Visma
Verzuim

Statement of Applicability
NEN 7510 Visma Verzuim B.V.

Author	Remco Koman | Information Security & Privacy Officer
Approved by	Information Security Committee
Version	1.1
Classification	Public

VISMA

Statement of Applicability

SoA details	
Company	Visma Verzuim B.V.
Last review	14-02-2023
Version	1.1
Norm	NEN 7510-1:2017+A1:2020
Purpose of this document	This document sets out which of the controls from the standard have been adopted and why any may have been excluded.
Management statement	The management of Visma Verzuim B.V. hereby declares that the measures stated in this SoA have been confirmed in relation to the assessments.
Scope of the SoA	Information security of customer information within development, hosting, maintenance, consultancy, sales and support for the Visma Verzuim B.V. Software as a Service products and information security of corporate information of Visma Verzuim B.V. itself in accordance with Statement of Applicability version 1.1 dated 14-02-2023. (Partly) Outsourced processes include: Physical security, Data center, ICT services.
Note	Some controls have a “-2” or “-3” added to the control number. For example “A.5.1.1-2 Policies for information security”. These controls are health specific.

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.5 Information Security Policies						
A.5.1 Management direction for information security	A.5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes	Required to define and execute the ISMS	No	Control implemented
	A.5.1.1-2 Policies for information security	Organizations must have a written information security policy adopted, approved by management, published and then communicated to all employees and relevant third parties.	Yes	Required to define and execute the ISMS	No	Control implemented
	A.5.1.2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes	Required to maintain the ISMS	No	Control implemented
	A.5.1.2-2 Review of the policies for information security	The information security policy must be subject to a continuous, phased review to ensure that the full policy is reviewed at least annually. The policy must be assessed if a serious security incident has occurred.	Yes	Required to maintain the ISMS	No	Control implemented
	Totals:		**4**			**4**

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.6 Organization of Information Security						
A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Yes	Risk assessment	No	Control implemented
	A.6.1.1-2 Information security roles and responsibilities	Organizations must have: ● Clear responsibilities in terms of defining and assigning information security. ● An Information Security Management Forum (IBMF) to ensure there is clear direction and visible support from management related to security initiatives on the security of health information, as described in B3 and B4 of Annex B (6.1.1) in NEN 7510-2. At least one individual must be responsible for the security of health information within the organization. The IBMF should meet on a regular, monthly or almost monthly basis. There should be a formal statement of scope produced defining the limit of compliance activities across people, processes, places, platforms and applications.	Yes	Required to maintain the ISMS	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	Yes	Risk assessment	No	Control implemented
	A.6.1.2-2 Segregation of duties	Organizations should, where feasible, have obligations and separate areas of responsibility in order to maximize opportunities minimizing unauthorized modification or misuse of personal health information.	Yes	Risk assessment	No	Control implemented
	A.6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Yes	Legal requirements	No	Control implemented
	A.6.1.4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	Risk assessment	No	Control implemented
	A.6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Yes	Risk assessment	No	Control implemented
	A.6.1.5-2 Information security in project management	Patient safety should be top priority in project management. Project risks are taken into account for each project that involves the processing of personal health information.	Yes	Risk assessment	No	Control implemented
	A.6.2.1 Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	Risk assessment	No	Control implemented
Section	Control	Control description	Control applicable	Justification	Outsourced	Control status

	A.6.2.2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes	Risk assessment	No	Control implemented
	Totals:		**10**			**10**
A.7 Human Resource Security						
A.7.1 Prior to employment	A.7.1.1 Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Risk assessment	No	Control implemented
	A.7.1.1-2 Screening	Organizations must at least verify the identity, current address and the previous employment of staff, contractors and volunteers during the job interview. Background verification checks of all candidates for a employment should include verification of the applicable qualifications for healthcare providers, if there is accreditation for the profession based on those qualifications (e.g. doctors, nurses staff etc.). If an individual is hired for a specific security role, the organization must ensure that: ● The candidate has the necessary competence to fulfill a security function.	Yes	Risk assessment	No	Control implemented

