HOW TO ENHANCE INFORMATION SECURITY IN HEALTHCARE

7 RECOMMENDATIONS AND GOOD PRACTICES
FOR HEALTHCARE ICT SERVICE PROVIDERS

AGENCE eSanté LUXEMBOURG
Agence nationale
des informations partagées
dans le domaine de la santé

eQualis
eHealth Qualification
for Interoperability & Security

LHC
Luxembourg House
of Cybersecurity

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy

COMMUNICATION
CRIME GUARD RISK SYSTEMS
FIREWALL
PASSWORD SAFE DATA
TECHNOLOGY
KEY RISK VIDEO
ACCESS ADWARE ATTACK BUSINESS CAMERA COMPUTER CRIME
PROTECTION
COMMUNICATION SECRET COMPUTER
SOFTWARE HACKER WORM
PRIVACY
ACCESS VIRUS CAMERA ONLINE
INTERNET IDENTITY
SURVEILLANCE
SYSTEM
ACCESS ADWARE ATTACK BUSINESS CAMERA
NETWORK
PRIVACY COMMUNICATION LOCK
COMMUNICATION
SYSTEM TECHNOLOGY TROJAN VIRUS
KEY
INTERNET DATA ACCESS PRIVACY RISK
PROTECTION

Healthcare data are highly sensitive data that demand to be processed in a secure and data protection compliant way. As a healthcare ICT service provider, you - and your ICT solution – are an essential part in the information security chain, together with the healthcare service providers.

In order to support you in that role throughout your interactions with the public healthcare system, Agence eSanté, the Ministry of the Economy and Securitymadein.lu have jointly developed this guideline with ***7 RECOMMANDATIONS*** *in the area of information security.*

The recommendations listed within this booklet are an excerpt and are based on the analysis of interviews with software development companies and IT-service providers. Find the content of this booklet and further information through this link or the QR-code on the last page.

1 ENCRYPTION

- ✓ Avoid managing the private keys of your clients and users to prevent loss, theft or misuse of keys. Managing the private keys of others could incur a liability risk in case of a dispute.
- ✓ Encrypt backups and data stored by your system or software in order to protect it against disclosure in an event of theft or loss and corruption, by using disk encryption software, file-system encryption or encrypted databases
- ✓ Use encryption for data in transit, by configuring encrypted connections
- ✓ Use a “state of the art” key length for your encryption algorithm, for symmetric algorithms min. 256 bit keys, for asymmetric cryptographic algorithms min. 2048 bits. Stay up-to-date with the latest recommendations in terms of key length, as increasing key length is important to ensure security of the encryption
- ✓ Consider using both symmetric and asymmetric encryption. In terms of choosing algorithms for symmetric and asymmetric encryption, check the most recent recommendations from the BSI

- ➔ You may support your customers on creating keys, but never deal with the private keys yourself
- ➔ Useful information and a comparison of disk encryption software can be found here
- ➔ Use https, up-to-date TLS and SFTP for encrypted data exchange
- ➔ For the latest recommendations related to key length for encryption, consider to check sites such as this one or these pages from the BSI

2 UPDATE AND PATCH MANAGEMENT

- ✓ Stay informed and apply necessary security patches to the operating system and application environment on your systems and the systems you manage for your customers. Whenever you install patches or security updates, you should use an account with the least privileges for the task of updating and patch management
- ✓ Automate software updates instead of relying on users to perform them, inform and warn your customers about the updates and schedule those to be performed outside normal business hours

- → Stay informed with latest developments and apply security patches regularly
- → Respect the least privileges recommendation
- → Consider enabling automatic updates outside working hours

3 REMOTE ACCESS TO USER WORKSTATIONS

- ✓ Consider data exfiltration risks when accessing remote computers. Always rely on the permission of the user, avoid permanent connections, and ensure logging and tracing of activities performed
- ✓ Always rely on the explicit permission of the user for each remote session
- ✓ Remote sessions for maintenance and support should be as short as possible
- ✓ Never ask for authentication data of your users, instead use your own credentials. Only if it is absolutely necessary to use another account, ask them to enter their credentials themselves
- ✓ Ensure that the remote access is removed by the user or automatically after the task is completed

