CPME/AD/Board/31102015/091_Final/EN

On 31 October 2015, the CPME Board adopted the 'CPME policy condemning cyber-attacks: Better protection of critical IT infrastructures' (CPME 2015/091 FINAL)

# CPME policy condemning cyber-attacks: Better protection of critical IT infrastructures

*The Standing Committee of European Doctors (CPME) represents national medical associations across Europe. We are committed to contributing the medical profession's point of view to EU and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues*[1].

Attacks on critical IT infrastructures, like those used in the field of energy and water supply or telecommunications, represent a growing potential threat to the general public. Such cyber-attacks on civilian networks of public interest, e.g. the infrastructure used in healthcare could place the general public at risk and lead to humanitarian disasters.

The European medical profession therefore calls for the condemnation of cyber-attacks on critical IT infrastructures of public interest and urges the operators of these infrastructures, as well as policy makers around the world, to work together to effectively combat the emergence of cyber-attacks and to cooperate to the best of their ability to defend against such attacks. These provisions must be particularly effective against cyber-attacks directed at IT structures in medical care, including hospital information systems, practice management systems or control systems for technical medical devices. Malfunctions or manipulations resulting from attacks on these IT structures in high-tech healthcare systems could quickly lead to patient vulnerability. For this reason, these IT networks are particularly in need of protection. Attacks could also lead to the exposure of sensitive patient data.

Given the impact this scenario would have on data privacy and patient safety, we appeal to physicians in Europe, as well as policy makers in the healthcare sector, to pay particular attention to cyber-attacks and to the measures needed to defend against them:

[1] CPME is registered in the Transparency Register with the ID number 9276943405-41. More information about CPME's activities can be found under www.cpme.eu

1. Since a cyber-attack generally represents a cross-border issue, strategies must be developed, particularly at the European level, to protect against cyber-attacks and to combat cyber warriors. The measures specified in the proposed Directive COM (2013) 48 concerning measures to ensure a high common level of network and information security across the Union, could form the basis of such a strategy.

2. Physicians need to be aware of the unique challenge cyber-attacks could pose to their ability to practice their profession. They should ensure, in accordance with deontological obligations and their contingencies, that their work environment is protected from cyber-attacks.

3. The competent authorities for cyber security in the Member States should reach out to the health sector to seek out ways to defend against cyber-attacks if the work environment represents a potential target.

4. In many cases, the expenditures required to defend against cyber-attacks surpass the financial resources of physicians and hospitals. Solo practices and small hospitals, in particular, could be overburdened by these expenses. If substantial investments in cyber security are required, they cannot be made at the expense of patient care. We therefore call upon the European Union and its Member States to establish separate budgets beyond the healthcare sector to deal with the challenges posed by cyber-attacks.