AbedGraham
Healthcare Strategies

A White | Paper

Dr Roshan Vara
Dr Gabriel K Ma

The NIS Directive: A Competitive Advantage for Health IT Suppliers

In order to maintain a competitive advantage in the current UK healthcare market, IT suppliers will need to prioritise policies and procedures about the development of robust service continuity plans, that allow clinical staff to continue treating patients effectively, in the event of an IT failure. These demands are being explicitly laid out in UK legislation in-line with the EU Network and Information Systems (NIS) Directive.

Healthcare IT suppliers that do not align their commercial operations accordingly could be at a competitive disadvantage, and at worst, could be setting themselves up for conflict with healthcare customers and regulators. This White Paper explores the most recent developments in these regulations and highlights key points for consideration.

Not Just About Data Privacy

"The NIS Directive relates to loss of service rather than loss of data, which falls under the General Data Protection Regulations (GDPR)"

Department for Digital, Culture, Media & Sport
August 2017

Data Regulations

Policy Overview

The release of EU GDPR was followed several months later by the release of the EU Network and Information Systems (NIS) Directive. Whilst EU GDPR is concerned with managing and safeguarding data loss and privacy, the NIS Directive is concerned with managing and safeguarding against the interruption of service delivery.

The UK has sought to integrate these bloc laws into its own legislature and has provided a roadmap for the implementation of these regulations aligning to its National Cyber Security Strategy 2016-2021, for national security and resilience from cyber threats. The release of these documents has been summarised in a timeline below, (Figure 1).

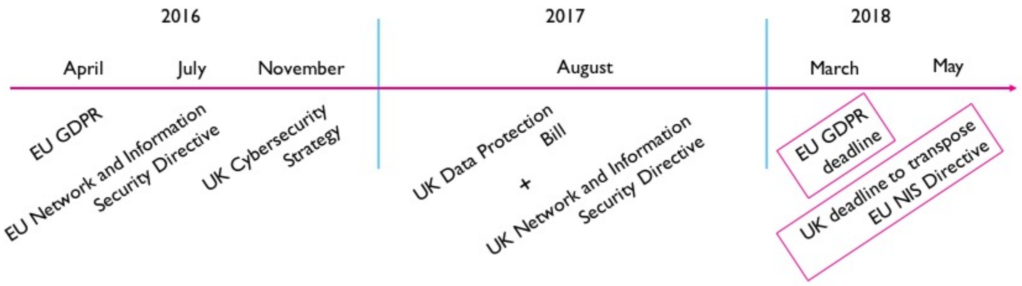
2016
2017
2018
April
July
November
August
March
May
EU GDPR
EU Network and Information Security Directive
UK Cybersecurity Strategy
UK Data Protection Bill
+
UK Network and Information Security Directive
EU GDPR deadline
UK deadline to transpose EU NIS Directive

Figure 1: Depicting the timeline of key EU and UK legislation on Data Privacy and Security

Responsibility

"Businesses and organisations must also understand that, if they are the victim of a cyber-attack, they are liable for the consequences"

National Cyber Security Strategy
November 2016

In August 2017, the UK released its Data Protection Bill 2017 that incorporated EU GDPR with UK-specific addenda. At the same time, the Department for Digital, Culture Media & Sport released a UK-specific NIS Directive in the wake of the WannaCry ransomware attack.

The NIS Directive seeks to enshrine service continuity measures in all UK essential services including healthcare providers and their IT suppliers. Failure to comply with the NIS Directive carries the same financial penalty as transgressing GDPR. **In essence, if an organisation fails to protect patient data rights as well as protect against Cyber Attacks (e.g. DDOS), they risk being fined by two separate regulatory bodies (with penalties that amount up to £17 Million or 4% of annual turnover for each body).**

As a result, whilst many healthcare organisations and IT vendors are focused on preparing for EU GDPR, it is equally important that activities are also directed towards preparations in advance of the NIS Directive.

The NIS Directive

Security Requirements

The UK-specific NIS Directive proposes regulations that will apply to both Operators of Essential Services (OESs) such as hospitals and other healthcare organisations, as well as Digital Service Providers (DSPs) including Health IT vendors (particularly those offering Cloud Computing Services).

