Kayentis

Dedicated to eCOA and patient engagement

How complex authentication should be in eCOA devices?

kayentis · Wednesday, June 15th, 2016

Authentication is a requirement that can't be underestimated. It is key that user's identity is guaranteed, but daily usage should not be forgotten.
One should keep in mind these basic principles and follow a few simple security rules in order to safely simplify the eCOA end-user daily life.

The right balance between IT complexity requirements… and sticker on the desk!

Most common IT requirements consist in complicating authentication by adding lots of rules such as mix of letters, digits, symbols, upper/lower cases; frequent change rate; history of previously used passwords etc.
This is definitely a must for accessing critical apps, remote servers or VPN. But it becomes counterproductive if the eCOA user puts a sticker on his desk (or even on the device) with the password on it!

How to define the complexity level of authentication?

1. Consider user's behavior

As part of the security framework, authentication should be considered globally and not ignore user's behavior. Do unauthorized access prevention and patient identity recognition require the same complexity?

2. Create an easy-to-remember login

eCOA users will be more comfortable if they face reasonable efforts for remembering and managing their credentials.
For investigators, use of email or email's prefix as login is a great help.

For patients, login can be pre-populated and patient will focus on remembering a simple pin code.

3. Reinforce the security of the password

Each user should be able to recover and change their password or pin code easily and securely without external help. Use of secret question is part of the process.
Is an ultimate password complexity required for these users? A reasonable length and a mix of 2 or 3 types of characters is probably enough for investigators. And pin code prohibiting basic sequences or repetition is also sufficient for patient.
Forcing password change is a good practice that should be preserved. Delay is the appropriate criteria. In addition, revocation after a long period without usage is important considering users can recover on their own.

4. No concession against security breaks

On the other hand, no concession against risk of security break is allowed. The system should clearly inform in case of multiple failed attemps to log-in or recover passwords. An external support involvement should then be used to clear out risks prior to reenabling user's authentication. Each access should also be traced and monitored.

eCOA authentication can be guaranteed and investigator & patient burden reduced by managing properly authentication complexity.

Jean-Michel COMBE, VP R&D, Kayentis – June 16, 2016

This entry was posted on Wednesday, June 15th, 2016 at 12:09 pm and is filed under Data management, Insights
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.