CDA Secure Send Message Retention Period Extended to 60 Days

Due to the large number of dental offices that are closed during the COVID-19 pandemic, messages sent using CDA Secure Send will now be retained in the system for 60 days. Under normal circumstances, messages are retained for 30 days. Extending the retention period will provide dentists and/or dental office staff additional time to retrieve important messages.

When dental offices begin to resume normal business operations, the message retention period will return to 30 days to help minimize the risk of data exposure. The Canadian Dental Association (CDA) will issue a new notification before this change comes into effect.

Important:

You should continue to have access to CDA Secure Send messages during the COVID-19 pandemic. Messages should be sent to an email address that you have access to.

Review your information:

Your current email address on file with CDA is:

Email Address:
Office Number:

Change your Email Address:

Please use the following steps if you need to change your email address on file with CDA:

1. Log into the CDA Practice Support Services website https://services.cda-adc.ca/.
   For help with your username/password, contact the CDA Help Desk: 1-866-788-1212
2. Click the *My Info* tab.
3. Click *Email Address.*
4. Click the *Add email* button.
5. Type in your new email address.
6. Go to your email inbox and open the verification email with the subject *CDA - Action Required - Email Validation.*
7. Click the link in the email that says *Click here to validate this email address.*
8. Your new email is now active and can be assigned to any of your offices by visiting the CDA Practice Support Services website and visiting your *My Info* tab and then *Email Address*.

Phishing Warning:
Please be aware that there are a range of COVID-19-related phishing scams going out to dental offices. These scams tempt users:

- to buy face masks and other personal protective equipment;
- with phony medical cures; and/or
- to give up personal bank or government login credentials to access federal funds as part of Canada's COVID-19 Federal Economic Response Plan.

Please be vigilant when opening or responding to emails. Make sure you only open emails from known sources. It's smart to avoid advertisements seeking to take advantage of the impacts of the COVID-19 pandemic.

Here are some tips to help spot phishing email:

Beware of online requests for personal information: A coronavirus-themed email that seeks personal information, such as your Social Insurance Number or login information, is a phishing scam. Legitimate government agencies will never for this information. Do not respond to the email with your personal data.

Check all links: You can inspect a link by hovering your mouse over the URL to see where it leads. Sometimes, it's obvious that the web address is not legitimate. Keep in mind that phishers can create links that closely resemble legitimate addresses. Delete the email.

Watch for spelling and grammatical mistakes: If an email includes spelling, punctuation and grammar errors, it's likely a sign that you've received a phishing email. Delete the email.

Look for generic greetings: Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal that an email is not legitimate. Delete the email.

Avoid emails that insist you act now: Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information immediately. Delete the email.

Help

For additional help, please call the CDA Practice Support Services Help Desk at 1-866-788-1212, Monday to Friday, 7:30 a.m. to 8:00 p.m. EDT.