		● The candidate can be entrusted with the position, in particular if the function is crucial to the organization.				
	A.7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	Risk assessment	No	Control implemented
	A.7.1.2-2 Terms and conditions of employment	All organizations whose employees are involved in the processing of personal health information, must document involvement in relevant job descriptions. Security roles and responsibilities, as defined in the information security policy of the organization, should also be in relevant job descriptions described. Particular attention to the roles and employment such as substitutes, students, trainees, etc.	Yes	Risk assessment	No	Control implemented
A.7.2 During employment	A.7.2.1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Yes	Risk assessment	No	Control implemented
	A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	Risk assessment	No	Control implemented
Section	**Control**	**Control description**	**Control applicable**	**Justification**	**Outsourced**	**Control status**

	A.7.2.2-2 Information security awareness, education and training	Organizations that process personal health information must ensure that information security education and training are given at the introduction of new employees and that there are regular updates to organizational security policies and procedures provided to all employees and, where relevant, third party contractors, researchers, students and volunteers who have personal processing health information. Organizations employees and, where relevant, third party contractors regarding information security violations.	Yes	Risk assessment	No	Control implemented
	A.7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	Risk assessment	No	Control implemented
A.7.3 Termination and change of employment	A.7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	Risk assessment	No	Control implemented
	Totals:		**9**			**9**

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.8 Asset Management						
A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	Risk assessment	No	Control implemented
	A.8.1.1-2 Inventory of assets	Organizations that process personal health information must: ● Accountability for information assets (i.e. maintain an inventory of assets); ● Having designated owners for information assets (see 8.1.2); ● Having rules for the acceptable use of these assets that are identified, documented and implemented.	Yes	Risk assessment	No	Control implemented
	A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	Yes	Risk assessment	No	Control implemented
	A.8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.8.1.4-2 Return of assets	All employees and contractors must upon termination of their employment: ● Return all non-electronic personal health information ● Ensure that all electronic personal health information is updated on relevant systems and securely erased from all devices where it was present.	Yes	Risk assessment	No	Control implemented
A.8.2 Information classification	A.8.2.1 Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Yes	Risk assessment	No	Control implemented
	A.8.2.1-2 Classification of information	Organizations that process personal health information must uniformly classify such data as confidential.	Yes	Risk assessment	No	Control implemented
	A.8.2.2 Labeling of information	An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Risk assessment	No	Control implemented
	A.8.2.2-2 Labeling of information	All information systems that process personal health information, must inform users that the system contains confidential personal health information when access is granted to a user (e.g. at startup or login), and must label paper output as confidential in case that output contains personal health information.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Risk assessment	No	Control implemented
A.8.3 Media Handling	A.8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Yes	Risk assessment	No	Control implemented
	A.8.3.1-2 Management of removable media	Media containing personal health information must be physically protected or its data must be encrypted. The status and location of media that contains unencrypted personal health information must be monitored.	Yes	Risk assessment	No	Control implemented
	A.8.3.2 Disposal of media	Media shall be disposed of or destroyed securely when no longer required, using formal procedures.	Yes	Risk assessment	No	Control implemented
	A.8.3.2-2 Disposal of media	All personal health information must be securely erased or otherwise the media must be destroyed when no longer needed.	Yes	Risk assessment	No	Control implemented
	A.8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes	Risk assessment	No	Control implemented
	Totals:		**16**			**16**

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.9 Access Control						
A.9.1 Business requirements of access control	A.9.1.1 Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.9.1.1-2 Access control policy	Organizations that process personal health information must control access to such information. In general users of health information systems must limit their access to personal health information to situations: ● In which there is a care relationship between the user and the person to which the data relate (the client to whose personal health information is accessed); ● In which the user performs an activity on behalf of the person to which the data relate; ● Where specific data is required to perform support activities. Organizations that process personal health information must have an access control policy to ensure access control is arranged.	Yes	Risk assessment	No	Control implemented

