Reference: ENISA-OUT-2020-4663
Date: 28/07/2020

European Union Agency
for Cybersecurity

Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Athens, 28th July 2020

Subject: Access to documents: Cyberattacks on EU hospitals

Dear Madam/Sir,

In accordance with Regulation 1049/2001 regarding the access to public access to documents we are attaching files to this letter with the information that you have requested regarding Cyberattacks on EU hospitals. Your request, registered on 8th July 2020, is related to:

1. *Any communication between hospitals or health authorities in the European Union and ENISA, since the start of the year (January 1st 2020). This could include but is not limited to, e-mails, text messages, basis documents, memos or drafts.*
2. *Any documentation transmitted between EU member states and ENISA since the start of the year (January 1st 2020), detailing information on national cyber attacks, cyber threats, weaknesses of cybersecurity systems, across EU health bodies or hospitals.*
3. *Any notification communicated from any public body within the EU to ENISA, concerning cyberattacks to hospitals or health authorities in the EU, and any follow up communication between ENISA and the specific body in such cases.*
4. *This request extends to any information that the ENISA holds in relation any of the above points, including information that may have been deemed short-lived or unimportant.*

Regarding your request, please consider that the documentation requested is regulated by Directive **(**EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union that establishes an absolute interdiction of disclosure of information that is essential to public security hereinafter referred to as NIS Directive,[1] (indicatively recital 8). Consequently, according to article 4 par.1 of Regulation 1049/2001, ENISA could disclose information that does not fall under the exceptions. In light of the above, we inform you that:

Related to the communication between hospitals or health authorities in the EU and ENISA; It is only at the request of a Member State (not of the Hospital itself) that ENISA assists by providing expertise and facilitating the technical handling of incidents that have a significant or substantial impact (art 7 (4) (b) Cyber Security Act, hereinafter referred to as: CSA[2]). Any data or information shared with ENISA,

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1595499067093&from=EN
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&qid=1594668174404&from=EN

ENISA will adhere to the obligation to preserve the security and commercial interests of the operator of essential services as well as the confidentiality of the information provided in the handling of incidents in line with art 14 (5) NIS Directive.,. Any data shared in the NIS Cooperation Group and the CSIRT's Network regarding individual incidents is marked as non-public, under Traffic Light Protocol (TLP)According to art 7 (4) (c) CSA, ENISA analyses vulnerabilities and incidents on the basis of public available information, or information provided voluntary by Member States for that purpose. Information in this public context that was analysed by the Agency as from January 2020 is provided to you in the attachments.

Your request related to ***documentation transmitted between EU member states or a public body within the EU and ENISA*** since the start of this year detailing information on national cyber attacks, cyber threats, weaknesses of cybersecurity systems, across EU health bodies or hospitals, we can inform you that EU health bodies or hospitals are considered as 'operator of essential services' as indicated in annex II of the NIS directive. This means that the processing of information is based upon the NIS Directive.

The Cooperation Group, composed of representative of the Member States, The Commission and ENISA, is tasked with the collection (article 11 (3) (i) NIS Directive) and exchange of best practice on the exchange of information related to incident notification (article 11 (3) (b) NIS Directive). The information ENISA receives, shares and processes within this context is marked as non–public and therefore cannot be made public.

Regarding the voluntary sharing of information of Member States within the CSIRT's Network, we can inform you that at the request of a representative of a CSIRT from a Member State ***potentially*** affected by an incident, information exchanging and discussions are related to non-commercially sensitive information and therefore non-public. (art 12 (3) (b) NIS Directive).

On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification. (art 14 (5) NIS Directive) Based upon this article this information is marked as non-public information. As stated under article 7(4) (b) CSA ENISA assists in the assessment of these incidents at the request of a member State in particular by supporting the voluntary sharing of relevant information and technical solutions, between Member States on a non-public basis.

According to art 14 (6) NIS Directive, only after consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest. In this respect ENISA is not the competent authority to inform the public, this is up to the competent authority of the Member State or the relevant CSIRT.

The CSIRT's Network has the opportunity to make non-confidential information concerning incidents information available **on a voluntary basis** according to article 12 (3) (c) NIS Directive, but until now this information is marked non-public. It may be possible that the CSIRTs Network decides in the future to make information public.

We included the information that the Agency is allowed to share with you, according to the relevant regulatory framework. This information has been made public and relates to cyber-attacks, cyber threats, weaknesses of cybersecurity systems, across EU health bodies or hospitals.

In response to your request please find attached the following presentations:

1. COCIR Webinar
2. Cybersecurity in the healthcare sector
3. Cybersecurity in the healthcare sector during the pandemic

Please be also informed that a relevant report will be published shortly on our website.

In accordance with Article 7(2) of Regulation (EC) No 1049/2001, you are entitled to make a Confirmatory Application requesting ENISA to review its position. Such a confirmatory application should be lodged within 15 working days of receipt of this reply by return to this email.

Kind regards,
ENISA