

Cybersecurity for Health Special Interest Group (CyberHealth SIG)

Purpose & Vision

Internationally and in Ireland the healthcare sector and its supply chain is increasingly targeted by cybersecurity threats, from ransomware to data breaches involving sensitive patient data.

The Cybersecurity for Health Special Interest Group (CyberHealth SIG) aims to provide a forum for organisations across the healthcare, health-tech and cybersecurity sectors in Ireland to share knowledge, identify gaps and opportunities, and strengthen cybersecurity best practices across Ireland's healthcare sector.

The CyberHealth SIG is managed by the [Connected Health & Wellbeing](#) Cluster and [Cyber Ireland](#) Cluster, and will unite organisations from both sectors- hospitals and healthcare providers, health-tech, med-tech and cybersecurity companies, regulatory authorities and government agencies.

Key Objectives

1. **Community Building:** Establish a trusted, cross-sectoral network across cybersecurity, digital health and healthcare providers through regular online and in-person meetings, fostering a safe and open environment for dialogue.
2. **Knowledge Sharing across health & industry:** Enable peer learning through expert talks, collaborative projects, and case studies.
3. **Challenge-focused:** Understand specific cybersecurity challenges of health stakeholders and address them through collaboration, around education and training, R&D projects, regulations and standards, and more.
4. **Solutions:** Identify cybersecurity problem statements and challenges of the health sector to be addressed by solution providers.

Membership

Open to Cyber Ireland and Connected Health & Wellbeing Cluster members, as well as key organisations in Ireland's health sector, including:

- Hospitals and healthcare providers
- Advocacy (e.g. patient organisations, NGOs, health professional representatives)
- Healthcare regulatory authorities
- Cybersecurity companies
- Digital health companies

- Medtech & Life Science companies

CyberHealth SIG member application:

- Expression of interest via online [Form](#)
- Applications are reviewed monthly by the SIG manager and approved by the SIG committee.
- New member is added to the mailing list, invited to next meeting and sent CyberHealth SIG Terms of Reference.

Structure & Governance

- **Managed by:** CyberHealth SIG Manager (employee of Cyber Ireland or CHW Cluster)
- **Committee:** representatives from healthcare (end-user / hospital), health-tech company, cybersecurity company and government agency.
- **Membership:** Application-based, vetted by committee, Cyber Ireland and Connected Health & Wellbeing Cluster.

Meetings & Communication

- Quarterly in-person workshops and online sessions. Topics selected by members, with guest speakers, case-studies and collaborative discussions
- Communication via email, and additional channels.

Topics of Interest

For Healthcare Providers

- Cybersecurity governance frameworks and risk management structures
- Cybersecurity tools adoption and effectiveness (products, services, support)
- Incident detection, response, and recovery capabilities
- International 'Best Practise' case studies and partnerships
- Cybersecurity awareness training programs
- Upskilling for IT and cybersecurity managers
- Cybersecurity workforce planning and role definition
- Greater understanding of healthtech cybersecurity systems

For Cybersecurity and Digital Health Companies

- Understanding and aligning with healthcare providers' cybersecurity needs
- Collaboration on incident response and threat intelligence sharing
- Compliance with healthcare-specific cybersecurity regulations and standards
- Market insights into healthcare cybersecurity challenges
- Networking and co-development with healthcare stakeholders
- Greater understanding of healthcare cybersecurity requirements

Membership Benefits – Why Join?

- **Access to a trusted, cross-sector network** of healthcare providers, health-tech companies, and cybersecurity professionals in Ireland
- **Peer learning and expert insights** through regular knowledge-sharing sessions and case studies.
- Opportunity to **address real healthcare cybersecurity challenges** through joint education, training, International projects, and R&D initiatives.
- Safe and **confidential environment to exchange** best practices, discuss shared challenges, and explore practical solutions.
- **Collaboration** opportunities for pilots, funding applications, and strategic partnerships.

Rules & Ethics

The CyberHealth SIG exists to work in the interest of organisations in the healthcare and cybersecurity sectors in Ireland and shall strive to ensure that all participants are treated equally and fairly

- Efforts shall be focused on the common interests of the CyberHealth SIG and not the interests of individual members or group of members.
- The general spirit shall be one of co-operation. Competition amongst private companies that may impair the effectiveness of the CyberHealth SIG, when possible, will be resolved by consensus. Competitors that see a conflict of interest in participating can withdraw, or may be asked to withdraw, their participation at any time.
- CyberHealth SIG members must not, directly or indirectly, use, disclose, reproduce or make available in any form any confidential information considered sensitive under Competition Law¹ and/or subject to Confidentiality Requirements. All meetings in-person and online will take place under Chatham House Rule, meaning participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.²
- There is a strict “no sales” rule applied to within the CyberHealth SIG. Solution providers should not pitch their solutions, unless explicitly invited to do so. CyberHealth SIG members should not be individually contacted for sales without permission.
- A list of CyberHealth SIG members will be shared within the group including, name and organisation. CyberHealth SIG members will be invited to join a CyberHealth SIG communications channel on signal, after they have participated in their first meeting.

¹ Information and/or data sensitive under Competition Law are for example: individual company prices, market shared, cost factors, business strategy, future plans, business plan, conditions of proposals to be submitted in order to participate to tenders on the market.

² [Chatham House Rule | Chatham House – International Affairs Think Tank](#)

- As a general information sharing rule, Traffic Light Protocol (TLP)³ should be applied in the official Forum discussions. TLP labels will be applied based on the sensitivity of discussions. Conversation facilitators should indicate to the Community Members which label is applied during the information exchange. The latest version of the TLP defines 4 sharing labels:
 - TLP RED
 - TLP AMBER (TLP AMBER+STRICT restricts sharing to within organisations only)
 - TLP GREEN
 - TLP CLEAR
- All CyberHealth SIG members are responsible and accountable for ensuring that the Rules are respected and followed.
- Any issues or concerns with fairness should be raised immediately with the CyberHealth SIG Manager and industry leads.
- Should non-compliance with the rules result in misconduct, Cyber Ireland will ensure that all such allegations or reports of any other irresponsible or unprofessional behaviour are acknowledged and receive an appropriate and proportional response. In the event of confirmed cases of misconduct, appropriate action will be taken, having been fairly and evenly considered regarding all the stakes involved.

³ Traffic Light Protocol (TLP) Definitions and Usage - <https://www.cisa.gov/news-events/news/traffic-lightprotocol-tlp-definitions-and-usage>