



The Canadian Association of Critical Care Nurses

Policy Statement

The Canadian Association of Critical Care Nurses acknowledges individuals have rights with respect to how the personal information they share with the Association is collected, used, stored, and disclosed.

We collect, use, store and disclose personal information in a manner which is consistent with our vision, mission, and philosophy statements.

This privacy policy is being issued to ensure the personal information provided to CACCN National and our chapters is adequately protected.

CACCN Privacy Policy

Information we gather:

The following information may be gathered from our members and conference delegates via mail, email, website, telephone and in person:

- ✓ Name
- ✓ Address
- ✓ Telephone numbers
- ✓ Email addresses
- ✓ Occupation
- ✓ Place of Employment
- ✓ Credit card information for membership/registration processing only (*credit card information is not stored with CACCN*)
- ✓ IP Address
- ✓ Username for the Members Only area
- ✓ Photographic image

At times, we may also gather additional information via our Awards and Grant application process and the Dynamics of Critical Care™ Conference Abstract process. This information could include:

- ✓ Resumes and/or Curriculum Vitae.
- ✓ Abstracts / References
- ✓ Dynamics presentations

How CACCN uses the information gathered:

CACCN uses the information gathered via mailed, faxed, emailed and/or online processing to:

- ✓ Update our database for new/renewing applications for membership/registration.
- ✓ Publication purchase.
- ✓ Dynamics of Critical Care™ Conference Registration.
- ✓ To enhance your visitor experience to our website.
- ✓ Review for Awards, Bursaries and Grants offered by the association.
- ✓ Update photos on our website.
- ✓ Use photos in CACCN publications both on the internet and in print.

Access to Your Information:

1. Your personal information is accessible to the Board of Directors and/or Designate, Chapter Presidents and/or designate, and the CACCN Chief Operating Officer (employee).
2. Your banking/credit card information through the online membership processing is not visible, available and/or accessible by any employee, board member, chapter president or chapter member of CACCN via the website, email notification of your purchase or through any other means; unless this information is provided by the member via a mailed, faxed, or emailed membership application or conference registration.
3. Your personal and credit information is safeguarded by our secure server, Eigen Developments, who meets and exceeds the Payment Card Industry Data Security Standards Canada (PCIDSS).
4. PCIDSS is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council.
5. It is our intent and goal to safeguard your information and as such, we do not at any time give, trade, or sell member/purchaser information to outside sources.

Emails:

1. When sending email to all members, the email field for member emails will be BCC (blind, carbon copy) to safeguard against release of personal email addresses.

Photographic Images:

1. Approval to use photographic or video graphic means must be provided on a Photographic Consent Form to CACCN.
2. If taking photos or videotaping at a place of employment, a signed Photographic Consent Form signed by the hospital / organization to CACCN.
3. Signed photographic consent forms are required when taking photographs of patients and colleagues. These consents must be signed by the patient or their substitute decision maker (SDM). The Photographic Consent forms must accompany any photos sent to CACCN.

4. Photographs without signed consent forms will not be used by CACCN.
5. CACCN does not share photographic images with parties outside of the Association, however, may use the photographs, videos for marketing purposes.

Education Days / Dynamics Conferences / Webinars:

1. Photographs may be taken at Education Days and the Dynamics Conference, where it may not be possible to obtain a photographic consent from all present.
2. Notification of photographic activity should be displayed in the area and should be noted on the education / conference flyer.
3. Photographers should announce they are taking a photograph, thus, providing attendees who do not wish to be photographed with sufficient time to vacate the area.
4. Members understand their photographic image may be captured at educational events, webinars, and/or conferences and should make every attempt to vacate the photographic area.
5. Members/attendees understand that CACCN has the right to use the photographs from events, conferences, webinars.

Security measures

Website Purchases:

1. We ensure all information is maintained on our secure server and your credit information is not accessible to anyone within CACCN or outside of the Association unless specifically provided to CACCN.
2. CACCN encourages all members clear their browser cache following a purchase via the CACCN website.

Mailed, Faxed, Emailed Purchases:

1. We ensure all information is maintained in a secure, locked environment and credit card information is not accessible to anyone, other than when a member directly provides the information to the Chief Operating Officer of the Association via the membership/registration form or via email or telephone.
2. Following processing of membership/registration via the membership form or via email or telephone, credit card information is securely destroyed by cross shredding.
3. In addition, annually in January, the CACCN National Office undertakes a secure shredding program to remove documentation past the seven-year timeframe.