4 PERSONAL DATA PROTECTION

- ✓ Keep in mind basic definitions:
  - o Personal data (DCP) are any information relating to an identified or identifiable natural person (Art 4.1 RGPD). Personal health data are covered by a special regime (Art 9.2 RGPD).
  - o Processing of personal data refers to any operation involving the handling of DCP (collection,sorting, consultation...). The processing of DCP and health DCP is regulated by a legal basis .
  - o A data controller is the entity that determines the purposes and means of the data processing. The joint controller represents another entity involved in the processing of DCP for its own purposes, so that it is decisive in determining the purposes and means of the processing.
  - o A processor is an entity that processes data on behalf of and under the instruction (by contract) of the data controller.
- ✓ No unnecessary processing of any personal data, to avoid potential data protection risks
- ✓ Do not store personal data unnecessarily, especially if it is medical data, to avoid data protection risks
- ✓ Clearly identify the role and function of those involved and communicate them with transparency
- ✓ Secure personal data processing and apply high physical, logical and organisational security measures

5 INCIDENT MANAGEMENT

- ✓ Set up a security incident handling process or procedure. Elements to be included are, beyond others:
  - o performing common steps to limit damage
  - o isolating the source of the incident
  - o taking recovery actions
  - o identifying whom to inform and when
  - o keeping a record of each incident and how it was managed
  - o learning from previous incidents so that they do not happen again

In case you are subject to an information security incident (attacks, malware, etc.) and require another expert point of view, you can always ask SecurityMadeInLuxembourg's CIRCL team for help (info@circl.lu).

6 RISK MANAGEMENT

- ✓ Review the maturity of your information security risk management
- ✓ Discover the actual weaknesses of your systems or software
- ✓ Good risk management involves preparation but also transparency towards your customers. In terms of transparency, you should ensure that the contracts with your customers define what are the responsibilities regarding the information security risks
- ✓ If you are able to list these risks, you should also list the actions that you have performed or will perform to deal with these risks, so that their impact is minimal. For a good risk management tool that comes for free, we can recommend MONARC

- ➔ You can use CASES's Fit4Cybersecurity or Fit4Privacy tools that are available for free to perform a self-assessment of your maturity in risk management
- ➔ Find out more here via the common vulnerability search offered by CIRCL
- ➔ Access the Cybersecurity Ecosystem directory offered by SecurityMadeinLuxembourg, in case you want to contact an expert to perform the scan for you
- ➔ Consider using MONARC as your risk management tool

7 SECURE DEVELOPMENT AND CODING PRINCIPLES

- ✓ Include password complexity and validity requirements
- ✓ Embed role-based access in your software
- ✓ Include strong encryption for data in transit and at rest
- ✓ Pay attention to the testing data set and the testing environment
- ✓ Be aware of and respect officially defined secure coding principles and perform code reviews
- ✓ Use source code management software
- ✓ Secure and encrypt backups of your source code
- ✓ Establish a proven and documented software development process
- ✓ Consider the good practices of security testing
- ✓ Stay away from deprecated libraries, programming languages and operating systems
- ✓ Avoid data transfers using unprotected or public wireless connections when your software is exchanging data with external machines or services
- ✓ Consider the use of modern programming languages that are supported by their vendors and by a large community and that are provided with regular updates and security patches

- ➔ Find more specific password complexity recommendations here or at NIST's password recommendations
- ➔ Apply secure coding principles, visit OWASP, M. Howard's "Writing Secure Code" reference, or G. McGraw's "Software Security: Building Security In" book
- ➔ Source code management software like GIT, Subversion etc. find more information here
- ➔ Lifecycle support for your Windows system, you can check this Microsoft page
- ➔ Click here for good cybersecurity practices

AGENCE eSanté LUXEMBOURG
Agence nationale
des informations partagées
dans le domaine de la santé

eQualis
eHealth Qualification
for Interoperability & Security

LHC
Luxembourg House
of Cybersecurity

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy

Questions or need assistance?

Contact Agence eSanté's eQualis team

E-mail: eQualis@esante.lu

More information?

Scan this code

https://gd.lu/3rQ56h