The European landscape for cloud computing in health

Brian Kelly, Attorney at Covington & Burling and member of the *eHealth Law & Policy* editorial board, takes a look at the European landscape for cloud computing in health, and examines policymakers' ongoing efforts to promote its adoption. Brian identifies several key themes and best practices in the way in which different countries are supporting the technology's use.

Cloud computing - the migration of IT to 'hyperscale' data centres operated by third parties - is capable of supporting much of today's health IT, and could help healthcare organisations ('HCOs') across the EU provide better, more efficient and more cost-effective patient care. Yet despite these benefits, adoption rates are slow in the healthcare sector. This article explores reasons for slow adoption and floats ideas for how these challenges can be overcome.

Cloud benefits for HCOs

A key property of cloud computing is that it is rented 'on demand': instead of having to forecast IT needs and then procure and operate a fixed fleet of servers and software licences, HCOs can instead 'pay as they go' and scale IT resources up or down as needed. This helps HCOs avoid major capital outlays, and reduces the risk of over-spending on redundant capacity, or being incapable of responding to unexpected demands. Computers - even supercomputers - can be rented by the minute. For example, a bioinformatician could rapidly spin up a new machine to test a novel cancer-detecting algorithm, and then - as desired - either shut it down or expand it out to frontline staff.

Availability and elasticity aside, cloud computing also offers significant advantages in terms of resilience, security and energy efficiency. It typically operates at scale, making it commercially viable for the provider to offer high-end equipment, back-up capacity and security even to small customers. And the security measures on offer usually dwarf those that can be implemented in-house - helping HCOs ensure that systems integral to patient care and privacy receive the highest levels of protection.

Many HCOs already rely on cloud services for their non-clinical operations. Typical use cases include webmail, remote storage and backup, data analysis (of facility, supply or HR data), or cloud-enabled voice and video communications platforms.

But cloud computing can also be a key enabling technology for an equally wide array of clinical uses, such as telemedicine, medical data storage, and advanced health analytics. Those are increasingly high priorities for many HCOs looking to improve care and contain costs.

The EU regulatory and policy landscape

Health IT operates in a relatively intricate regulatory and policy environment in the EU, marked by complex rules and policy initiatives that can vary significantly from one Member State to another. The landscape is by no means unsurmountable, but can be difficult to navigate.

The key regulatory issues when adopting cloud computing solutions tend to revolve around privacy and data security. The basic rules in the EU are set out in the EU Data Protection Directive - but there is substantial variation in how these rules are implemented at national level.

Although even non-health data can be subject to different obligations in different EU Member States, it is the handling of data concerning health, genetics, ID numbers or other sensitive personal characteristics that presents the greatest challenge. This data is often subject to more detailed (and often inconsistent) rules and standards, as illustrated by the situation in France, England, Germany, Poland and Belgium.

France

French requirements are somewhat unique. Cloud service providers ('CSPs') are required to appoint a French-speaking doctor to 'oversee' processing of patient data (including its storage).

CSPs must also complete a demanding and lengthy review of privacy, contractual, security, ethical and financial aspects of their service, which are assessed by two bodies: the national data protection authority (the 'CNIL') and a multi-disciplinary Host Accreditation Committee ('CAH'). The review, shepherded by the national eHealth agency, ASIP Santé, takes around eight months, and hopefully culminates in approval from the Ministry of Health.

While certification of CSPs is sensible, the French process can be unwieldy and does not sync well with international certifications that a CSP may already have obtained. Moreover, recent statistics indicate that of 265 applications submitted since 2009, only 131 have been approved. The rest have been rejected, withdrawn, or are caught in an examination backlog[1].

Legal reforms introduced in January 2016 should ease that backlog: they will create an alternative process, managed by one or more approved

(independent) certification bodies[2]. Ideally, the new process will rely on standards that are more closely aligned with international standards that many CSPs, particularly those doing business outside France, will already be using (such as ISO/IEC 27001, 27002 and 27018, or the PCI-DSS standards for financial cardholder data).

Even so, France will for the time being remain one of the few countries in the world that specifically requires all outsourced IT service providers to be government-certified before they can handle any patient data.

England

England illustrates another constraint on the use of cloud services: data localisation.

European data protection law restricts the export of personal data from the EEA to countries that have not been whitelisted by the European Commission. But England goes further: a 2009 policy restricts English National Health Service ('NHS') organisations and their private sector suppliers from storing certain patient data outside England.

That policy, enforced by the NHS Health and Social Care Information Centre ('HSCIC'), dictates that '[i]n respect of systems and applications connected to [HSCIC] systems and applications Patient Identifiable Data should not be recorded outside of the England boundary in any format for any reason without the prior explicit written permission of [HSCIC].' This is a potent restriction, since HSCIC systems are of central importance in the NHS; they include, for example, the vital 'N3' network that interconnects NHS facilities throughout the country.

By contrast, systems not connected to HSCIC systems - such as a clinic's own segregated databases - are not subject to that restriction, and can readily be migrated to the cloud even if the provider is not in England. That dramatically widens their choice of provider for such data; many have data centres in Ireland or Germany, for example.

The key regulatory issues tend to revolve around privacy and data security. The basic rules in the EU are set out in the EU Data Protection Directive - but there is substantial variation in how these rules are implemented at national level

Germany, Poland and Belgium

The German legal and policy landscape for medical data protection is remarkably complex. Applicable rules can vary substantially according to State ('Länder'), type of care (health or social care), and even by type of HCO (religious hospitals, for instance, can set their own data protection rules).

In some cases, data localisation and outsourcing rules can be even stricter than the NHS HSCIC policy described above: in some Länder, HCOs are restricted from entrusting patient data to any third-party data processor, wherever they may be located. Others sometimes stipulate that only local processors can be used.

