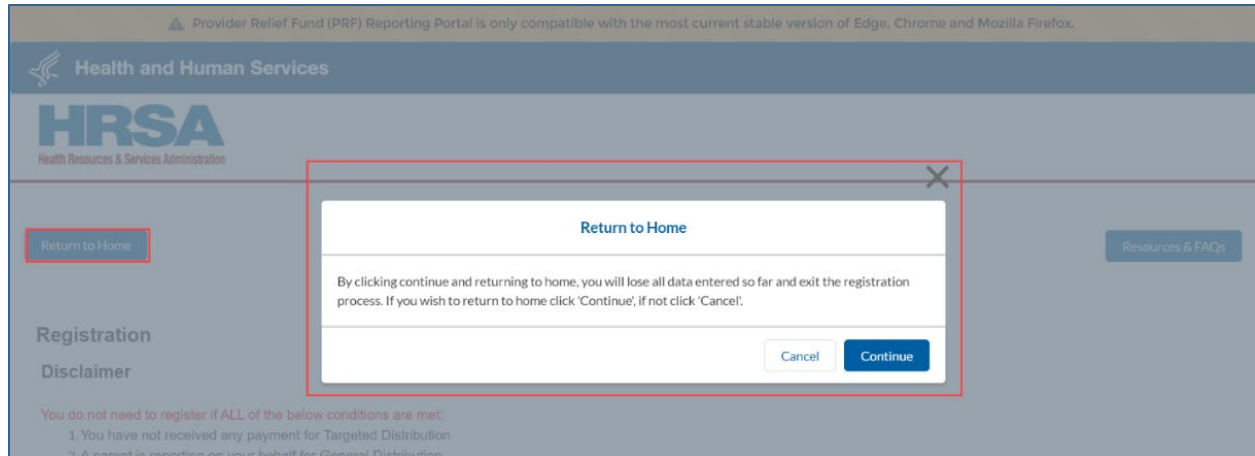
Figure 2 Return to Home Screen

In addition to this ***PRF Reporting Portal User Guide – Registration***, reporting entities should reference the following key PRF resources during the registration process:

- [PRF Frequently Asked Questions (FAQs)](#)
- [PRF Reporting and Auditing Requirements](#)
- [PRF Terms and Conditions](#)
- [PRF General Information](#)
- [Reporting Resources](#)

Information entered by portal users will not be saved until the registration is submitted successfully. **A user's registration session in the PRF Reporting Portal will timeout after 15 minutes of inactivity and information entered will be lost upon timeout.**

2 PRF REPORTING PORTAL HOME SCREEN

The PRF Reporting Portal home screen allows reporting entities to create an account, access key resources, and login to submit a report on the use of funds.

2.1 HOW TO ACCESS

The PRF Reporting Portal can be accessed at *https://prfreporting.hrsa.gov*. The PRF Reporting Portal is only compatible with the most current version of Microsoft Edge, Google Chrome, and Mozilla Firefox.

2.2 GENERAL LAYOUT

A screenshot of the PRF Reporting Portal home screen is shown in *Figure 3 PRF Reporting Portal Home Screen*. Important elements have been marked and defined below.

1. **Log In Fields**: Reporting entities that are already registered as PRF Reporting Portal users can enter the portal by clicking on the 'Log In' button displayed under the 'Already a registered PRF Reporting Portal User?' heading. After clicking the 'Log In' button, reporting entities will be prompted to enter the username created during the registration process, check the 'I'm not a robot' box, and click the 'Continue to Log In' button. Users that do not remember their password can reset their password using the 'Forgot Password?' link on the TIN and password screen. Clicking this link will redirect the user to a screen called 'Password Reset' where the username associated with their portal account and TIN is required to reset the password. On the next screen, the user will accept the HRSA Terms and Conditions, then click Next.
    a. If the user has not already done so, they will be taken to a screen where they can set their two-factor authentication preference.
    b. If the user has already selected their two-factor authentication preference, a verification code will be sent to the selected preference. (Submission of a valid verification code is required prior to gaining access to the PRF Reporting Portal.)

2. **Portal Registration:** PRF Reporting Portal user registration is the first step in the reporting process. To begin registration, portal users should click the blue 'Register' button below the heading, 'First Time User? Click on 'Register' to create an account.'

