imprivata®

Supporting the Saudi Arabian NCA Essential Cybersecurity Controls

The Kingdom of Saudi Arabia's Vision 2030 aims at a comprehensive improvement of the nation, its security, economy, and citizens' well-being. One of the essential goals of Vision 2030 is continued transformation into the digital world and improvement of the digital infrastructure in order to keep up with the accelerated global progress in digital technology and services.

This digital transformation also requires maintaining and supporting the cybersecurity of the Kingdom, and, to that end, the National Cybersecurity Authority (NCA) developed the Essential Cybersecurity Controls (ECC-1: 2018) which define minimum requirements for national organisations.

Healthcare organisations, as providers of critical national services, must ensure that they are, and continue to be, compliant with the controls.

Imprivata solutions can be a vital element of a healthcare organisation's strategy to achieve compliance.

Security considerations

Cybersecurity is, of course, a very broad term that covers a wide range of areas including governance, policy and process, and technology. The overall focus of cybersecurity is to protect confidential data and systems and control the access to those systems and data. There are numerous solutions and strategies that can be implemented to deliver a high level of security. However, the weak link in any line of defence is often perceived to be the user.

A key question in approaching implementation of cybersecurity, therefore, is why is the user considered a weak link and what can be done to address this?

If one looks to other nations for guidance on the implications of higher security, some valuable insight can be found. For example, The UK National Cyber Security Centre (NCSC) makes the following observation:

"If a product has to be used in a particular way in order to be secure - but people cannot easily use it that way - the product is not secure in any meaningful sense."

This very concisely describes the challenges faced with introducing stronger security requirements either with technology or process.

Understanding users

Security is always a balance. In theory you can have a very high level of access security by implementing complex, frequently changing passwords on a per-system, per-user basis with multifactor authentication included. The reality of that approach is that users will become overburdened with the requirements, frequently forget access details, become frustrated with the technology, and find workarounds.

Whilst cybersecurity has become a necessity in the modern hospital and clinicians accept this, the repeated need to login and retype credentials to use these systems frequently becomes a source of frustration. This leads to unhappy users who do not leverage technology, and, at worst, circumvent security to remove this barrier. In fact, University College London (UCL) observe in their paper "Users aren't the Enemy:"

"Insecure work practices and low security motivation among users can be caused by security mechanisms and policy which take no account of users' work practices, organizational strategies and usability"

It should be remembered that clinicians come to work to care for and help patients, they want to be able to focus on their job and not be distracted by tasks they feel are unnecessary or that act as a barrier to this. In addition, placing barriers to the technology that clinicians need to do their jobs can impact on the care that they provide and in the worst case, potentially lead to adverse events.

Therefore, it is common to see workarounds such as:

- Generic accounts through which multiple users access EMR data
- Simple passwords
- Passwords written down and left by computers
- Leaving computers unlocked for anyone to access

These workarounds occur because implementation of policy and processes has not considered the impact on end users, so whilst the policies may mandate strong controls, that theoretically high level of access security is actually quite low. As UCL further observe:

"Unless security departments understand how the mechanisms they design are used in practice, there will remain the danger that mechanisms which look secure on paper fail in practice."

This inevitably leads to situations where data could be compromised and organisations non-compliant with the Cybersecurity Controls. Therefore, a balanced approach that considers the impact of controls, and mitigates any impact on end users, is the right way to approach achieving and maintaining compliance.

It should be remembered that clinicians come to work to care for and help patients, they want to be able to focus on their job and not be distracted by tasks they feel are unnecessary or that act as a barrier to this.

People will happily choose the more secure way if it's quick and straightforward, and allows them to accomplish their task.

A balanced approach

The balanced approach is to ensure cybersecurity policies are implemented in such a way as to not act as a barrier for clinicians but to ensure that only authorised users can access systems and data is protected.

In analysing the NCA Essential Cybersecurity Controls, section 2-2, "To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks," addresses the approach to identity and access management, specifically.

The cybersecurity requirements for identity and access management must include at least the following:

- **2-2-3-1** – User authentication based on username and password
- **2-2-3-2** – Multifactor authentication for remote access
- **2-2-3-3** – User authorization based on identity and access control principles: need-to-know and need-to-use, least privilege, and segregation of duties
- **2-2-3-4** – Privileged access management
- **2-2-3-5** – Periodic review of users' identities and access rights

In implementing these requirements, a hospital may consider things such as removing generic accounts, forcing complex password requirements, or other such technical controls combined with training to educate users on the necessity of security. These approaches have been observed in many hospitals to have a negative impact and lead to policy not being followed at the front line. Why may this happen? Because, as mentioned earlier, these approaches act as a barrier to the main function of clinicians, which is the care of patients.

So, how can a balanced approach be delivered, and how can policy be realised whilst not impacting on the care of patients? The UK NCSC suggest:

"...people will happily choose the more secure way if it's quick and straightforward, and allows them to accomplish their task."