		The organization's policy regarding access control must be determined based on predefined roles with associated powers consistent with, but limited to, the needs of that role. The access control policy (as part of the described in 5.1.1 information security policy framework) must reflect professional, ethical, legal and client-related requirements and the duties performed by caregivers and the workflow of the task must be taken into account. The organization must identify and document all parties with which client data is exchanged. With these parties contractual agreements must be agreed on access and rights prior to exchanging client data.				
	A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Yes	Risk assessment, contractual obligations	No	Control implemented
A.9.2 User access management	A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.9.2.1-2 User registration and de-registration	Access to health information systems that contain personal health information must be subject to a formal user registration process. Procedures for registering users must guarantee the required level of authentication of users' claimed identity matches the access level(s) that the user will have. The user registration data should be reviewed regularly to ensure the completeness, correctness and that access is still required.	Yes	Risk assessment	No	Control implemented
	A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes	Risk assessment	No	Control implemented
	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Yes	Risk assessment	No	Control implemented
	A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	Risk assessment	No	Control implemented
	A.9.2.6-2 Removal or adjustment of access rights	All organizations that process personal health information must revoke user access rights for each leaving (temporary) employee, third party contractor or volunteer as soon as possible after termination employment or work.	Yes	Risk assessment	No	Control implemented
A.9.3 User responsibilitie s	A.9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes	Risk assessment	No	Control implemented
A.9.4 System and application access control	A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.9.4.1-2 Personal information isolation	Health information systems that contain personal health information must determine the identity of users and must do so through authentication involving at least two factors. Access to information and applications related to processing personal health information must be isolated (and separated) from access to information and applications unrelated to processing personal health information.	Yes	Risk assessment	No	Control implemented
	A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes	Risk assessment	No	Control implemented
	A.9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	Risk assessment	No	Control implemented
	A.9.4.5 Access control to program source code	Access to program source code shall be restricted.	Yes	Risk assessment	No	Control implemented
	Totals:		**18**			**18**