3. **Resources:** Portal users are able to access important PRF resources on the home screen. These resources can also be accessed using the blue 'Resources & FAQs' button (upper right corner) available throughout the portal. Clicking the 'Resources & FAQs' button will open a new browser tab which will not effect previously entered data.

4. **Technical Questions and Language Assistance:** For technical questions regarding the use of the portal or questions regarding reporting that cannot be answered by this user guide or other available resources, portal users should contact the Provider Support Line. Provider Support Line contact information and hours of operation are found in the footer of the Reporting Portal Home Page and all subsequent pages. The footer also has other web links to standard government websites and language assistance.

Figure 3 PRF Reporting Portal Home Screen

2.3 HOW TO REGISTER

To begin registration, portal users should navigate to the **PRF Reporting Portal**, then click the blue 'Register' button below 'First Time User? Click on 'Register' to create an account.' This

step is labeled as '2' in *Figure 3 PRF Reporting Portal Home Screen*. This action will take portal users through the steps necessary to complete registration in the portal.

Portal users should expect the registration process to take approximately 20 minutes. **The registration process must be completed in one session as it is not possible to save a partially completed registration.** A detailed list of all information required to complete the registration process can be found in Section *1.5 Before Starting*. For step-by-step instructions of the registration process, reporting entities should reference *Section 3 Registration Process*.

Note: Reporting entities are not required to delete unused portal accounts.

Reporting entities may contact the Provider Support Line at (866) 569-3522; for TTY dial 711 if they have registration questions. Hours of operation are 8 a.m. to 8 p.m. Central Time, Monday through Friday. Hours are subject to change.

3   REGISTRATION PROCESS

Registration is the first of a two-step process required for reporting entities to report on the use of PRF payments. All reporting entities must register as PRF Reporting Portal users before they can complete the reporting requirements. A one-time registration covers all reporting periods. This section of the registration user manual describes the steps involved to complete the registration process after portal users click the 'Register' button on the PRF Reporting Portal home screen.

3.1   TERMS AND CONDITIONS

Terms and conditions related to the use of the PRF Reporting Portal are visible after portal users click the 'Register' button on the PRF Reporting Portal home screen.

All portal users must certify that they have read and accepted the terms and conditions related to the use of the portal before proceeding to the next step. Once portal users accept the terms and conditions, they should click on the radio button as shown in (button is boxed in red), *Figure 4 Terms and Conditions Screen* and then click the 'Next' button that will appear after the radio button is selected.

Figure 4 Terms and Conditions Screen

3.2   STEP 1 – PROVIDER IDENTITY INFORMATION

The first step of the registration process is shown in *Figure 5 Provider Identity Information Screen.* This step requires that reporting entities share identifying information including the TIN (or other number submitted during the application process [*e.g.,* Social Security Number (SSN), Employer Identification Number (EIN)]), business name (as it appears on IRS Form W-9), contact information, and address (as it appears on an IRS Form W-9). **It is very important to enter the TIN correctly as a reporting entity will only be able to register a primary TIN one time.** The TIN entered here may be the TIN of a parent entity that is submitting a consolidated report on behalf of its subsidiaries.

The contact email address must be a valid, monitored email address. The contact email address associated with each PRF Reporting Portal account will be used for any PRF communications that are necessary in the future, including but not limited to questions about the reporting entity's registration, updates on the reporting portal, and questions about the reporting entity's report on the use of funds. If one individual is responsible for registering and submitting reports for multiple entities, the same **contact** email address may be used. A confirmation email message will be sent to the email address reported on this screen when registration is successfully completed.

The contact email address and username do not need to be the same, but they can be. The username must be in the form of an email address and the username created must be unique for each non-consolidated report being submitted, even if the **contact** email address is the same for each entity. *Please confirm the exact username (including the spelling) as this cannot be changed once submitted.* The username will be used to log into the PRF Reporting Portal, along with the TIN and password. Communications will be directed to the **contact** email address, not the username. For two-factor authenication preferences, the portal user will be able to select either the mobile number or the email address entered in this page.

Portal users should choose from a drop-down list in the 'State' field. The 'State' field defaults to 'Alabama' and must be corrected before the user proceeds to the next screen.

Portal users must enter all of the required information (marked by a red asterisk[*]) and click 'Next' at the bottom of the screen. Users should hover or click on the tooltip icon (🛈) to see additional details about data entry fields. For some data entry fields, users are required to enter information in a particular format or style. For example, the phone number must consist of only ten digits and no special characters, such as brackets and dashes ('(', ')', '-'); the username must be in the form of an email address and is not case sensitive (i.e., AbC123@xyz.org); the ZIP code must be five digits. After portal users have completed all of the required data entry fields without errors, they will be allowed to advance to the next screen.

