imprivata®

Supporting the United Arab Emirates National Cybersecurity Strategy

The UAE's Vision 2021 aims to make the UAE one of the best countries in the world. In order to achieve this ambition, the UAE launched the National Agenda comprising a range of key performance indicators (KPIs), of which one of the key elements of that agenda is the National Cybersecurity Strategy. This strategy aims to create a safe and strong cyber infrastructure in the UAE that enables citizens to fulfil their aspirations and empowers businesses to thrive.

An important aspiration as part of this strategy is to protect critical information infrastructure assets of the UAE. Healthcare is categorised as one of the nine critical sectors.

The strategy will be achieved through a robust Critical Information Infrastructures Protection (CIIP) program:

- Identify critical sectors, assets, and associated risks
- Establish world-class risk management standards
- Implement robust processes for reporting, compliance, and response

Healthcare organisations, as providers of critical national services, must ensure that they are, and continue to be, compliant with any and all relevant standards. More specifically, healthcare organisations should be compliant with the Telecommunications Regulatory Authority (TRA) aeCERT Standard Information Security Policy.

Imprivata solutions can be a vital element of a healthcare organisation's strategy to achieve cybersecurity 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."[1]

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"[2]

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 "never events," which are "serious incidents that are wholly preventable."[3]

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

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.

1. UK National Cyber Security Centre - https://www.ncsc.gov.uk/blog-post/security-and-usability--you-can-have-it-all-
2. Users are not the enemy, UCL - http://discovery.ucl.ac.uk/20247/2/CACM%20FINAL.pdf
3. NHS Never Events policy and framework - https://improvement.nhs.uk/documents/2265/Revised_Never_Events_policy_and_framework_FINAL.pdf

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

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."[4]

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.

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 TRA aeCERT Standard Information Security Standards, section 3.2 Password Management Policy, "Passwords are a common form of verification and are considered the only barrier between a user and his/her personal information." addresses the approach to authentication. Specifically, the objectives of this policy are:

- Enforce adequate password controls in systems and user level
- Protect information and information assets related to the user
- Ensure that only authorized users can access certain information, applications, services, and systems
- Protect the Confidentiality, Integrity and Availability of information, systems, services, and applications within the organization's network

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:

4. Users are not the enemy, UCL - http://discovery.ucl.ac.uk/20247/2/CACM%20FINAL.pdf

"...people will happily choose the more secure way if it's quick and straightforward, and allows them to accomplish their task."[5]

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.

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

The Imprivata solution

One of the key elements of the cybersecurity standards is access: usernames, passwords, permissions, and auditing. To be compliant with the aeCERT section 3.2 Password Management Policy, and to ensure adherence at the front line, Imprivata digital identity solutions ensure you can be compliant whilst providing streamlined, barrier free access for clinicians.

Imprivata OneSign® directly addresses the challenges of compliance with this policy 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 the requirement "Protect the Confidentiality, Integrity and Availability of information, systems, services, and applications within the organization's network." 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 defined in section 3.19 User Access Management Policy.

Further enhancing this support of the requirements of section 3.19 is Imprivata Identity Governance, a solution which supports the full end-to-end management of users, their digital identities, and access permissions. Reviews of assigned rights, permissions, and access can be performed from a single dashboard in minimal steps and many of the processes around user management are automated making providing a powerful, efficient, and effective way to manage this.

5. UK NCSC - https://www.ncsc.gov.uk/blog-post/security-and-usability--you-can-have-it-all-

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.

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 3.10 Remote Access Policy. 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. 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 3.2, Screen Saver Password.

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.

The aeCERT Information Security Policy incorporates mobile devices within its requirements, recognising the need to protect such devices in section 3.12. In regard to accessing these devices, the section specifies “As technology and business demand moves forward, there has been an introduction of many devices that can be classed as Portable Media. The organization allows usage of these devices as part of normal business processes. However, care needs to be taken over their use, and of the data that they hold.” 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 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.

imprivata®

About Imprivata

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

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

However, implementing any kind of security can potentially be a barrier to use. It is in this space that Imprivata Mobile solutions and Imprivata Medical Device Access can support compliance.

Imprivata Mobile solutions provide a range of functionality to support the provisioning of devices, secure access for users, and SSO to applications they use on both the Android and iOS platforms. These solutions ensure data held or accessible on devices is secure and that devices and the data they hold can be securely wiped after each use. By providing the same seamless access management and SSO to mobile platforms, users can access these devices securely and in compliance with the Controls.

It is also becoming increasingly common to see medical devices such as vital signs monitors, infusion pumps, and dispensing cabinets being connected to the hospital network and having access to the systems and applications that store patient data. Imprivata Medical Device Access can secure those devices, requiring users to tap their badge to log in and access the device, thus protecting data. Whilst this workflow could be achieved using a username and password, the same problems with entering those time and time again present themselves, particularly as many of these devices have touch screen keyboards which can be frustrating for end users. This often results in devices that are configured with no access controls or generic user accounts that minimise security and auditing of usage, thus meaning non-compliance with security policies.

Conclusion

Imprivata solutions are a key element for organisations looking to meet and maintain compliance with the United Arab Emirates National Cybersecurity Standards, 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 standards and should be considered a primary tool in delivering this.

OS-WP-UAE-cybersecurity-INTL-ME-0520