

Preparing a compressed, encrypted and password-protected archive to submit Roster Billing Forms electronically via e-mail

When using e-mail to send HIPAA protected data, such as that on the Roster Billing Form, it is important to ensure that any data is visible only by the intended recipient. This document describes one method to ensure compliance with HIPAA when sending documents containing Personal Health Information via e-mail.

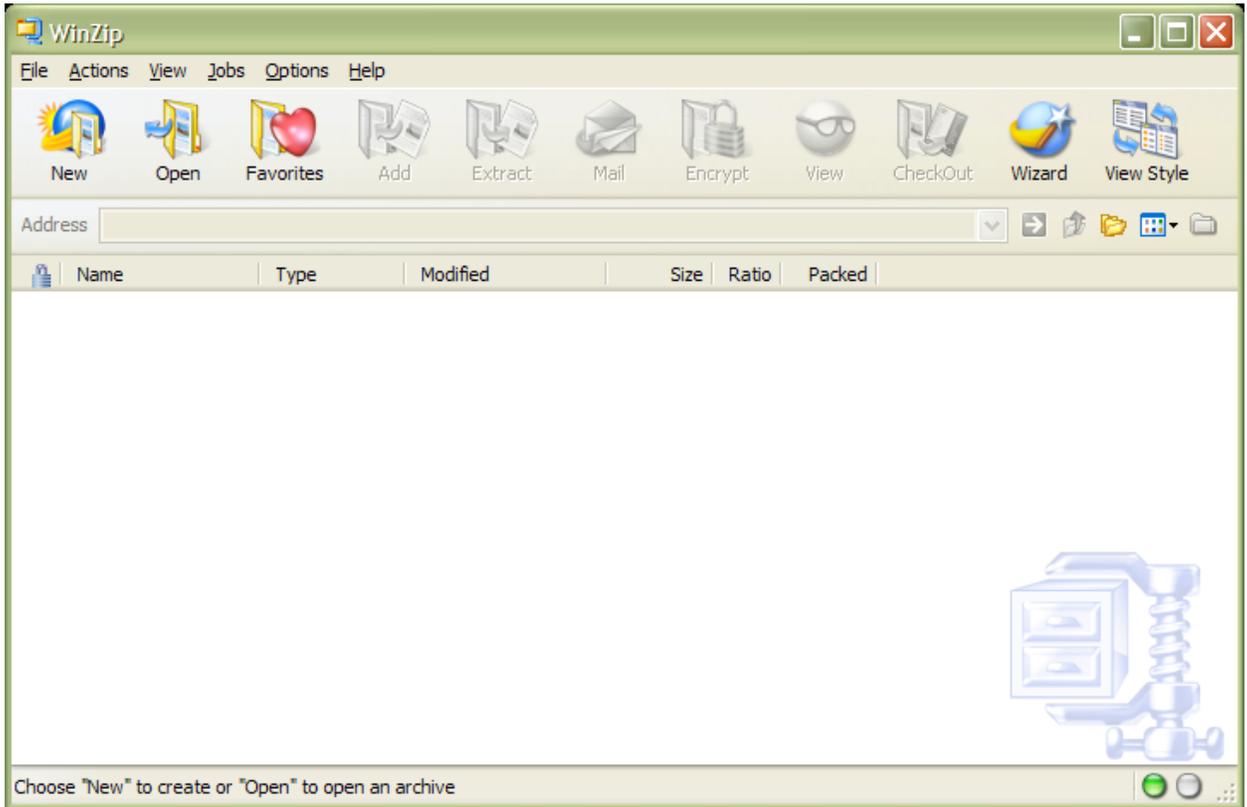
The Wisconsin Department of Health Services suggests using WinZip version 11 or higher to compress, encrypt and password protect files to be sent as e-mail attachments. This version of WinZip permits a very high level of protection, while employing a ubiquitous attachment file format. DHS does not provide WinZip software or support to its business partners.