Note: *Save the username, TIN, and password somewhere secure outside of the portal as you will need this information to log into the portal for reporting purposes at a later date.*

Figure 5 Provider Identity Information Screen

If the user has not completed a required field, an error message in red will appear below the required data entry fields as shown in *Figure 6 Provider Identity Information – Required Field Error.* **The user will not be able to proceed to the next screen until all required fields have been completed without errors.**

Figure 6 Provider Identity Information – Required Field Error

If a user enters a TIN that has already been registered and tries to proceed to the next step of Registration, they will be directed to a screen with an error message as shown in *Figure 7 Provider Identity Information – Duplicate Primary TIN Error*. If the portal shows this error and the reporting entity has not registered this TIN before, the user should either click the 'Previous' button and correct the TIN or call the Provider Support Line for assistance if they think the TIN they entered is correct.
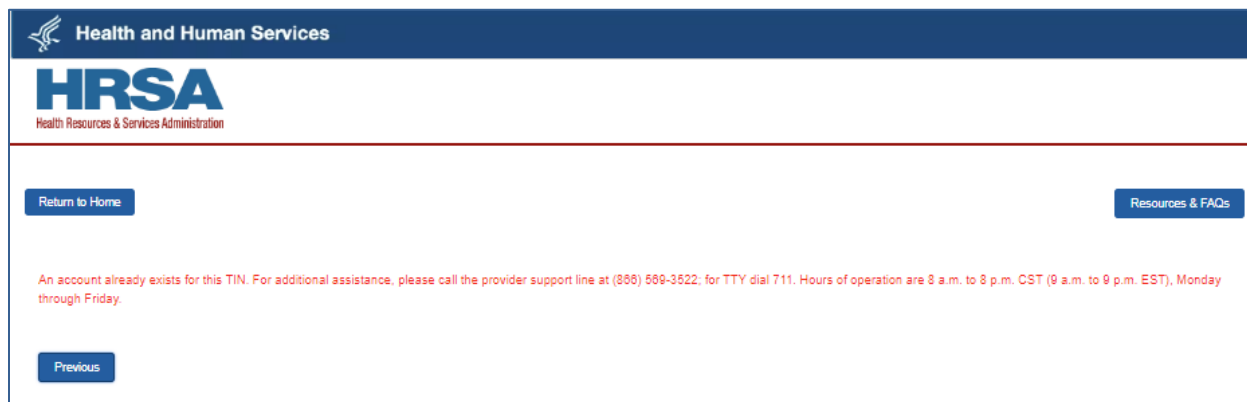
Figure 7 Provider Identity Information – Duplicate Primary TIN Error

Note: In rare circumstances, two reporting entities share a TIN. In these cases, the EIN of a recipient matches the SSN of a second recipient. In these cases, the user should call the Provider Support line.

3.3   STEP 2 – SUBSIDIARY INFORMATION

After completing the Provider Identity Information screen, the portal user is taken to the Subsidiary Information screen as shown below in *Figure 8 Provider Identity Information – Subsidiary Information*. Here, the reporting entity will be required to provide a 'Yes' or 'No' response to 'Will you report on behalf of subsidiaries that received a **General Distribution** payment?' as shown in the image. It is very important that reporting entities answer this question correctly, as the answer to this question will affect the data entry on the following screen. Portal users should click on the tooltip to see the help text. If users respond 'Yes' to this question, they will be required to enter all of the subsidiary TINs on whose behalf they will be reporting on the next screen.

Figure 8 Provider Identity Information – Subsidiary Information

If the user does not respond to the question, the reporting entity will be directed to the error message page as shown in *Figure 9 Subsidiary Information Questionnaire - Required Field Error*. The user should click the 'Previous' button to go back and respond to the question as either 'Yes' or 'No' to be able to continue with the registration.

Figure 9 Subsidiary Information Questionnaire - Required Field Error

3.4   STEP 3 – SUBSIDIARY/PAYMENT INFORMATION

After completing the Subsidiary Information screen, the portal user is taken to the Subsidiary/Payment Information screen. Reporting entities will be presented with a screen based upon the responses in *Step 2 – Subsidiary Information*.

