Data Breach management & Communications Plan

Hearing and Speech Nova Scotia (HSNS) takes the protection of information and systems seriously. HSNS is approved to hold personal health information related to its services. We take every precaution to protect this information from cyberattacks. Our plan ensures we are prepared, transparent, and proactive should a data breach or ransomware event occur.

Why This Matters

- Healthcare is one of the top targets for cyberattacks.
- Attacks may involve:
    - Ransomware (locking data until payment is made)
    - Theft of data (selling or misusing stolen information)
    - Third-party breaches (attacks on platforms HSNS uses, like email or scheduling tools)
- Even if HSNS systems are not the intended target, attackers may assume otherwise.

How HSNS Responds

1. Immediate Situation Analysis
    - An Ad Hoc Crisis Management Team meets right away to assess the scope of the breach.
    - Systems and data are analyzed to understand what happened, what information (if any) was affected, and who may be impacted.
    - Evidence is preserved and documented for legal and security purposes.

2. Response & Communication
    - HSNS works with IT specialists, legal counsel, insurers, and public health partners.
    - Depending on the situation, we may:
        - Notify law enforcement (RCMP/Halifax Police)
        - Involve the Department of Health and Wellness, Cybersecurity and Digital Solutions Nova Scotia, and other stakeholders
        - Communicate directly with affected employees, clients, or vendors
    - Public statements are only made once facts are clear, to avoid misinformation. Communication will be coordinated with NS government as appropriate.

3. Crisis Communication Principles
    - Honesty and transparency with those affected.
    - Clear updates on what happened, what risks exist, and what HSNS is doing.

- Support offered to impacted individuals (e.g., credit monitoring if personal data were ever compromised).
- Coordinated communication across all platforms (media, social media, direct communications).

4. After the Breach
   - HSNS reviews how the incident was managed.
   - Lessons learned are applied to improve policies, strengthen security, and refine communication plans.
   - A report is provided to the Board of Directors and all necessary government agencies as required by law.

Our Commitment

HSNS is committed to:
- Protecting systems, personal information, and data to the highest standards.
- Acting quickly and responsibly in the event of a breach.
- Being transparent and supportive with employees, clients, and stakeholders.

Your privacy and trust are a top priority. HSNS continues to strengthen cybersecurity safeguards to protect our community.

If you would like to comment or share your feedback with us, please:
- Call us at 1-888-780-3330, or
- Visit the HSNS website and enter your feedback