EUROPEAN UNION AGENCY
FOR CYBERSECURITY

6TH eHEALTH SECURITY CONFERENCE HIGHLIGHTS

The outbreak of COVID-19 has made the dependency on virtual services rise exponentially and proportionally increased cybersecurity risks, even for the healthcare sector.

Medical data and systems have become a major target of cybercrime. Phishing campaigns and ransomware attacks are just a few examples of malicious actions. This is why healthcare organisations need to enhance their cybersecurity posture.

A set of guidelines based on the discussions taken place during the online series of the eHealth Security conference pave the way towards a strong cybersecurity strategy in healthcare organisations.

6th EHEALTH SECURITY CONFERENCE 2020 – ONLINE SERIES

Together with the support of the Danish Health Data Authority, the EU Agency for Cybersecurity (ENISA) organised three eHealth Security Conferences on the following topics:

1# **Cybersecurity in healthcare during the COVID-19 crisis**

2# **Cybersecurity for COVID-19 tracing mobile apps**

3# **Incident response procedures across Europe's heath system**

These guidelines is a snapshot of key findings and recommendations addressed in the discussions initiated by the conferences.

CYBERSECURITY GUIDELINES

1. **DEVELOP AN INTERNAL CYBERSECURITY POLICY**

   Define a cybersecurity policy to apply strict cybersecurity measures addressing all working methods including remote working.

2. **BUILD CYBERSECURITY CAPACITY AND ENHANCE PREPAREDNESS**

   Organise drills and cyber exercises as often as possible: Running exercises such as cyber games will help reduce human errors and induce the most efficient behaviour responses needed when an attack occurs.

3. **ENHANCE PRIVACY AND DATA PROTECTION**

   Find the solutions you need in the existing legislative frameworks based on recommendations that provide required flexibility.

4. **PROMOTE CYBERSECURITY GOOD PRACTICES**

   - Implement traffic monitoring using VPN. Specific criteria allow monitoring and setting of alerts in the VPN traffic and even failed user login.
   - Make it a priority to patch most critical components in a timely manner;
   - Enforce use of Two-Factor Authentication (2FA).

5. **STRENGTHEN YOUR CYBERSECURITY RESILIENCE WITH NEW TOOLS**

   - Investing in cybersecurity will help raise the levels of security required to operate both securely and efficiently.
   - Cloud is an enabler for cybersecurity for healthcare organisations lacking resources.

6. **PROMOTE AWARENESS TO HEALTH WORKFORCE AND PROFESSIONALS**

   Inform and train staff to empower them with vigilance ensure cyber hygiene.

7. **IDENTIFY INTERDEPENDENCIES AND ENHANCE CYBERSECURITY PROTECTION**

   Cybersecurity protective mechanisms must be enhanced at any crossroads where healthcare meets actors of other economic sectors to identify links and apply hardening mechanisms.

8. **SUPPORT INFORMATION SHARING**

   Timely sharing of information at national and European level for a faster response to and resolution of incidents at both national and cross-border levels.

9. **ENSURE REGULATORY COMPLIANCE**

   Implement the requirements of EU regulations specifically tailored to the health sector.

10. **ENGAGE IN COOPERATION WITH THE DIFFERENT ACTORS OF THE EU CYBERSECURITY COMMUNITY**

    Initiate dialogue with European partners. To widen your perspectives and identify solutions most fitted to your organisation.