Reporting entities that respond 'No' to 'Will you report on behalf of subsidiaries that received a **General Distribution** payment?' on the previous screen will be prompted to complete payment information as shown in *Figure 10 Payment Section with No Subsidiaries*. Portal users must enter all data fields accurately. If any of the payment information entered is incorrect, a reporting entity will not be able to proceed to the next step in the registration process.

Reporting entities that respond, 'Yes' to 'Will you report on behalf of subsidiaries that received a **General Distribution** payment?' on the previous screen will be prompted to complete a subsidiary TIN(s) field and payment information as shown in *Figure 11 Payment Section with Subsidiaries.* Reporting entities must provide a comma-delimited list of all subsidiary TINs on whose behalf they intend to report for one or more payments (*e.g.,* 123456789,987654321, 135791357). The subsidiary TIN information will not be validated upon submission, so it is important that portal users enter this information accurately. **Do not re-enter the TIN being registered as a subsidiary or parent of themselves or an error message will appear.** Reporting entities will be able to review, edit, and validate all of the subsidiary TINs as part of the reporting process. Portal users must then enter accurate payment information for *any one* of the payments they or a subsidiary listed received. If any of the payment information entered is incorrect, a reporting entity will not be able to proceed to the next step in the registration process.

Figure 10 Payment Section with No Subsidiaries

Figure 11 Payment Section with Subsidiaries

If a user clicks 'Next' without providing information in a required field, an error message will appear in red below the required data entry fields as shown in *Figure 12 Payment Section with No Subsidiaries - Required Field Error* and *Figure 13 Payment Section with Subsidiaries - Required Field Error*. Portal users will not be able to proceed to the next screen until all required fields have been completed.

On the payment information screen, reporting entities must enter information for *any one* of the payments made to their TIN or any of the subsidiary TIN(s) on whose behalf they are reporting. The payment information submitted during registration is used for identity verification purposes. Users must choose a 'Mode of Payment' ('Direct Deposit ACH' or 'Check') from a drop-down list. If 'Direct Deposit ACH' is selected, a 'Settlement Date (ACH)' is required. The settlement date (ACH) is the date the PRF payments were electronically deposited into the recipient's bank account. This date usually excludes weekends and federal holidays. The date must be formatted as MMM DD, YYYY (*e.g.,* Sep 1, 2020). Portal users may alternatively select the calendar icon in the data entry field and click on the accurate date in the calendar. If 'Check' is selected as the 'Mode of Payment,' a 'Check Number' data entry field will become visible and the user must complete this data entry field accurately. Again, portal users must enter all payment information accurately. **If any of the payment information entered is incorrect, a reporting entity will not be able to proceed to the next step in the registration process.**

Figure 12 Payment Section with No Subsidiaries - Required Field Error

Figure 13 Payment Section with Subsidiaries - Required Field Error

If a portal user does not enter payment information for the TIN provided in *Step 1- Provider Identity Information* or one of the Subsidiary TINs provided in the 'TIN(s) of Subsidiaries' data entry field in *Step 3 – Subsidiary/Payment Information*, and clicks 'Next,' an error message will appear as shown in *Figure 15 Incorrect Payment TIN*. If a user receives this error message, they should click the 'Previous' button and ensure they are entering payment information associated with one of the already reported TINs.

If a user enters their own TIN as a subsidiary, the system will provide an error, as shown in *Figure 14 Subsidiary TIN Cannot be That of Parent*.

Figure 14 Subsidiary TIN Cannot be That of Parent

Figure 15 Incorrect Payment TIN

If the portal user does not enter accurate payment information or the payment information is not able to be validated, an error message will appear as shown in *Figure 16 Incorrect Payment Information Error*. The user should click the 'Previous' button to go back to Step 3 and ensure that all information was entered correctly. If the payment entered was made within the last five business days, the portal may not be able to validate the payment. Reporting entities should use alternate payment information if available or return five business days after the payment date to register.

If the portal user continues to have difficulty entering information they believe to be valid, they should contact the Provider Support Line at (866) 569-3522; for TTY, dial 711.

Figure 16 Incorrect Payment Information Error

3.5   STEP 4 – PROFILE SUBMISSION

Reporting entities that successfully complete *Step 3 - Subsidiary/Payment Information*, will be directed to the final registration screen as shown in *Figure 17 Profile Submission Screen.* At this time, portal users will be able to review all of the data entered throughout the registration process for accuracy.

Once a portal user has reviewed the summary data, including TIN, username, and contact email address, they must respond to the question at the bottom of the screen 'Do you certify that the above information is accurate to the best of your knowledge?' by using the drop-down menu.

If a reporting entity certifies that the data is accurate by selecting 'Yes,' a new section will appear below the certification that directs the portal user to 'Create a Username and Password.' The username will be prepopulated with the username selected in *Step 1 – Provider Identity Information*. The only way to change the username is to go back to *Step 1 – Provider Identity Information.* Reporting entities are unable to change the username associated with a PRF Reporting Portal account once the registration is submitted and the account is successfully created.

Portal users must select a password that complies with the password policy indicated in *Figure 17 Profile Submission Screen.* Passwords must:
- o Be a minimum length of fifteen (15) characters.
- o Contain at least three of four character types: uppercase, lowercase, numbers, or special characters.
- o Not be the same as the username or any part of the contact name provided in Step 1.
- o Not contain any variation of the word 'password'.

Reporting entities should print the information on this page from the browser and save it in a secure location. Portal users must click the 'Submit' button before exiting the portal.

Figure 17 Profile Submission Screen

If a portal user certifies that the data is not accurate by selecting 'No' to the question 'Do you certify that the above information is accurate to the best of your knowledge?,' an error message will appear in red, as shown in *Figure 18 Incorrect Information Screen*, and the user must use the 'Previous' button to go back to correct the inaccurate data. Data entered will not be lost unless the user returns to the PRF Reporting Portal Home Page. The reporting entity must certify to the accuracy of the information entered in order to successfully complete registration.

Figure 18 Incorrect Information Screen

If a portal user does not provide a compliant password, an error message will appear, outlined in red in *Figure 19 Non-Compliant Password*.

Please confirm the exact username (including spelling) as this cannot be changed once submitted. The username, TIN, and password will be used to log into the PRF Reporting Portal in conjunction with two-factor authentication. Please save this information in a secure location outside of the portal for future reference.

Create a Username and Password

*Username

> youruserid@domain.com

Password Policy
- Password must be of a minimum length of fifteen (15) characters.
- Password must contain at least three of these four character types:
  Uppercase, Lowercase, Numbers, or Special Characters.
- Use a "pass phrase" to help you create a complex password.
- Do not use your username or any part of your full name.
- Do not reuse your last twenty four (24) passwords.
- Password must not contain the word "password".

*Password

*Confirm Password

Please enter a valid password. This field is required.

Figure 19 Non-Compliant Password

3.5.1 Setting Up Security Questions

Cybercrime has been an increasingly severe problem in recent years. As a result, the Provider Relief Fund (PRF) has added a new security feature to the PRF Reporting Portal to comply with the HRSA Office of Information Technology security standards to improve account security. Upon logging in, the system will allow you to set up security questions on the PRF Reporting Portal as shown in *Figure 20 Setting Up Security Questions*, providing your account information with an extra layer of security.

Set Up Security Questions for Your PRF Reporting Portal Account Login

- The answers to your security questions must contain letters or numbers and cannot be less than 3 characters.
- The answers to your security questions cannot be longer than 30 characters.
- The same question and/or answer cannot be used multiple times.
- Answers are not case sensitive.
- Cannot repeat the same character more than twice in succession (e.g., RRR, 111).
- The following special characters are allowed, as long as they follow a letter or number: apostrophe ('), hyphen (-), spaces, period (.). (This means that your answers cannot start with one of these characters.)

* Question 1:
In what city did you meet your first spouse/partner?

* Answer 1:
'Security Answer 1

* Question 2
In what city did your parents meet?

* Answer 2:
-Security Answer 2

* Question 3:
In what city does your nearest sibling live?

* Answer 3:
.Security Answer 1

* Question 4:
In what city was your father born?

* Answer 4:
Security Answer 2

* Question 5:
In what city was your first job?

* Answer 5:
Security Answer 3

Figure 20 Setting Up Security Questions

You will be required to select 5 security questions/answers. Please follow the following rules for setting up your security questions/answers:

- The answers to your security questions must contain letters or numbers and cannot be less than 3 characters.
- The answers to your security questions cannot be longer than 30 characters.
- The same question and/or answer cannot be used multiple times.
- Answers are not case sensitive.
- Cannot repeat the same character more than twice in succession (e.g., RRR, 111).
- The following special characters are allowed, as long as they follow a letter or number: apostrophe ('), hyphen (-), spaces, period (.). (This means that your answers cannot start with one of these characters).

