The information provided in this presentation is intended only as a general informal summary. It is not intended to take the place of the statutes, regulations, and formal policy guidance that it is based upon. This presentation summarizes current policy and operations as of the date it was presented. Links to certain source documents have been provided for your reference. We encourage audience members to refer to the applicable statutes, regulations, and other interpretive materials for complete and current information about the requirements that apply to them.

RDS Secure Website Modernization Webinar and Feedback Session

November 14, 2018

- You can listen to the event using your computer speakers or headphones. Please ensure your computer speakers are not muted and the volume is turned up.
- Remember to turn off your pop-up blockers so you can participate in our feedback opportunities. Participants will answer poll questions throughout the presentation and be able to ask questions via WebEx Q&A.

Agenda

- RDS Secure Website Modernization
- RDS Secure Website Data Archival
- Implementing Multi-Factor Authentication (MFA) and the impact to RDS Secure Website users
- RDS Program Reminders
- Open forum Q&A

RDS Secure Website Modernization

- CMS' RDS Center is modernizing the RDS Secure Website interface with an estimated implementation throughout 2019
  - New design
  - Modified screen flows for all sections of the application
- New and improved functionality
  - Modification to Support Request feature to include on-screen suggested resolutions based on Topic and Category
    - Technical Support "Knowledge Base"
    - Submit a Support Request if the suggested resolution is not applicable
  - Multi-Factor Authentication will be required for all user accounts in the RDS Secure Website, per CMS' increased security requirements
- Data archival for applications that are no longer eligible for Appeal
- Updated educational materials including user guide documentation and on-demand training videos

RDS Secure Website Data Archival

CMS' RDS Center is considering archiving RDS Secure Website applications that meet the following criteria:

- The most recent post-reconciliation determination is greater than 4 years old
- Applications that are no longer eligible for appeal will be archived

Important to note:

- Archived applications will not be visible on the RDS Secure Website
- If data from an archived application is needed, it can be requested by sending a request to CMS' RDS Center

Benefits:

- Pages such as the Application List page will be greatly simplified by displaying only applications whose post-reconciliation determination is within the last 4 years
- Lower data volumes being retrieved by the RDS Secure Website will quicken response times

What is Multi-Factor Authentication (MFA)?

- MFA is a security architecture which requires more than one method of authentication derived from independent sources
  - MFA adds a level of security by requiring something the user knows (password) and something the user has (randomly generated token)
  - MFA has become an industry standard for websites containing sensitive information, Personal Health Information (PHI), and/or Personally Identifiable Information (PII)

- Examples:
  - User logs into their bank account online with username and password then enters an additional token code that is sent to them via email or text message
  - User logs into a computer or application with username and password then enters an additional token generated by an application such as Google Authenticator

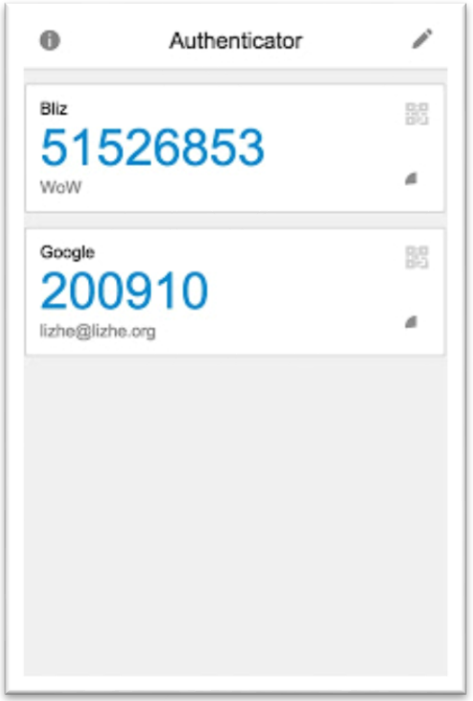
MFA Impact to RDS Secure Website Users

- All RDS Secure Website users will be required to activate MFA
- RDS will implement Google Authenticator as the primary MFA mechanism
- MFA only needs to be activated once per user account. Switching roles or re-registering will require users to activate MFA again for the new account.
- CMS' RDS Center will provide step-by-step instructions and training materials prior to the implementation of MFA. These materials will be disseminated via email and the RDS Program Website.

REMINDER: It is a violation of Federal law to share or transfer user accounts or login and password information.

What is Google Authenticator?

- Google Authenticator is a free tool that generates a unique token every 30 seconds
  - Phone app for IOS and Android available from App Store or Google Play
- Google Authenticator generates the token based on multiple factors including a secret key associated with your user account
- A token generated with Google Authenticator will only work with the user account to which it is associated during activation
- Google Authenticator can only be activated on one device per user account
- Once implemented, a field will be present on the login screen that prompts the user for the current token displayed by Google Authenticator
- Google Authenticator does not share or transfer data between your device and the RDS Center; it simply generates a code which will be manually typed into the login page



One-Time Token

- An option for a one-time token will be available in the event a user's Google Authenticator device is not available
- One-time token is for use in emergencies only and the number of times it may be used will be limited
- One-time token will be delivered via text message or email. CMS' RDS Center will only send a one-time token to the text enabled number or email address associated with the user's RDS Secure Website user account
- One-time tokens will only be valid for 10 minutes
- An optional field for Text Enabled Number will be added to all registration pages as well as the Manage User Information page
- It is imperative that each user keeps his/her account information up to date

RDS Program Reminders

- ✓ Protect Your Secure Website Account
  - It is a violation of Federal law to share or transfer user accounts or login and password information.
  - Plan Sponsors are encouraged to protect account information and manage users responsibly.
- ✓ Keep Personal Information Up-To-Date
  - Ensure that your email address is kept current. Email is the main form of communication from CMS' RDS Center.
  - CMS' RDS Center is unable to update your Secure Website user account on your behalf.
- ✓ Keep Retiree Information Up-To-Date
  - Regularly download Covered Retiree Lists, submit updated retiree files to CMS' RDS Center during the Plan Year, and review Retiree Response Files and Weekly Notification Files to ensure costs are being reported based on the latest retiree information.

Questions and Open Forum

Use the Q&A feature to submit feedback:

- Enter your feedback in the Q&A feature located on the right hand side of the screen.
- Your questions will only be visible to the webinar presenters, who will read the question to the attendees and provide a response.
- If your question is not answered on the call, we will follow up with you directly.
- Please do not submit application or Plan Sponsor specific questions at this time. Those may be emailed to rds@cms.hhs.gov.