PURPOSE: For decision
CONCERNING: Professional Practice/e-Health
AUTHOR: CPME Secretariat / AS

CPME NUMBER: **2021/91 REV1**
DATE: 9 September 2021

CPME Statement on e-Evidence Regulation COM(2018) 225

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.

European doctors are gravely concerned by implications of the draft e-Evidence Regulation COM(2018) 225 ("Proposal") and in particular by the Council's negotiating position of 9 of July 2021. The European Union is based on the rule of law. Fundamental rights are protected by the Charter of Fundamental Rights of the European Union. This proposal undermines these two central foundations of the EU. It must be either withdrawn or redacted.

What is the Proposal about?

On 17 April 2018, the European Commission presented its legislative proposals on cross-border access to electronic evidence in criminal matters, *i. e.* a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters ("Proposal")[1] and a Directive establishing uniform rules on the appointment of representatives for the purpose of obtaining evidence in criminal proceedings.[2] The proposed legislation is intended to provide a legal framework for direct cooperation between investigating authorities and service providers. The production and preservation of electronic evidence in the EU should thus be made easier and more efficient. The difference compared to previous international cooperation in criminal matters is that the investigative authority can address an order directly to the service provider operating in another Member State, or rather to its representative. The service provider is then obliged to transmit or provisionally secure the requested data without requiring a prior decision by the respective national authority. In this way, the bureaucratic official channels of mutual legal assistance are bypassed.

How does the Proposal impact the health sector?

Online platforms or cloud services that store patient data could be requested to produce or preserve patient data by an order issued from another Member State - without any judicial review by the enforcing Member State, including any potential review by a national medical association or medical regulator. Equally, patient data resulting from telemedicine services or electronic medical records could be easily seized. This new "cooperation mechanism relieves the enforcing Member State from

[1] COM(2018)225 final.
[2] COM(2018)226 final.

its protective function insofar as the production order is executed without enforcement being necessary.

Instead, the issuing Member State and the service provider are assigned with this function, but neither of them is in the position to ensure an equivalent protection of the user's privacy rights."[3] Neither the Proposal nor the Council's position offer any special protections or guarantees to properly involve the enforcing Member State to check, verify and potentially waive medical confidentiality.

What does the Proposal mean for patients?

The proposal violates the right to privacy and the human dignity of patients. People and patients who are neither suspected nor accused of any crime come under investigation by the judiciary while their most sensitive data may be preserved or produced. And even if patients are suspects or defendants, doctors, offering telemedicine services,[4] are by no means state agents tasked to help state prosecutors to find a suspect of an offence punishable by 3 years' imprisonment or more.[5]

What does the Proposal mean for doctors?

The proposal violates professional secrecy and medical confidentiality that doctors have to comply with. If there are suspicions that what is communicated to a doctor does not stay with the doctor and that it can and will be used against the patient in a court of law, the profession will have to refrain from recommending the use of these technologies. Therefore, secure networks designed for the exchange of patient information between health professionals, patients, national health systems and/or health insurance funds should be excluded from the scope of the legislation.

CASES *where confidential patient data stored by physicians or health systems can be affected and compromised. Here the proposed safeguards to protect sensitive patient information are insufficient, as they rely on procedures which are not workable in practice:*

CASE I*: A production order aimed at obtaining patient information protected by professional privilege*

An investigating authority issues a production order addressed at a physician, requesting her/him to deliver information on one of her/his patients who is a suspect in criminal investigations. The physician is required to produce this information, or invoke professional privilege.

In this case, the possibility to invoke professional privilege must be clearly stated in the production order. Physicians who are entrusted with their patients' right to privacy must not be put at risk of facing sanctions for non-compliance. Therefore, where a production order is addressed to a physician, a judicial authority in the physician's Member State must always be involved. In all cases where it becomes apparent that the requested data is protected by professional privilege, a competent professional body should be informed and be given the possibility to comment and to consult with the physician and the judicial authorities concerned. Article 5(6) of the proposal provides that a production order may only be addressed to the service provider where investigatory measures addressed to the company or entity for which the service provider operates (e.g. a physician´s practice) are not appropriate. This safeguard itself is insufficient and needs to be reinforced. The list of cases in which a service provider may exceptionally be addressed directly must be short and exhaustive.

[3] Prof. Martin Boese, "An assessment of the Commission's proposals on electronic evidence", Study requested by the LIBE Committee, 2018, Chapter 5, p.38 ff., https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf.

[4] For a definition of telemedicine see 'CPME Policy on Telemedicine' (March 2021) as defined in the World Medical Association Statement on the Ethics of Telemedicine, October 2007, amended October 2018.

[5] The Proposal foresees that production orders for subscriber and access data can be issued for any criminal offence, whilst for transactional or content data can only be issued for criminal offences punishable in the issuing state by a maximum custodial sentence of at least three years. This could include minor offenses, such as theft.

What does the Proposal mean for the digital transformation in healthcare?

European doctors along with European patients, dentists, pharmacists and nurses acknowledge the value of digital innovation in bringing benefits for citizens, patients and health systems. Like in the analogue world, in the digital world healthcare professionals have to remain a trusted point of contact for patients.[6] However, if this trust is jeopardised, the use of digital tools in healthcare will remain in its infancies.

***CASE II**: A production order incidentally concerning patient information protected by professional privilege*

An investigating authority issues a production order addressed at digital service provider, requesting her/him to deliver information (e.g. a complete set of emails sent and received by the person) on a suspect in criminal investigations. This suspect could be a physician or a patient who has had correspondence with a physician. In both cases, the production order could -often unintentionally- concern information subject to professional secrecy. The service provider will generally not be aware of the fact that the production order concerns (partly) information subject to professional secrecy. Service providers do not have the technical or staff resources, nor the legal knowledge to carry out such an assessment. Moreover, they face the risk of penalties for non-compliance. Therefore, service providers are not in a position to raise the investigating authority´s awareness of the fact that professional privilege applies. As also the issuing authority may be unaware -or indeed unwilling to consider- that privilege may apply to (part of) the data requested, Article 5(7) of the proposal does not provide for an effective safeguard either. As a result, in cases where a production order is addressed at a service provider, protection of sensitive patient data remains very fragmented.

Recommendations

European doctors request an exemption for professions subject to professional secrecy, as there is no EU mechanism harmonising how privileges and immunities must be dealt with. Such exemption would be easier for service providers to put in place, and it could immediately trigger national procedures for verifying and potentially waiving privileges and immunities.

If an exemption is non-implementable, at least any new EU cooperation mechanism must provide for a systematic *ex ante* review of foreign orders by judicial authorities in the country of execution. It should include clear grounds of refusal when the requested data are covered by professional secrecy.[7]

In any case, where there is no risk to jeopardise an investigation and data is covered by professional secrecy, the production and preservation orders must first be addressed to the doctor, hospital or laboratory to ensure the adequate protection and respect of the data subject's right to privacy, data protection and human dignity, and are knowledgeable to interpret health data.

***

[6] The Consensus Framework on the Digital Transformation of Healthcare is available here.

[7] Cross-border data access in criminal proceedings and the future of digital justice, Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic Report of CEPS and QMUL Task Force, Centre for European Policy Studies (CEPS) Brussels October 2020, p. 78, https://www.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf .