# The impact of the EU's cyber security Directive on eHealth

On 7 December 2015, after nearly three years of negotiation, the EU institutions reached an informal agreement on the EU Network and Information Security ('NIS') Directive, which *inter alia* imposes security and incident reporting obligations on 'operators of essential services' in critical sectors and on some digital service providers. Mark Young and Brian Kelly of Covington & Burling LLP explain how the NIS Directive will impact on the security of eHealth in the EU.

Broadly speaking, the NIS Directive will be a positive development for making eHealth in the EU more secure by ensuring that minimum levels of protection are implemented to protect networks and systems in the health sector, and that there are coordinated national and EU systems for combatting cyber security threats. National authorities, in turn, will be able to impose sanctions on operators that fail to adopt the necessary measures. By requiring healthcare providers to take appropriate security measures and notify serious incidents to the relevant national authority, the Directive may build public confidence in eHealth security.

One of the key aims of the NIS Directive is to help ensure that services that are essential for the maintenance of critical societal and/or economic activities in the EU are protected from security incidents and cyber attacks and to minimise the possibility of such services being interrupted. The Directive therefore requires certain organisations in the health, energy, transport, banking, financial market infrastructure, water supply, and digital infrastructure sector, as well as some digital service providers, to implement security measures and report significant security incidents to national authorities (broadly, the aim and nature of the obligations mirror existing obligations at EU level that already apply to telecommunications providers).

To be clear at the outset, the NIS Directive is separate from another new EU law that will shape cyber security in an eHealth context: the General Data Protection Regulation ('GDPR'). The GDPR contains numerous obligations pertaining to the processing of personal data, including security and incident reporting-related obligations. There are particularly heightened security obligations relating to special categories of personal data, such as health data, which will be applicable to eHealth operators. There is some overlap between the NIS Directive and the GDPR with respect to requirements to report security incidents under the NIS Directive and to notify personal data breaches under the GDPR. The key distinction is that the NIS Directive focuses on the security of networks and information systems that are used to provide essential services to ensure the continuity of those services, and incident reporting obligations apply to 'incidents' that have an adverse impact on the security of networks - whether or not those incidents impact personal data; by contrast, the GDPR and its data breach provisions apply to personal data only.

## Key obligations and enforcement

The NIS Directive imposes two key obligations on operators of essential services, including in the health sector, namely:

- to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems that they use in their operations; and
- to notify to the competent national authorities incidents having a significant impact on the continuity of the essential services the operator provides. (Article 14.)

Competent authorities are empowered to audit operators and request information relating to the assessment of the security of their network and information systems. Following this audit, competent authorities may issue binding instructions to those operators to remedy their operations. It is not yet clear how these instructions may take shape but the Directive appears to leave considerable discretion for those competent authorities. (Article 15.)

The NIS Directive has a lighter touch regime for some digital service providers, namely online marketplaces, cloud computing services, and search engines. For instance, whereas the rest of the Directive is a minimum harmonisation measure - meaning that Member States ('MS') are free to impose national rules that are more onerous than those under the Directive (Article 2) - MS would not be able to impose stricter security or notification requirements on digital service providers when transposing the Directive into national law (Chapter IVa).

## Which healthcare providers will be covered?

Operators of essential services include '[operators in] healthcare settings (including hospitals and private clinics)' as well as 'any natural or legal person or any other entity legally providing healthcare on the territory of a Member State' (see Annex II to the Directive and Article 3(g) of

Directive 2011/24/EU).

Much will turn on how MS transpose the Directive into national law and designate relevant operators - MS are required 'to identify the operators of essential services with an establishment on their territory' (Article 3a(1)). MS will do this applying the following criteria under the Directive:

1. an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
2. the provision of that service depends on network and information systems; and
3. an incident to the network and information systems of that service would have significant disruptive effects on its provision. (Article 3a(1a).)

To determine the significance of a disruptive effect - the third criteria above - MS are required to take into account several factors, including: the number of users relying on the services provided by the entity; the impact that incidents could have, in terms of degree and duration, on public safety; and the marketshare of the entity. (Article 3b(1).) MS are also required to take into account sector-specific factors where appropriate; recitals explain that the number of patients under the provider's care per year is a relevant factor in the health sector. (Article 3b(2) and recital 27.)

## Impact on eHealth

Given the prevalence of electronic medical devices in hospitals and clinics and the increasing use of online or electronic patient medical records, it has become increasingly important to protect networks, systems, and the information contained within them, and to ensure that only known, authorised devices are able to connect to network(s). The Directive should help to ensure that systems that are used in certain healthcare settings receive a minimum level of protection, and increase cooperation across the EU to combat cyber security threats.

**While it seems likely that many major hospitals and clinics will have to comply with national laws that implement the Directive, the position of other eHealth operators is less certain**

As explained above, implementation of the Directive will depend largely on how MS transpose it into national law and apply the designated criteria to identify covered healthcare providers. The respective particularities of national health systems will also be a relevant factor (e.g., there may be particular variation depending on the degree of private sector involvement in MS health systems). In any event, healthcare operators that are identified by MS will be required (i) to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of their network and information systems, and (ii) to notify the competent national authorities of incidents having a significant impact on the continuity of the essential services that the operator provides.

While it seems likely that many major hospitals and clinics will have to comply with national laws that implement the Directive, the position of other eHealth operators is less certain. An interesting convergence exists where healthcare operators who are subject to the rules interact with those who are not. For example, a hospital that is subject to the rules may contract to receive web-based, remote medicine adherence monitoring for a group of patients from a private eHealth platform that is not subject to the rules. In such cases, the hospital is likely to require the private provider to provide commensurate safeguards, which may result in a trend towards increased security and incident reporting provisions in service contracts.

The impact of the Directive will also vary by MS depending on the current regulatory environment. Some MS already have fairly robust cyber security measures in place for health systems and health contractors, whereas others will have to introduce new rules in order to meet the minimum level of protection established under the Directive. Where an entity provides a healthcare service that meets the criteria under the Directive in two or more MS, those MS are required to engage in consultation with each other before identifying the entity as being subject to local laws. There does seem to be a risk that cross-border eHealth service providers that provide services to healthcare providers that are subject to different national laws may have to comply, under contract, with varying security obligations, thus increasing internal compliance costs and obligations. Hopefully this risk will be reduced by the EU Agency for Network and Information Security ('ENISA') - the principal EU agency on network and information security - helping to determine what constitutes appropriate and proportionate technical and organisational measures, and providing practical guidance on and methods for incident reporting.

## Next steps

A few formal legislative steps remain, but the Directive is expected to come into force later this year, and then MS will have 21 months to transpose it into national law. Healthcare providers that may be covered would be well-served to track MS' implementation of the new law.

**Mark Young** Special Counsel
**Brian Kelly** Associate
Covington & Burling LLP, London
myoung@cov.com
bkelly@cov.com