How We Protect Your Information

At **Windsor Regional Hospital** we use strict security measures, including encryption and regular audits, to protect your personal health information.

We comply with all laws and regulations to ensure your data remains secure.

If you have any questions or concerns, please don't hesitate to contact our **Privacy Officer** at 519-254-5577, ext. 52510.

COMPASSION is our PASSION

Ouellette Campus
1030 Ouellette Avenue
Windsor, ON
N9A 1E1

Met Campus
1995 Lens Avenue
Windsor, ON
N8W 1L9

www.wrh.on.ca

For information about the new Windsor-Essex Hospital System
www.windsorhospitals.ca

9458-U (Rev: 06/12/2025)

Protecting Your Personal Health Information

WINDSOR REGIONAL HOSPITAL
OUTSTANDING CARE – NO EXCEPTIONS!

At **Windsor Regional Hospital** we are committed to safeguarding your personal health information (PHI).

Your health and privacy are our top priorities, and it's important for you to understand how you can help protect your information.

Please read the following tips to ensure your PHI stays secure:

1. Keep Your Health Information Private

- **Don't Share Your Login Credentials:**
  If you use an online portal or health app, never share your username, password, or security codes with others.
- **Limit What You Share:**
  Only share your health information with trusted providers and when necessary for your care.

2. Be Cautious with Emails and Phone Calls

- **Verify Who's Contacting You:**
  Be suspicious of unsolicited phone calls or emails asking for personal or health information.
  Verify the caller's identity before sharing anything.
- **Avoid Public Wi-Fi for Sensitive Conversations:**
  Never discuss your personal health information over public Wi-Fi networks. Use a secure, private network instead.

3. Understand Your Rights

- **You Have Control Over Your Information:**
  You have the right to request access to your health records, correct errors, and decide who can access your information.
- **Consent is Key:**
  You must give explicit consent before your information can be shared with others, except in situations where law or healthcare regulations require it.

4. Beware of Phishing Scams

- **Watch for Fake Emails:**
  Phishing emails often look like legitimate requests from healthcare organizations, asking you to click on links or provide personal information. ***Always verify through trusted channels***.
- **Use Strong, Unique Passwords:**
  Protect online health accounts with strong passwords and consider using two-factor authentication for extra security.

5. Secure Your Devices

- **Keep Your Devices Locked:**
  Always lock your phone, tablet, or computer with a password, PIN, or biometric security (like fingerprint or face recognition).
- **Use Encryption:**
  If available, encrypt your personal health data on your devices to protect it from unauthorized access.
- **Install Updates:**
  Regularly update your devices and apps to fix security vulnerabilities.

6. Be Careful with Paper Records

- **Store Documents Safely:**
  Keep any paper health records or documents in a locked, secure location.
- **Shred Sensitive Documents:**
  Shred old health-related documents that are no longer needed, especially those containing sensitive information.

7. Properly Dispose of Your Patient Identification Arm Band

- **Dispose Securely:**
  After your visit, be sure to remove and properly dispose of your patient identification armband.
  Do not leave it in public places or discard it in easily accessible trash bins, as it contains personal health information that could be used maliciously.
- **Shred or Cut It:**
  For extra security, consider cutting or shredding the armband before disposal to protect your identity and health information.

8. Report Privacy Concerns

- **Tell Us If You Suspect a Privacy Breach:**
  If you suspect that your health information has been accessed or shared without your consent, please notify us immediately.