Dynamics Presentations:

1. Presentations from the Dynamics of Critical Care™ Conferences will be converted from PowerPoint to PDF.
2. The PDF will be password secured against editing and printing.

3. Presentations will be posted in the public area of the CACCN website.
4. Presentations will only be posted if the presenter provides permission in writing.

Members Only Username and Password:

1. CACCN maintains a list of the current usernames.
2. Passwords are encrypted and CACCN does not have access to member/registration password information.
3. CACCN has provided a safe/secure password retrieval system for members who have misplaced their passwords to ensure their passwords are not compromised.
4. To recover a password, the member must use the 'reset password'.
5. Should the member request CACCN reset the password, they understand their password is not secure and they should visit the member database to change the password.

Use of Website Cookies (updated January 2021):

1. Our website makes use of "cookies", small digital files that are stored in your web browser.
2. Cookies are used to make it easier and more convenient for our users to move around our website, allowing faster access to information.
3. Cookies are stored on your computer's hard drive.
4. Your browser settings may allow you to block these cookies, but we recommend you have them enabled to help personalize your experience of our websites.
5. Our advertising partners may participate in the 'audience extension' program offered with their leaderboard advertisements on the top/bottom/side of the CACCN webpages:
 - a. The audience extension program reads the 'behaviour' of the visiting party and further personalizes your experience on the CACCN website and other websites you may visit.
 - b. Audience extension is a common practice with digital media.
 - c. No information of a personal nature is available, shared, divulged, or tracked with the use of cookies and/or the audience extension program.

CACCN File Review Prior to Release of Information

CACCN has implemented the following policy as a preventative measure against Privacy Breaches:

1. The Chief Operating Officer will review the file to ensure all personal information is removed unless the member has provided written permission to include.
2. Personal information includes, but is not limited to:

- a. Name
 - b. Address
 - c. Telephone numbers
 - d. Email addresses
 - e. Occupation
 - f. Place of Employment
3. Secondary review of the file will be completed by the Board of Directors to ensure all identifying information is redacted unless the member has provided written permission to include.
4. The Board of Directors will appoint two board members to complete the review.

CACCN Chapters

1. CACCN Chapters are required to uphold the policies of the CACCN.
2. This Privacy Policy extends to the handling of information by CACCN Chapters.

Managing Privacy Breaches

CACCN National Office:

Should a privacy breach occur at the National level, the following steps will be taken immediately:

The Chief Operating Officer will provide a written report on the day of the breach to the Board of Directors detailing the following information:

- a. Date and time (if available) of the privacy breach
- b. How the breach was discovered
- c. Member(s) affected by the breach.
- d. Type of information released.
- e. Where the breach occurred – i.e., website, mail, etc.
- f. Cause of the breach – human error, electronic malfunction, etc.

The Board of Directors will review the Privacy Breach report.

Written notification from the CACCN National Office will be provided to those affected via email and regular mail detailing the breach and the action taken to resolve the breach.

CACCN Chapters:

Should a privacy breach occur at the Chapter level, the following steps will be taken immediately:

The Chapter President will provide a written report on the day is discovered to the Chief Operating Officer detailing the following information:

1. Date and time (if available) of the privacy breach.
2. How the breach was discovered.
3. Member(s) affected by the breach.
4. Type of information released.
5. Where the breach occurred – i.e., website, mail, etc.
6. Cause of the breach – human error, electronic malfunction, etc.
7. Remedies to ensure a similar breach does not occur in the future.

The Chief Operating Officer will notify the CACCN Board of Directors, who will review the Privacy Breach report.

Written notification from the CACCN National Office will be provided to those affected via email and regular mail detailing the breach and the actions the Chapter will or has taken to remedy the breach.

Disclaimer

Members must not share their username / password with non-CACCN members. This is considered a breach of the CACCN Membership/Registration Policy.

CACCN has no control over and will not be responsible should any member choose to share their personal information as noted above or their username / password via the CACCN Members Only, email or in person.

Such instances will not be considered a breach of privacy on the part of the Association and thus the Association will not be responsible for conducting a privacy breach review should this occur.

***Approved by the CACCN Board of Directors
Revisions Approved August 2021***

*Revisions Approved January 2020
Revisions Approved January 7, 2014
Original Approval October 13, 2011*