To compound matters, federal laws such as the Social Code can also impose restrictions. There is even a lingering doubt in some quarters over whether the use of a third-party data processor, without explicit patient consent, might violate a doctor's professional duty of confidentiality - in breach of the German Criminal Code.

To address similar concerns, Poland recently made a range of helpful changes to national law, which now explicitly authorises the use of third-party data processors (such as CSPs). In most cases, an express permission should not be necessary - in many Member States it is generally accepted that so long as a data processor handles and uses patient data strictly in accordance with the healthcare provider's instructions, there is no breach of doctor-patient confidentiality.

In some cases, a strict data localisation requirement, preventing the use of cloud computing, is unintentional; it can be a historical artefact in a law that has not kept up with the times. In 2014, for example, Belgium amended its Hospital Act so that it no longer required patient records to be created and maintained 'at' the hospital, but rather 'by' the hospital - a one-word amendment that enabled cloud-based hosting of those records.

Best practices

Given the potential benefits offered to HCOs by expanded cloud usage, including for patient data, the question is how to enable cloud usage in the healthcare sector. Four best practices stand out:

1. 'Cloud-first' policies and cloud-ready skills. Clear direction from a Ministry (or other prominent authority) is critical to giving HCOs confidence in cloud adoption.

The UK government, for example, stated in 2013 that "when procuring new or existing services, public sector organisations should consider and fully evaluate potential cloud solutions first - before they consider any other option."[3] It then created tools to help those organisations obtain cloud services, including a procurement framework (the 'G-Cloud') and an online 'Digital Marketplace.'

The NHS also has a dedicated agency for IT and information governance, the HSCIC (which will be renamed 'NHS Digital' later this year), which can help organisations procure cloud services (via G-Cloud and otherwise). Many other Member States also have eHealth agencies, albeit not always so well-resourced.

Efforts such as these need to be

supported by initiatives to boost digital literacy. A recent study showed that only 66% of NHS staff were aware of cloud computing, and only 33% said they felt confident using it[4]. The problem is EU-wide: the European Commission's eHealth Action Plan also acknowledged that 'a significant barrier [to eHealth] lies in the lack of awareness of eHealth opportunities and challenges for users (citizens, patients, health and social care professionals).'[5]

2. Funding. Funding is sometimes an important factor holding back cloud migration. Although cloud computing can have substantial cost benefits, its cost structures are not always a natural fit for CapEx-oriented funding programmes; funding bodies should therefore be more open to supporting transition costs and periodic 'pay as you go' fees, rather than just up-front asset purchases.

3. Updating existing regulations. Recent reforms in Belgium, France and Poland exemplify an ongoing trend towards eliminating regulatory barriers to cloud adoption.

As noted above, some historic restrictions were unintentional, whilst others were overly cautious responses to privacy and data security fears. In the latter case, reforms result from an important reassessment of the appropriate balance between data protection concerns and public health imperatives. That is something that data protection and healthcare policymakers can work together to achieve, provided they adopt pragmatic and balanced attitudes to data protection.

Reforms should also aim for greater harmonisation of rules across the Single Market. Many hoped that the new EU General Data Protection Regulation would help, but it ended up leaving Member States with discretion to maintain and potentially even extend many of their national, health-specific data protection rules. Additional harmonisation measures will therefore be needed.

4. Workable, internationally-aligned auditing/certification requirements. The EU Data Protection Directive requires the use of appropriate 'technical and organisational measures' to keep personal data safe and confidential - but it does not prescribe what measures. Many EU Member States have seen fit to create their own, localised IT security and privacy rules and standards.

Alignment of these requirements to internationally accepted standards - including ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (part of the ISO 27001 family of standards) - would be a significant step forward, enabling CSPs to more quickly demonstrate compliance (and if necessary, become accredited) to national requirements, through compliance with a single set of global requirements[6]. This will be one of the most anticipated features of France's reforms to its patient data-hosting accreditation requirements. In England, the NHS Secure Email Standard (ISB 1596) is already aligned with ISO 27001, as is much of the Information Governance Toolkit.

Any certification and auditing requirements must also be workable in practice. It should be sufficient - throughout the EU - for HCOs to rely on certifications or 'seals of approval' issued by reputable auditors against widely-accepted standards and assurance frameworks, rather than needing to conduct their own audits of service providers, which HCOs may not be appropriately resourced to do.

In addition, clear statements of regulatory requirements are useful to ensure that HCOs and CSPs know what needs to be done to stay compliant. There can be particular value in consolidating requirements (which can stem from different legal and policy sources) into a single reference, as the English NHS has done in its Information Governance Toolkit[7].

Closing comments

Cloud computing offers significant promise for the improvement of patient care and healthcare systems. Despite this, regulatory burdens, funding limitations and inexperience are constraining cloud computing's adoption by HCOs - there is therefore a clear case for swift and decisive policy support throughout the EU. The experience of various Member States suggests a core set of actions are needed: adoption of 'cloud-first' policies, development of e-skills, removal of funding restrictions, regulatory reform, and the implementation of efficient, harmonised approaches to auditing and certification.

Brian Kelly Attorney
Covington & Burling, London
BKelly@cov.com

1. See Kahina Haddad, Agrement HDS: Quelles Evolutions A Venir? Hospitalia n.32 (p. 62-63), February 2016: http://www.wobook.com/WBUU4e75MZ20/Hospitalia/Hospitalia_32_Fevrier_2016.html (in French).
2. Ibid.
3. https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it
4. https://www.huddle.com/blog/dods-nhs-research/
5. European Commission, Communication COM/2012/0736 final: eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century (December 2012), available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0736
6. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498
7. https://www.igt.hscic.gov.uk/