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.10 Cryptography						
A.10.1 Cryptographic controls	A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Yes	Risk assessment / Contractual obligations	No	Control implemented
	A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	Risk assessment / Contractual obligations	No	Control implemented
	Totals:		**2**			**2**
A.11 Physical and Environmental Security						
A.11.1 Secure areas	A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes	Risk assessment / Contractual obligations	Partial	Control implemented
	A.11.1.1-2 Physical security perimeter	Organizations that process personal health information must use secure zones to protect areas that contain information processing facilities with health applications. These secure areas must be protected by appropriate control measures for physical access to ensure only authorized personnel get access.	Yes	Risk assessment / Contractual obligations	Partial	Control implemented
	A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes	Risk assessment / Contractual obligations	Partial	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Yes	Risk assessment / Contractual obligations	Partial	Control implemented
	A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attacks or accidents shall be designed and applied.	Yes	Risk assessment / Contractual obligations	Partial	Control implemented
	A.11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Yes	Risk assessment	Partial	Control implemented
	A.11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Yes	Risk assessment	Partial	Control implemented
A.11.2 Equipment	A.11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	Risk assessment	Partial	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.5-2 Removal of assets	Organizations that use equipment, data or software to support a healthcare application with personal health information, must not allow equipment, data or software to be removed off site, entered or be moved without the organization's consent and given approval.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.6-2 Security of equipment and assets off-premises	Organizations that process personal health information must guarantee any use of medical devices outside their building is authorized. This must include equipment used by remote workers, even if this use is permanent (i.e. where it is a core aspect of the role of the employee, as is the case with paramedics, therapists, etc.).	Yes	Risk assessment	Partial	Control implemented
	A.11.2.7 Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Risk assessment	Partial	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.11.2.7-2 Secure disposal or reuse of equipment	Organizations that process health information must securely erase or destroy all media with application software or personal health information when no longer needed.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Yes	Risk assessment	Partial	Control implemented
	A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Yes	Risk assessment	No	Control implemented
	Totals:		**19**			**19**
A.12 Operations Security						
A.12.1 Operational procedures and responsibility	A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Yes	Risk assessment	No	Control implemented
	A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.12.1.2-2 Change management	Organizations that process personal health information must process changes to information processing facilities and systems through a formal and structured change management process to ensure the proper control of host applications and systems and to ensure continuity of customer care.	Yes	Risk assessment	No	Control implemented
	A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	Risk assessment	Yes	Control implemented
	A.12.1.4 Separation of dev, test and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Yes	Risk assessment / Contractual obligations	No	Control implemented
	A.12.1.4-2 Separation of development, testing and operational environments	Organizations that process personal health information must separate development and test environments (physically or virtually) from operational environments where those health information systems are hosted. There are rules for migrating software from the development to an operational state and are defined and documented by the organization operating.	Yes	Risk assessment / Contractual obligations	No	Control implemented
A.12.2 Protection from malware	A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	Risk assessment / Contractual obligations	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.12.2.1-2 Controls against malware	Organizations that process personal health information must implement appropriate prevention, detection and response management measures to provide protection against malicious software and implement appropriate awareness training for users.	Yes	Risk assessment / Contractual obligations	No	Control implemented
A.12.3 Backup	A.12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	Risk assessment / Contractual obligations	Yes	Control implemented
	A.12.3.1-2 Backup storage	Organizations that process personal health information must store back ups in a physically secure environment in order to guarantee that the information will be available in the future. Encrypted backups should be made to protect their confidentiality of personal health information.	Yes	Risk assessment / Contractual obligations	Yes	Control implemented
A.12.4 Logging and monitoring	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes	Risk assessment, legal requirement	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.12.4.2-2 Protection of log information	Audit reports must be secure and cannot be manipulated. Access to tools for auditing systems and audit trails must be secured against misuse or compromise prevent.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	Risk assessment	Yes	Control implemented
	A.12.4.4 Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Yes	Risk assessment	Yes	Control implemented
	A.12.4.4-2 Clock synchronization	Health information systems that support time-critical (shared) activities must support in time synchronization services to trace and reconstruct the timelines for support activities where required.	Yes	Risk assessment	Yes	Control implemented
A.12.5 Control of operational software	A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Yes	Risk assessment	No	Control implemented
A.12.6 Technical vulnerability management	A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes	Risk assessment, contractual obligations	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Yes	Risk assessment	No	Control implemented
A.12.7 Information systems audit considerations	A.12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Yes	Risk assessment	No	Control implemented
	Totals:		**20**			**20**
A.13 Communications Security						
A.13.1 Network security management	A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Yes	Risk assessment	Yes	Control implemented
	A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes	Risk assessment	No	Control implemented
	A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Yes	Risk assessment	Yes	Control implemented
A.13.2 Information transfer	A.13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	Risk assessment	No	Control implemented

