Ellymed BV (Labplusarts)

Statement of Applicability NEN:7510

October 2023

Classification: Public

Document name: Statement of Applicability NEN 7510
Date: October 2023
Distribution: Public

Document History

Version	Version Note	Date
1.0	First draft	10/2023

Contents

Introduction

This document contains the Statement of Applicability (hereinafter SoA) for the certification of the NEN7510:2017 standards. The purpose of this document is to identify the applicable control measures that must be implemented to monitor and manage the threats against the Elly med(Labplusarts) organization and business processes. The control measures have been identified on the basis of the management measures included in the NEN7510 standard. The applicability is declared per control measure. For each applicable control measure, a reference is made to the relevant defined security control. If a control measure does not apply, an explanation is given for this.

Management Statement

The management of EllyMed(Labplusarts) hereby declares that the measures mentioned in this SoA are validated in relation to the performed risk analyzes and accepts any residual risk of measures not taken.

The management hereby confirms that all measures selected in this document have actually been implemented.

Ali Naimi, Founder, CEO, and Developer, October 2023

Scope

Developing software, as well as blood tests for the healthcare sector.

Statement of Applicability

Table Clarification
Columns 1-3 show the description and reference to the NEN7510 controls.

Column “Reasons for selection” shows the reason why the control applies to Elly Med(LabplusArts) and can have the following values:

BR/BP: Business Requirements/adopted Best Practices
TBI: To Be Implemented
N/A: Not Applicable

The final column shows if a control is excluded.

Cause	Control Objectives NEN 7510	Status
5 **Security Policies**	A5.1.1 Organizations must have a written information security policy that is approved by management, published and then communicated to all employees and relevant external parties	Done
	A5.1.2 The information security policy should be subject to ongoing, phased reviews so that the entire policy is reviewed at least annually. The policy should be reviewed if a serious security incident has occurred.	Done
6 **Organization of information Security**	A6.1.1 Organizations should: a) clearly define and assign information security responsibilities b) have an information security management forum (IBMF) in place to ensure that there is clear direction and visible management support for security initiatives related to have on the security of health information, as described in B3 and B4 of Appendix B (6.1.1) in NEN 7510-2. At least one individual must be responsible for health information security within the organization. The health information security forum should meet regularly, monthly or near-monthly. (It is usually most effective if the forum meets at a time halfway between two meetings of the governing body to which the forum reports. This allows urgent matters to be addressed within a short period of time. appropriate meeting will be discussed.) A formal scope statement should be produced defining the boundary of compliance activities across people,	NA There is only one person in the company who works in the tech department

	processes, places, platforms and applications.	
	A6.1.2 Organizations should, where feasible, separate duties and areas of responsibility to reduce the opportunities for unauthorized modification or misuse of personal health information.	Done
	A6.1.2 Organizations should, where feasible, separate duties and areas of responsibility to reduce the opportunities for unauthorized modification or misuse of personal health information.	Done
	A6.1.3 Contact with authorities	TBI
	A6.1.4 Contact with special interest groups	TBI
	A6.1.5 Healthcare-specific control measure When managing projects, patient safety must be taken into account as a project risk for any project that involves the processing of personal health information.	Done
	A6.2.1 Mobile device policy	Done
	A6.2.2 Teleworking	Done
7 Human resource Security	A7.1 .1 Organizations must, as a minimum, verify the identity, current address and previous employment of staff and contractors and volunteers at the time of application. Background verification checks of all candidates for employment should include verification of applicable healthcare professional qualifications, where	Done

	there is accreditation to the profession based on those qualifications (e.g. doctors, nurses, etc.) If a person is hired for a specific security function, the organization must ensure that: a) the candidate has the necessary competence to fulfill the security function; b) the candidate can be entrusted with the position, especially if the position is crucial for the organization.	
	A7.1.2 All organizations whose staff are involved in the processing of personal health information must record that involvement in relevant job descriptions. Security roles and responsibilities, as defined in the organization's information security policy, should also be captured in relevant job descriptions. Special attention should be paid to the roles and responsibilities of temporary or short-term staff such as substitutes, students, trainees, etc.	NA
	A7.2.1 Management responsibilities	Done
	A7.2.2 Organizations that process personal health information should ensure that information security education and training is provided when inducting new employees and that regular updates to organizational security policies and procedures are provided to all employees and, where relevant, third parties contractors, researchers, students and volunteers who process personal health information. Employees of the organization and, where relevant, third party contractors should be made aware of disciplinary processes and consequences relating to information security breaches.	Done