Importantly, any incident that can or has affected the **provision of healthcare** will come under direct scrutiny of the NIS Directive. By May 2018, healthcare organisations will be expected to implement appropriate risk management and mitigation protocols for such events. Amongst many high-level security requirements, there is a significant focus on the management of service continuity plans for both OESs and DSPs. For OESs there is a particular reference to having:

"Capabilities to minimise the impacts of a cyber security incidents on the delivery of essential services, including the restoration of those services", Department for Digital, Culture, Media and Sport, August 2017

Clarification of the principles that DSPs are expected to follow from the UK NIS Directive have been laid out in the EU Implementing Act (in co-operation with the Information Commissioner's Office as the UK's national supervisory authority for GDPR, and the NCSC). When outlining the appropriate and proportionate technical and organisational measures that a DSP will need to work on in the management of risks to healthcare network and information systems, again there is a significant focus on **Incident Handling** and **Service Continuity Management** including *"the systematic management of network and information systems which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system lifecycle management and where applicable, encryption and its management"*, (Directorate-General for Communications Networks, Content and Technology, 2017).

It Affects Both OESs & DSPs

"The role of the competent authority in the event of any incident will be to assess whether the incident was foreseeable, whether effective risk management was in place, and whether the operator (or digital service provider) had appropriate security measures in place."

NIS Directive Public Consultation
August 2017

It is likely that healthcare organisations will therefore make it a mandatory procurement process for any Health IT service provider to demonstrate competency with these security requirements, not just those vendors who are solely Cybersecurity solution suppliers. At AbedGraham it is our belief that the implementation of these security principles through the NIS Directive in fact provides an opportunity for vendors to demonstrate that they can work jointly with healthcare organisations to address these issues effectively, providing two main benefits for the vendor:

1) **A reduction in vendor liability in the event of a cybersecurity incident and its consequent fall-out and associated financial penalty**

2) **A gain in competitive advantage for the vendor by providing solutions matching both OES and DSP requirements**

The Importance of Clinical Workflows

Mapping Clinical Workflows

Understanding the complexity of hospital workflows allows for the optimised development and implementation of appropriate policies and procedures that provide robust contingency plans in the event that network and information systems go down. When mapping workflows, it is important to note that not only can there be significant variation in operational processes between different specialties and departments, but additionally also within departments and between staff roles.

In the event that network and information systems do go down, hospitals will look to both their own and vendor contingency plans to maintain service delivery in order to minimise patient harm. For the vendor, this will involve planning contingency services that complement the existing clinical workflows, so staff can continue to provide unimpeded clinical care.

Vendors who can support OESs to implement effective security solutions in line with a comprehensive understanding of clinical workflows across the enterprise, can expect to establish a strong position in the marketplace.

Change Management

At AbedGraham we work with vendors to engage with healthcare organisations and their end-users so that they can maximise the benefits associated with different health IT platforms and solutions. This is particularly important in hospitals with complex IT infrastructures that are intertwined with a myriad of clinical and non-clinical workflows.

When implementing a new solution, frontline clinical staff are more likely to be prepared for adverse events if they have been proactively consulted about service continuity during the risk management component of the deployment process. Vendors will need to have clear processes, developed internally, that demonstrate a granular understanding of how their solutions can impact different end-users and their workflows. These challenges should ideally be led through peer to peer conversations managed by clinical risk and workflow experts from the vendor's team in order to encourage maximum co-operation with stakeholders from healthcare organisations.

This type of change management process can be facilitated as its own initiative through a benefits realisation study or under the supervision of a vendor's Clinical Safety Officer as part of a clinical risk management programme (as per NHS Digital standard SCCI0129). These are valuable methods that help to track and measure project management progress and outcomes while also enabling healthcare organisations to identify and implement best practices to reduce the impact on clinical productivity should network or information systems be affected.

Preserving Clinical Productivity

At AbedGraham we have been particularly vocal about the importance of managing human factors when managing technological change. In a previous white paper *"The Wachter Review: A Clinical Analysis"* we discussed the AbedGraham Transformation Curve, and highlighted how reducing dips in productivity during the implementation of new processes, is very much dependent on gaining a granular understanding of the people and workflows that are affected, (Figure 2).

