EFN Policy Statement on Cybersecurity

The healthcare sector has become increasingly digitalised and interconnected, depending heavily on personal and sensitive data, and with cyber threats that have become very frequent. As reported by the European Union Agency for Cybersecurity (ENISA), for the period 2021-2023, EU and European hospitals, and healthcare providers, have been targeted by at least 215 cyber-attacks, including ransomware attacks, data breaches and leaks, and Denial of Service (DoS) attacks. These were caused by different types of perpetrators, including cybercriminals primarily driven by financial gain motives, hacktivists, and state-sponsored actors.

These attacks can have a huge impact on the day-to-day health and care activities of hospitals and healthcare providers, forcing them to cancel appointments, postpone treatments and surgeries, diverting the inflow of patients to non-affected hospitals, and discharging patients to homecare whenever possible. From a frontline nursing perspective, a cyber-attack can have huge implications, resulting in a complete transition to manual operations - Electronic Health Records (EHRs) need to become paper health records, medication administration and reporting become manual, diagnosis, treatments, and exams planning also become manual, and critical care patients require closer observation and monitoring, all resulting in the need for increased staffing levels, and increasing the risk of incidents that may result in negative patients health outcomes.

Therefore, the President of the European Commission, Ursula Von Der Leyen (2024), proposed in the Political Guidelines for the Next European Commission 2024-2029, a European Action Plan on the cybersecurity of hospitals and healthcare providers, which was officially published on 15 January 2025. EFN welcomes this Action Plan, as hospitals and healthcare providers are increasingly subject to cyber threats, however, at this stage, the Action Plan fails to address concretely the needs and challenges faced by frontline nurses and allied healthcare professionals. For EFN, it is therefore crucial that the European Commission integrates the nursing perspective in the planned revision of the Action Plan, in consultation with key stakeholders, until the end of 2025.

From an EU Policy perspective, the revised Action Plan must build on and complement the European Health Data Space (EHDS) Directive, and especially the revised Directive on measures to ensure a high common level of cybersecurity in the Union (NIS2 Directive). Under this Directive, healthcare facilities are required to protect patient data from cyber threats by implementing cyber

risk management measures, having a clear incident-reporting process, and securing patient data through proper storage and handling practices. Furthermore, regular testing and updates of cybersecurity systems and regular staff training are also mandated. Finally, the NIS2 Directive also introduced the important concept of the liability of senior management, which protects individual nurses from being liable for the negative consequences of a cyber threat if this is the result of human error on the nurse's side. These are very important aspects, which the updated version of the European Action Plan on the cybersecurity of hospitals and healthcare providers can build on and improve if the nursing perspective is considered during the revision phase and implementation.

Therefore, the EFN recommends the European Institutions and the Member States to:

1. Ensure full alignment between the European Action Plan on the cybersecurity of hospitals and healthcare providers, the EHDS, and the NIS2 Directive – the Action Plan must go further than the NIS2 Directive by focusing on the specific needs of frontline nurses and allied healthcare professionals (HCP).
2. Integrate in the Action Plan a requirement to develop interoperable, co-created, local/regional/national cyberattack contingency plans, based on existing good practices from the EFN Members. The focus of these cybersecurity contingency plans should be on:
    - the appointment of a crisis steward, who should be someone at the management or administrative level (preferably an experienced nurse) who can guide frontline nurses and allied healthcare professionals in interprofessional teams during the cyberattack;
    - focused education and training on preparedness and prevention of cyberattacks – awareness raising for frontline nurses and allied HCPs, as well as regular training to guarantee readiness to implement cyberattack contingency plans, will contribute to both preventing cyberattacks and ensuring that patients are not affected if a cyberattack takes place. Being prepared will also ensure the resilience of the physical and mental well-being of frontline nurses and allied HCPs;
    - focused dialogue between doctors, nurses and allied HCPs, ensuring a smooth transition from digital to manual tasks in the event of a cyberattack;
    - ensuring that patients' EHRs are saved daily in offline encrypted backups and/or paper format, enabling the continuity of care in the event of a cyberattack.
3. Invest in EU domestic nursing workforce capacity building in line with the Directive 2013/55/EU and the Updated Annex V – In a time marked by crises and more frequent cyberattacks, it is essential to recognise healthcare and nurses as an essential part of the critical infrastructure. Healthcare preparedness is part of the overall preparedness. The nursing shortages are already harming the resilience of EU healthcare ecosystems.

4. Make available adequate funding through the Recovery and Resilience Facility (RRF), as well as other existing funding streams like the Digital Europe Programme and Horizon Europe, or innovative funding streams, for the implementation of both the NIS2 Directive and the Action Plan. Due to lack of standardisation, ageing technology and devices, the cost of educating and training frontline nurses and allied healthcare professionals, and budget cuts, hospitals and healthcare providers too often lack the resources to implement cybersecurity measures.
5. Ensure that cybersecurity measures match the needs of frontline nurses as end-users, and that they fit into everyday workflows without compromising care provision, by coordinating closely since the outset and throughout the implementation phase with the National Nurses' Associations.

Further readings:

- EFN Policy Statement on improving frontline nurses' time for direct patient care with digitalisation and responsible AI (2024). Available at: https://efn.eu/wp-content/uploads/2024/10/EFN-PS-improving-frontline-nurses-time-for-direct-patient-care-with-digitalisation-responsible-AI-Oct.-2024.pdf
- EFN Policy Statement on the European Health Data Space (EHDS) (2023). Available at: https://efn.eu/wp-content/uploads/2023/04/EFN-Policy-Statement-onEHDS-April-2023.pdf
- EFN Position Statement on Nurses Co-Designing Artificial Intelligence Tools (2021). Available at: https://efn.eu/wp-content/uploads/EFN-PS-on-Nurses-CoDesigning-Artificial-Intelligence-Tools.pdf
- EFN Policy Statement on Nurses Digital Competencies (2019). Available at: https://efn.eu/wp-content/uploads/EFN-Policy-Statement-on-Nurses-DigitalCompetencies-Nov.2019.pdf
- The Recovery and Resilience Facility. European Commission. Available at: https://commission.europa.eu/business-economy-euro/economicrecovery/recovery-and-resilience-facility_en
- The European Semester. Available at: https://commission.europa.eu/business-economyeuro/economic-and-fiscal-policy-coordination/european-semester_en
- The European Pillar of Social Rights. Available at: https://ec.europa.eu/social/main.jsp?catId=1226&langId=en
- The Pact for Skills. Available at: https://pact-for-skills.ec.europa.eu/index_en

Please contact Dr Paul De Raeve, Secretary General of the European Federation of Nurses Associations, for more information. Email: efn@efn.eu - Tel: +32 2 512 74 19 - Web: www.efn.eu