	A7.2.3 Disciplinary process	Done
	A7.3.1 Termination or change of employment responsibilities	Done
8 **Asset management**	A8.1.1 Organizations that process personal health information must: a) Account for information assets (i.e. an inventory maintaining such assets); b) have designated an owner for these information assets (see 8.1.2); c) have rules for the acceptable use of these assets that are identified, documented and implemented.	Done
	A8.1.2 Ownership of assets	Done
	A8.1.3 Acceptable use of assets	Done
	A8.1.4 Return of assets; All employees and contractors must, upon termination of employment, return all personal health information in non-electronic form in their possession and ensure that all personal health information in electronic form in their possession is kept up to date on relevant systems and then securely erased from all devices where it was present.	Done
	A8.2.1 Organizations that process personal health information shall uniformly classify such data as confidential.	Done
	A8.2.2 All health information systems that process personal health information must alert users to the confidentiality of personal health information accessed from the system (e.g., at startup or login), and must label paper output as confidential if that output contains personal health information	NA

	A8.2.3 Handling of assets	Done
	A8.3.1 Media containing personal health information must be physically protected or its data must be encrypted. The status and location of media containing unencrypted personal health information should be monitored.	Done
	A8.3.2 All personal health information should be securely erased or the media destroyed when no longer required.	Done
	A8.3.3 Physical media transfer	NA
9 Access Control	A9.1.1 Organizations that process personal health information must control access to such information. In general, users of health information systems should limit their access to personal health information to situations: (a)where there is a healthcare relationship between the user and the person to whom the data relates (the client whose personal health information is being accessed); b) where the user carries out an activity on behalf of the person to whom the data relates; c) where specific data is needed to support this activity. Organizations that process personal health information should have an access control policy that governs access to this data. The organization's policy regarding access control should be established based on predefined roles with associated privileges appropriate to, but limited to, the needs of that role.	Done
	A9.1.2 Access to networks and network services	Done
	A9.2.1 Access to health information systems that process personal health information shall be subject to a	Done

	formal user registration process. Procedures for registering users must ensure that the required level of authentication of the claimed identity of users corresponds to the access level(s) that the user will have. User registration data should be reviewed regularly to ensure it is complete and accurate and that access continues to be required.	
	A9.2.2 User access provisioning	Done
	A9.2.3 Management of privileged access rights	Done
	A9.2.4 Management of secret authentication information of users	NA
	A9.2.6 All organizations that process personal health information shall, as soon as practicable after termination of employment or work as a contractor or volunteer, for any departing departmental or temporary employee, third party contractor or volunteer,access rights as users to such information to end.	Done
	A9.3.1 Use of secret authentication information	Done
	A9.4.1 Health information systems that personal one process health information, need the identity of users and this must be done through authentication where at least two factors are involved. Access to information functions and application systems associated with the processing of personal health information must be insulated be separated) from access to information processing infrastructure that no connection keeps processing Personal health information.	TBI
	A9.4.2 Secure log-on procedures	Done

	A9.4.3 Password management system	Done
	A9.4.4 Use of privileged utility programs	Done
	A9.4.5 Access control to program source code	Done
10 Cryptography	A10.1.1 Policy on the use of cryptographic controls	Done
	A10.1.2 Key management	TBI
11 Physical and Environmental Security	A11.1.1 Organizations that provide personal process health information, must use secure zones to protect areas that information processing facilities contain such health applications to support. This secured areas must be protected through appropriate management measures for physical access to ensure that only authorized personnel get access.	NA
	A11.1.2 Physical entry controls	Done
	A11.1.3 Securing offices, rooms and facilities	Done
	A11.1.4 Protecting against external and environmental threats	Done
	A11.1.5 Working in secure areas	Done
	A11.1.6 Delivery and loading areas	NA
	A11.2.1 Equipment siting and protection	Done
	A11.2.2 Supporting utilities	Done
	A11.2.3 Cabling security	NA
	A11.2.4 Equipment maintenance	Done
	A11.2.5 Organizations that provide equipment, data or software for it supporting a healthcare application with personal provide health information or	Done

	use, should not allow that equipment, data or software of the location will be deleted or there is or will be moved indoors without the organization having to do this has given approval.	
	A11.2.6 Organizations that provide personal process health information, must guarantee that any use outside their building medical devices that are used to record data or to report is authorized. This must include equipment used by remote workers are used,even where this use is permanent (i.e. where it is a core aspect of the employee's role, as is the case with ambulance staff, therapists etc.)	Done
	A11.2.7 Organizations that process health information must securely erase or destroy any media containing health information application software or personal health information when it is no longer required.	Done
	A11.2.8 Unattended user equipment	NA
	A11.2.9 Clear desk and clear screen policy	Done
12 Operations Security	A12.1.1 Documented operating procedures	TBI
	A12.1.2 Organizations that process personal health information shall manage changes to information processing facilities and systems that process personal health information through a formal and structured change management process to ensure appropriate control of host applications and systems and continuity of client care.	NA
	A12.1.3 Capacity management	NA