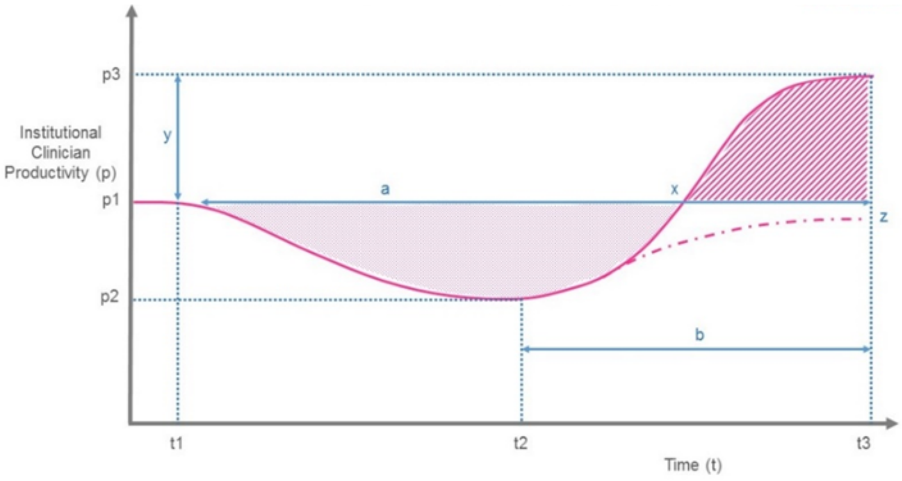

Figure 2: The AbedGraham Transformation Curve

This curve can also be used to interpret the drop in clinical productivity if a cyber event were to affect a hospital's network and information system. If a healthcare institution fails to implement strong contingency plans to maintain service delivery, the drop in clinical productivity can be steep, leading to a lower p2 over a short period of time (t2). The longer a hospital continues to function without technical and organisational back-up measures put in place by the vendor or healthcare institution, the longer clinical productivity will remain low (area under a-x) which leads to delayed clinical care, potentially patient harm and quantifiable operational losses.

On the other hand, strong contingency plans implemented by a vendor and healthcare organisation that seek to maintain service delivery in the event of IT system failure can lessen the drop in clinical productivity, (shallow p2). A vendor who is cognizant of a hospital's requirement to increased clinical productivity as quick as possible, (to p3), will help facilitate two main benefits:

1) Smaller area under a-x and therefore a reduced total time spent with low institutional clinical productivity

2) Rapid overcompensation and consequent increased clinical productivity in the hospital to balance the initial reduction in clinical care and lessen the long-term “hangover effect” of the institution suffering downtime

Ideally, contingency plans should be implemented within seconds to minutes by a vendor, with a quick or no dip in clinical productivity, enabling rapid overcorrection of increased clinical productivity with a return to baseline within minutes- hours.

Our Recommendations

With a view to maintaining service continuity within a hospital, the requirement in managing the security risk to network and information systems should be seen as a high priority, particularly with numerous authorities potentially able to impose financial sanctions on those who transgress UK/EU NIS.

It is AbedGraham’s view that with many health organisations already in growing financial difficulties, it is less likely that they will be targeted for further financial sanctions, and that penalties are more likely to be directed to the institutions that have more considerable resources available, thereby placing vendors at increased risk of being penalised, and being considered the responsible party for any regulation breaches. Therefore, in order to succeed in European public –sector healthcare, IT vendors must adapt accordingly by taking a proactive, clinically led consultative approach to risk management with their customers in order to turn this challenge into a competitive advantage in the market.

About AbedGraham

AbedGraham is Europe’s leading, exclusively clinically based, healthcare IT strategy, operations and risk consultancy. The organisation’s combination of clinical and strategic expertise is utilised by global IT infrastructure industry leaders to shape corporate strategies, clinical engagement and leadership initiatives, business case developments, major project bids and project management processes to maximise the positive impact of their solutions for healthcare providers. For more information, visit http://www.abedgraham.com or follow on Twitter at @AbedGraham.

Contact the Authors

Dr Roshan Vara BSc MBBS, Clinical Strategist, AbedGraham
E-mail: rvara@abedgraham.com

Dr Gabriel K Ma BSc MBBS, Clinical Strategist, AbedGraham
E-mail: gma@abedgraham.com