If you want to check the answer you have entered for one of the security questions, click the *Show* icon as shown in *Figure 21 Errors While Setting Up Security Questions*.

If you do not follow all rules while creating your security questions/answers, you will receive error(s) as shown in *Figure 21 Errors While Setting Up Security Questions*.

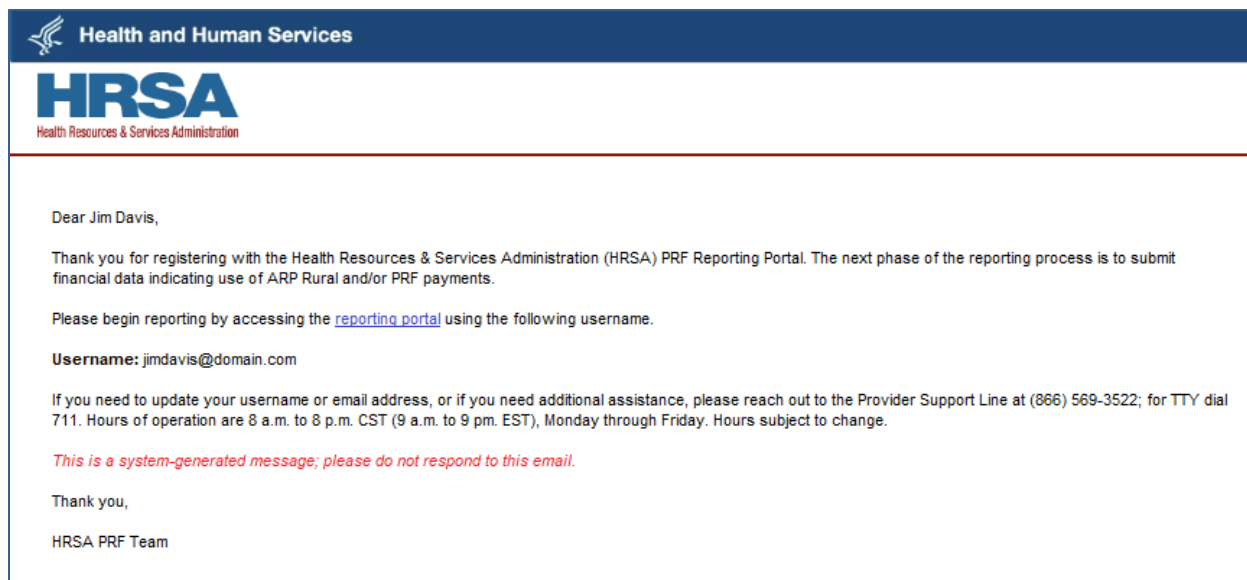*Figure 21 Errors While Setting Up Security Questions*

Registration is complete after a portal user certifies the accuracy of the information, enters a password that passes the validation, sets up their security questions successfully and clicks the 'Submit' button. Portal users that successfully register will see a pop-up message with the words 'Registration Successful!' as shown in *Figure 22 Successful Registration Screen*. Portal users that do not see this message may have blocked pop-ups on their computers. Portal users that register successfully will also receive an email from 'PRFReporting-NoReply@hrsa.gov' confirming the registration as shown in *Figure 23 Successful Registration Email.* Portal users should make sure to check their junk mail folder or spam folder if they do not receive the message. The email address 'PRFReporting-NoReply@hrsa.gov' should also be added to the email sender safe list. Please note that this mailbox is not monitored and should not be used to communicate with HRSA staff.

Figure 22 Successful Registration Screen

Figure 23 Successful Registration Email

Once registration is completed for a primary TIN, the reporting entity will not be able to re-access the registration data and make changes until reporting.

A reporting entity must keep the contact email address and phone number(s) associated with their account up-to-date because it will be used for communication by HRSA and for two-factor authentication. Registration is completed one time to cover all reporting periods.

Portal users responsible for submission of reports for multiple entity organizations that are not reporting on a consolidated basis must create a new PRF Reporting Portal account for each of the entity organizations for which they are reporting.