	A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	Risk assessment	No	Control implemented
	A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.13.2.4 Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.13.2.4-2 Confidentiality or nondisclosure	Organizations that process personal health information must have a confidentiality agreement in place in which the confidential nature of this information is described. The agreement must apply to all personnel that have access to health information.	Yes	Risk assessment, contractual obligations	No	Control implemented
	Totals:		**8**			**8**
A.14 System Acquisition, Development and Maintenance						
A.14.1 Security requirements of information systems	A.14.1.1 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.14.1.1-2 Information security requirements analysis and specification	Health information systems that process personal health information must: ● Ensure that each client can be identified within the system; ● Be able to merge duplicate or multiple registrations if it is determined that there are inadvertently more registrations for the same client created, or during a medical emergency.	Yes	Risk assessment	No	Control implemented
	A.14.1.1-3 Information security requirements analysis and specification	Health information systems that process personal health information must provide personal identification information that helps healthcare providers confirm that the requested electronic health record corresponds to the client being treated.	Yes	Risk assessment	No	Control implemented
	A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Yes	Risk assessment	No	Control implemented
	A.14.1.3 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.14.1.3-2 Protecting application services transactions	Publicly available health information (not being personal health information) must be archived. The integrity of publicly available health information must be protected to prevent unauthorized changes. The source (authorship) of publicly available health information must be reported and its integrity must be protected.	Yes	Risk assessment	No	Control implemented
A.14.2 Security in development and support processes	A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Yes	Risk assessment	No	Control implemented
	A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification		Control status
	A.14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes	Risk assessment	No	Control implemented
	A.14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.	Yes	Risk assessment	No	Control implemented
	A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Yes	Risk assessment	No	Control implemented
	A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.14.2.9-2 System acceptance testing	Organizations that process personal health information must establish acceptance criteria for planned new information systems, upgrades and new versions. Prior to acceptance they must perform appropriate tests of the system.	Yes	Risk assessment	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.14.3 Test data	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.	Yes	Risk assessment, contractual obligations	No	Control implemented
	Totals:		**17**			**17**
A.15 Supplier Relationships						
A.15.1 Information security in supplier relationships	A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.15.1.1-2 Information security policy for supplier relationships	Organizations that process health information must review and implement security controls related to access by third parties to systems associated with the identified risk level and applied technologies.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization's information.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Yes	Risk assessment, contractual obligations	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes	Risk assessment, contractual obligations	No	Control implemented
	Totals:		**6**			**6**
A.16 Information Security Incident Management						
A.16.1 Management of information security incidents and improvement	A.16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	Risk assessment, legal requirement	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.16.1.2-2 Reporting information security events	Organizations that process personal health information have responsibilities and procedures related to managing security incidents: • To ensure an effective and timely response to information security incidents; • To ensure that there is an effective and prioritized escalation path for incidents so that under the right conditions and timely appeal plans can be made for crisis management and business continuity management; • To collect and maintain incident related audit reports and other relevant evidence. Information security incidents include corruption or accidental disclosure of personal health information or health information systems becoming unavailable where this unavailability adversely affects or contributes to the care of clients adverse clinical events. Organizations must always inform the client if personal information is accidentally disclosed and health information has been made public.	Yes	Risk assessment, legal requirement	No	Control implemented

		Organizations must inform the client if unavailability of health information systems may have had a negative impact on the care delivery.				
	A.16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.16.1.6 Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	Risk assessment, legal requirement	No	Control implemented
	Totals:		**7**			**7**

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.17 Information Security Aspects of Business Continuity Management						
A.17.1 Information security continuity	A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes	Risk assessment	No	Control implemented
	A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes	Risk assessment, contractual obligations	No	Control implemented
	A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Yes	Risk assessment, contractual obligations	No	Control implemented
A.17.2 Redundancies	A.17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Risk assessment	No	Control implemented
	Totals:		**4**			**4**

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
A.18 Compliance						
A.18.1 Compliance with legal and contractual requirements	A.18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes	Risk assessment, legal requirement	No	Control implemented
	A.18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Yes	Legal requirement	No	Control implemented
	A.18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Yes	Legal requirement	No	Control implemented
	A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	Legal requirement	No	Control implemented
	A.18.1.4-2 Privacy and protection of personally identifiable information	Organizations that process personal health information must manage clients' consent.	Yes	Legal requirement	No	Control implemented

Section	Control	Control description	Control applicable	Justification	Outsourced	Control status
	A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Legal requirement	No	Control implemented
A.18.2 Information security reviews	A.18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Yes	Risk assessment	No	Control implemented
	A.18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Yes	Risk assessment	No	Control implemented
	A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Yes	Risk assessment	No	Control implemented
	Totals:		**9**			**9**