Primarily understanding how implemented policies manifest themselves on the front line of care, and how they affect clinician's ability to treat patients, it can then be seen how effective a policy is. By seeing the impact of a particular policy decision, you can then understand how to refine it to be both effective and sympathetic to the clinical setting.

Once you understand the impact of policy, you can then look for solutions that help smooth that impact and allow you to be compliant not just on paper, but in reality, too.

The Imprivata solution

One of the key elements of the Cybersecurity Controls is access: usernames, passwords, permissions, and auditing. To be compliant with section 2-2 of the ECC, and to ensure adherence at the front line, Imprivata OneSign® ensures you can be compliant whilst ensuring streamlined, barrier free access for clinicians.

Imprivata OneSign directly addresses the challenges of compliance with NCA section 2-2-3-1 by allowing users to utilise something such as a door access card to access the computer, potentially in combination with a password or PIN to provide multifactor authentication.

Further, Imprivata OneSign then provides single sign-on (SSO) to all of the applications a user needs to access. In that way, all users can be compliant through use of a username and password (that is behind the badge tap) to access the computer along with any application they use. Users do not need to use group or shared accounts as the single sign-on component will remember their username and password, meaning that access to applications can be properly controlled using identity and access control principles. This helps ensure compliance with section 2-2-3-3 which requires “Need-to-know and Need-to-use, least privilege and segregation of duties.” Furthermore, Imprivata OneSign provides a full audit trail of access ensuring that the systems a user has access to are recorded. This supports the periodic review of user’s identities and access rights as required by section 2-2-3-5.

If any kind of data access happens outside of the four walls of the hospital, then remote access controls including dedicated multifactor authentication is required to be implemented according to section 2-2-3-2. Imprivata Confirm ID® for Remote Access supports multifactor authentication on remote devices, fully integrating with the wider Imprivata OneSign solution. Users can provide the second factor of authentication using a range of modalities including a mobile phone application. Once authenticated, users can continue to take advantage of SSO to access applications and resources within the internal network.

Another area that Imprivata solutions can address is data and information protection, section 2-7 of the ECC. It can be common to see desktop computers unlocked with confidential data visible on screen, often as a result of clinicians being called away to emergencies at short notice. Imprivata implements fade-to-lock functionality to automatically blank the screen after a short period of time before eventually moving to a full lock requiring username and password or strong authentication. This approach allows data to be protected whilst allowing the user immediate access if returning within the defined window. In addition, by utilising Imprivata OneSign, privacy and confidentiality of data can be further maintained as a result of stronger security and therefore fewer work arounds such as group accounts, generic passwords, or passwords that are written down. This helps to ensure compliance with section 2-7-3.

Imprivata OneSign ensures you can be compliant whilst ensuring streamlined, barrier free access for clinicians.

imprivata®

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience.

For further information please contact us at:

1 781 674 2700
or visit us online at
www.imprivata.com/intl

Offices in:

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

Extending beyond the desktop

Connected devices such as mobile and medical devices can open up opportunities for new workflows, allow access to patient data much closer to the point of care, and allow hospitals to move towards a paper free environment. This is particularly relevant as more hospitals strive to achieve the higher levels of HIMSS EMRAM accreditation, something that is only achievable by digitising a wider range of clinical workflows. As access to data extends beyond the traditional desktop/thin-client to these devices, the need for associated security becomes a necessity.

ECC incorporates mobile devices within its requirements, recognising the need to protect such devices in section 2-6. In regard to accessing these devices, section 2-6-3-2 specifies “Controlled and restricted use based on job requirements,” necessitating security to both the device and the applications that are used on it.

Additionally, in the case of mobile devices, providing every clinician with a permanent device is not a cost-effective approach and is often not required as devices are only needed whilst the user is at work. In looking at section 2-6-3-1, it requires “Separation and encryption of organization’s data and information stored on mobile devices and BYODs,” making it prohibitive to utilise personal (BYOD) devices within the clinical setting.

Thus, in the context of the hospital, shared devices are the most logical option. However, implementing any kind of security can potentially be a barrier to use.

It is in this space that Imprivata Mobile Device Access and Imprivata Medical Device Access can support compliance. By providing the same seamless access management and single sign-on to mobile platforms, users can access these devices securely and in compliance with the Controls.

Conclusion

Imprivata solutions are a key element for organisations looking to meet and maintain compliance with the Kingdom of Saudi Arabia’s Essential Cybersecurity Controls, reducing the challenges for hospital management in ensuring policies are being actively applied and adhered to by frontline staff. By freeing staff from the burden of time-consuming security processes and removing barriers that could lead to circumvention, potential breaches, incidents, or non-compliance can be avoided.

Imprivata solutions are designed for healthcare environments, they support the needs of clinicians in delivering high quality care whilst maintaining compliance with Cybersecurity controls and should be considered a primary tool in delivering this.

OS-WP-Saudi-ECC-INTL-ME-0919