3.6   STEP 5 – SET UP TWO-FACTOR AUTHENTICATION PREFERENCE

The PRF Reporting Portal has enhanced the portal security by integrating two-factor authentication (2FA). If you have not configured the 2FA preference, the portal login process will require the user to set up 2FA preference once registration is complete. Upon successful registration, the system will take you to *Figure 24 Set Your Two-Factor Authentication Preferences.*

3.6.1 Preference: Email

By default, the 2FA authentication preference is set to email. The email address is read-only and is pulled from the user profile. (The Reporting Portal preferred verification method is email.)

Figure 24 Set Your Two-Factor Authentication Preferences

3.6.2 Preference: SMS

If the user is unable to receive email from the PRF Reporting Portal, the user may select to receive the 2FA verification code through SMS on a mobile device. To receive the verification code via SMS, please click on the SMS radio button and, if the correct mobile number is not reflected in the Mobile Number field, click on the "Update Mobile Number" hyperlink below it.

Figure 25 Set SMS as Preferred 2FA Method

The "Mobile Number" field will be enabled allowing the user to enter the mobile phone number to be used for 2FA verification.

- The 2FA mobile phone number is not used for PRF communications.
- Entering an SMS-enabled mobile phone number will not update the contact phone number in the "entity Overview" page.

Once the user has entered an SMS-capable mobile phone number, click on the "Send Code" button. An email will be sent verifying a new verification method was added to the PRF Reporting Portal user account. The user will receive the verification code on the mobile phone. The user must enter the code in the "Verification Code" field and then click the "Submit" button.
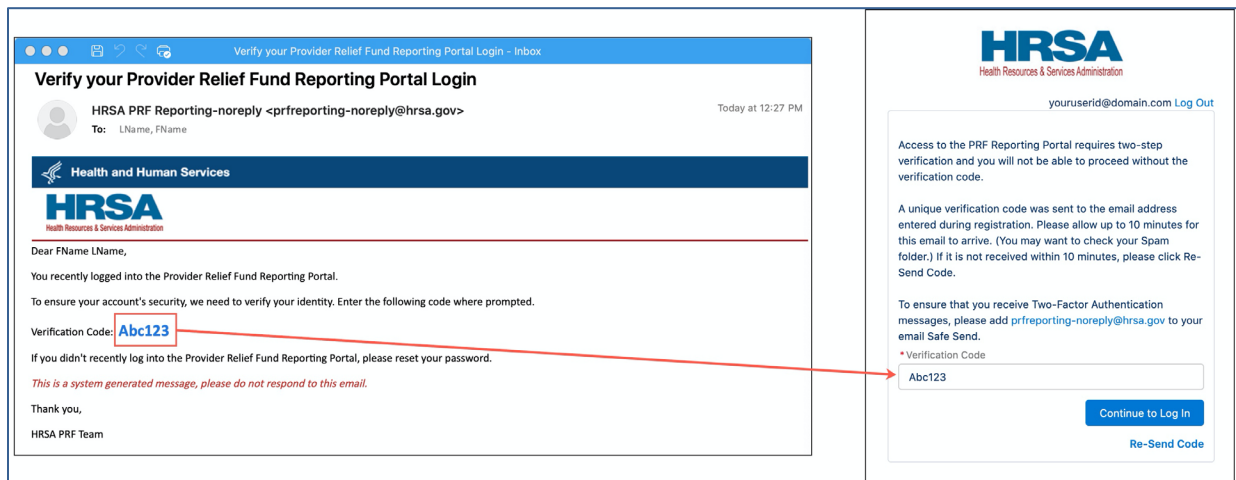

Figure 26 Enter Verification Code

3.6.3 Logging in Using 2FA

After setting up your 2FA preference, the system will require you to log in using 2FA.

Upon successful validation of the username and password, a 2FA verification code will be sent using the selected preference.

- If you selected Email as the preferred 2FA method, the verification code will be emailed to the email address in your PRF Reporting Portal Contact profile. (The email may take up to ten minutes to be received.)
- If you selected SMS as the preferred 2FA method, the verification code will be sent to your mobile number.

Once received, please enter the verification code in the "Verification Code" field and click the "Continue to Log In" button.

Figure 27 Verification Code

To receive a new verification code, click on the "Re-Send Code" hyperlink. A new verification code will be delivered to the preferred 2FA option. The 2FA verification code entry page will reload and display a warning message. Within a single login attempt, users are allowed to request re-sending three verification codes before the account is locked. If the account is locked, the user will have to wait 15 minutes before requesting another verification code.

Upon successful validation of the 2FA verification code, you will be taken to the PRF Reporting Portal landing page.

Figure 28 Re-Send Verification Code