It is important to understand that individual Roster Billing Forms do not need to be encrypted if they are made part of a compressed file that is itself encrypted prior to submission via email. Follow these steps to submit Roster Billing Forms electronically as attachments to an email:

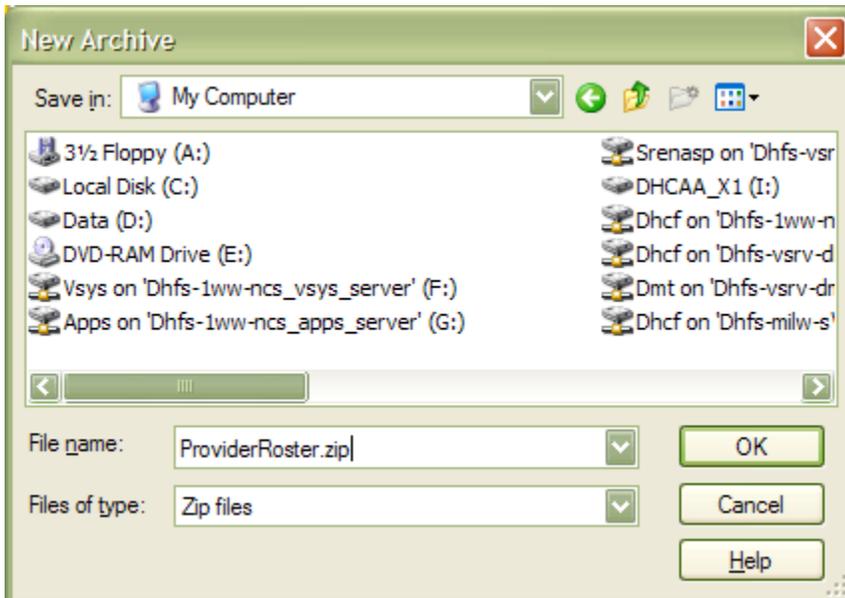
1. Complete and save the Roster Billing Forms you wish to send. You may combine multiple Roster Billing Forms within a single compressed transport file. (Note: Many e-mail systems have arbitrary limitations governing the maximum size of a single message, including any attachments to it. The arbitrary limit DHS observes is 15MB per message. Anything larger is rejected by the e-mail server. Business partners should consult their own IT staff to determine whether or not there are any limitations imposed by their own e-mail systems.)
2. Open WinZip by double-clicking on the WinZip icon. Your WinZip icon should look something like this:



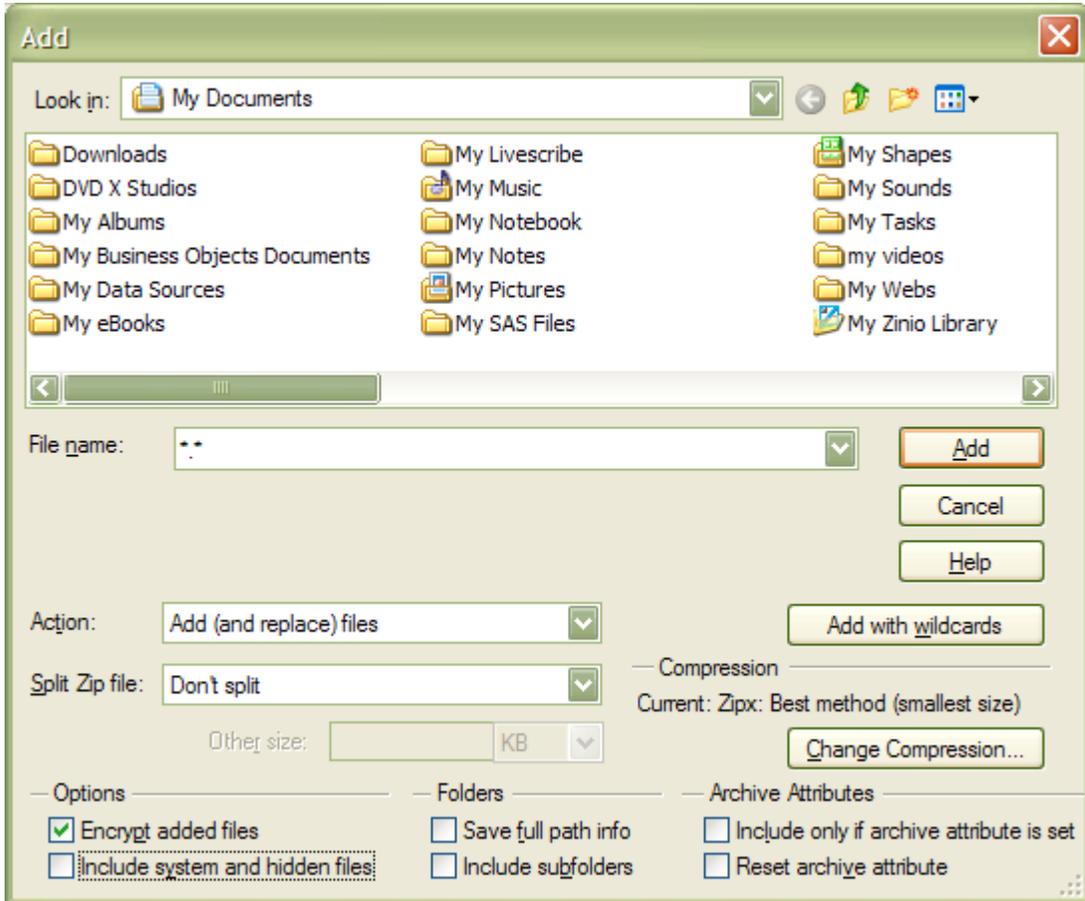
When you double-click the WinZip icon and the program starts, you will see a window similar to this:



Click on "New" and the following dialog will appear.



In the “File name” text box, enter a name for the archive (compressed file) you are about to create. In the above example, we named the file “ProviderRoster.” You can choose any file name you want. Then press the <Enter> key to proceed. You will see the following dialogue box.



3. To add the Roster Billing Form(s) to the archive, select the location on your local PC or network where the completed Roster Billing Forms are stored by using the “Look in:” dropdown box. Verify that the “Encrypt added files” option box is checked; then select the appropriate completed Roster Billing Form(s) from the “File name:” dropdown box. (To select more than one Roster Billing Form, hold down the <Ctrl> key on your keyboard while you select the Roster Billing Forms.) Click the “Add” button and this will appear:



Click "OK."

4. Next, you will be prompted to enter a password.



5. If you choose to hide the password, you will need to re-enter it for confirmation. For the password, use the 10-digit phone number of one of the Participating Provider's service delivery sites. Be sure to use the phone number for the service delivery site as it was indicated by the Participating Provider on Attachment 1 of the Memorandum of Agreement. Do not include any spaces, hyphens, or special characters in the password (e.g., 6085551234). Choose the "256-Bit AES encryption" method to ensure HIPAA compliance. Then Click "OK." The compressed, encrypted and password protected archive transport file has been created.

6. WinZip will display the names of the documents or files you have chosen to include in the archive transport file. Documents and filenames showing an asterisk (*) after the filename are encrypted.
7. You may now close WinZip.
8. Open your e-mail client if it is not already open and follow the e-mail client software's instructions for attaching the compressed transport archive you created with WinZip. (If you need help using your email system, please consult your in-house support staff.) In the body of the email, indicate the Participating Provider's name and the name and address of the service delivery site corresponding to the phone number that was used as the password for the encrypted Zip file. Also include the contact information of the individual sending the email, and please include a phone number we can call in case of problems or questions.
9. A final note: Only the attachment to the email you send to us will be encrypted and HIPPA compliant. You cannot rely on the message portion of the e-mail being encrypted. Therefore, avoid including any Personal Health Information or other sensitive information in the message portion of the e-mail. **Never disclose any password in the body of an email.**