	A12.1.4 Organizations that process personal health information shall separate development and test environments for health information systems that process such information (physically or virtually) from operational environments where those health information systems are hosted. Rules for migrating software from development to an operational state should be defined and documented by the organization hosting the affected application(s).	Done
	A12.2.1 Organizations that process personal health information must implement appropriate prevention, detection and response management measures to protect against malicious software, and implement appropriate user awareness training.	Done
	A12.3.1 Organizations that process personal health information must back up all personal health information and store it in a physically secure environment to ensure its future availability. To protect its confidentiality, encrypted backups of personal health information must be made.	Done
	A12.4.1 Event logging	Done
	12.4.2 Audit reports must be secured and cannot be tampered with. Access to tools for auditing systems and audit trails must be secured to prevent misuse or compromise.	Done
	A12.4.3 Administrator and operator logs	TBI
	A12.4.4 Health information systems supporting time-critical shared care activities shall provide time synchronization services to support tracking and	NA

	reconstruction of activity timelines as required.	
	A12.5.1 Installation of software on operational systems	Done
	A12.6.1 Management of technical vulnerabilities	Done
	A12.6.2 Restriction on software installation	TBI
	A12.7.1 Information systems audit controls	Done
13 Communications security	A13.1.1 Network controls	Done
	A13.1.2 Security of network services	Done
	A13.2.3 Electronic messaging	Done
	A13.2.4 Organizations that process personal health information must have a confidentiality agreement that describes the confidential nature of this information. The agreement should apply to all personnel who have access to health information	Done
14 System acquisition, development and maintenance	A14.1.1 Information security requirements analysis and specification	Done
	A14.1.1.1 Uniquely identify care recipients; Health information systems that process personal health information must: a) ensure that each client can be uniquely identified within the system; b) be able to merge duplicate or multiple registrations if it is determined that more registrations have been inadvertently created for the same client, or during a medical emergency.	Done
	A14.1.1.2 Validation of output data; Health information systems that process Personal health information must provide personally identifying information that helps health care providers confirm that	Done

	the requested electronic health record corresponds to the client being treated.	
	A14.1.2 Securing application services on public networks	Done
	A14.1.3 Protecting application services transactions	Done
	A14.1.3.1 Publicly available health information; Publicly available health information (other than personal health information) must be archived. The integrity of publicly available health information should be protected to prevent unauthorized changes. The source (authorship) of public available health information should be mentioned and the its integrity must be protected.	Done
	A14.2.1 Secure development policy	Done
	A14.2.2 System change control procedures	Done
	A14.2.3 Technical review of applications after operating platform changes	Done
	A14.2.4 Restrictions on changes to software packages	Done
	A14.2.5 Secure system engineering principles	Done
	A14.2.6 Secure development environment	Done
	A14.2.7 Outsourced development	NA
	A14.2.8 System security testing	Done

	A14.2.9 Organizations that provide personal process health information, must establish acceptance criteria for planned new ones information systems, upgrades and new versions. Prior to acceptance they must test appropriately of the system.	Done
	A14.3.1 Protecting of test data	Done
15 Supplier relationships	A15.1.1 Organizations that process health information must consider the risks associated with access by third parties to these systems or data they contain, assess and then security controls implement it the identified risk level and the applied technologies fit.	Done
	A15.1.2 Addressing security within supplier agreements	NA
	A15.1.3 Information and communication technology supply chain	NA
	A15.2.1 Monitoring and review of supplier services	NA
	A15.2.2 Managing changes to supplier services	NA
16 Information security incident management	A16.1.1 Responsibilities and procedures	Done
	A16.1.2 Organizations that provide personal process health information, must have responsibilities and procedures related to it managing identify security incidents: a) to ensure an effective and timely response to information security incidents to bring about; b) to ensure that there is a effective and prioritized escalation path is for incidents so that in the right circumstances and in a timely manner profession possible are done on plans for crisis management and	Done

	business continuity management; c) incident-related audit reports and other collect and submit relevant evidence to stand firm.	
	A16.1.3 Reporting information security weaknesses	Done
	A16.1.4 Assessment of and decision on information security events	Done
	A16.1.5 Response to information security incidents	Done
	A16.1.6 Learning from information security incidents	Done
	A16.1.7 Collection of evidence	Done
17 Information security aspects or business continuity management	A17.1.1 Information security planning continuity	Done
	A17.1.2 Implementing information security continuity	Done
	A17.1.3 Verify, review and evaluate information security testing	Done
	A17.2.1 Availability of information processing facilities	Done
18 Compliance with legal requirements	A18.1.1 Identification of applicable legislation and contractual requirements	Done
	A18.1.2 Intellectual property rights	Done
	A18.1.3 Protection of records	Done
	A18.1.4 Organizations that provide personal health information process, the informed permission from manage clients. Wherever possible it should be informed	Done

	permission from clients are obtained before personal health information by email, fax or communicated by telephone or otherwise made known to parties outside the healthcare institution.	
	A18.1.5 Regulations of cryptography controls	Done
	A18.2.1 Independent review of information security	Done
	A18.2.2 Compliance with security policies and standards	Done
	A18.2.3 Technical compliance review	Done