IPS • Statement of applicability NEN 7510
v 1.3 | 09-08-2017

Index: LR: Legal Requirements, **CO**: Contractual Obligations, **BR**: Business Requirements/Best Practice), **RRA**: Results of Risk Assessment

Nr.	Control objectives and controls NEN7510:2011	Applicable & Implemented Y/N	Substantation (when not applicable)	Reason of selection (see index) LR	CO	BR/BP	RRA
5	**Security Policy**						
5.1	**Information security policy**						
5.1.1	Information security policy document	Yes				■	
5.1.2	Review of the information security policy	Yes				■	
6	**Organization of the information security policy**						
6.1	**Internal organization**						
6.1.1	Management commitment to information security	Yes				■	
6.1.2	Information security coordination	Yes				■	
6.1.3	Allocation of information security responsibilities	Yes				■	■
6.1.4	Authorization process for information processing facilities	Yes				■	
6.1.5	Confidentiality agreements	Yes			■		
6.1.6	Contact with government authorities	Yes		■			
6.1.7	Contact with special interest groups	Yes				■	
6.1.8	Independent review of information security	Yes				■	
6.2	**External parties**						
6.2.1	Identification of risks related to external parties	Yes				■	■
6.2.2	Addressing security when dealing with customers	Yes				■	■
6.2.3	Addressing security in third party agreements	Yes			■		■
7	**Asset Management**						
7.1	**Responsibility for assets**						
7.1.1	Inventory of assets	Yes				■	■
7.1.2	Ownership of assets	Yes				■	
7.1.3	Acceptable use of assets	Yes				■	
7.2	**Information Classification**						
7.2.1	Classification guidelines	Yes				■	■
7.2.2	Information labelling and handling	Yes				■	■
8	**Human Resources Security**						
8.1	**Human resource security prior to employment**						
8.1.1	Roles and responsibilities	Yes				■	■
8.1.2	Screening	Yes					■
8.1.3	Terms and conditions of employment	Yes				■	■
8.2	**Human resource security during employment**						
8.2.1	Management responsibilities	Yes				■	
8.2.2	Information security awareness, education and training	Yes					■
8.2.3	Disciplinary process	Yes					■
8.3	**Termination or change of employment**						
8.3.1	Termination responsibilities	Yes					■
8.3.2	Return of assets	Yes				■	■
8.3.3	Removal of access rights	Yes					■
9	**Physical and Enviromental Security**						
9.1	**Secure areas**						
9.1.1	Physical security perimeter	Yes					■
9.1.2	Physical entry controls	Yes					■
9.1.3	Securing offices, rooms, and facilities	Yes					■
9.1.4	Protecting against external and environmental threats	Yes					■
9.1.5	Working in secure areas	Yes					■
9.1.6	Public access, delivery, and loading areas	No	IPS does not make use of a loading and unloading area.				
9.2	**Equipment security**						
9.2.1	Equipment siting and protection	Yes				■	
9.2.2	Supporting utilities	Yes					■
9.2.3	Cabling security	Yes				■	
9.2.4	Equipment maintenance	Yes					■
9.2.5	Security of equipment off-premises	Yes				■	■
9.2.6	Secure disposal or re-use of equipment	Yes					■
9.2.7	Removal of property	Yes					■
10	**Communications and Operations Management**						
10.1	**Operational procedures and responsibilities**						
10.1.1	Documented operating procedures	Yes				■	
10.1.2	Change management	Yes				■	
10.1.3	Segregation of duties	Yes				■	■
10.1.4	Separation of development, test and operational facilities	Yes					■
10.2	**Third party service delivery management**						
10.2.1	Service delivery	Yes			■	■	
10.2.2	Monitoring and review of third party services	Yes				■	
10.2.3	Managing changes to third party services	Yes				■	
10.3	**System planning and acceptance**						
10.3.1	Capacity management	Yes				■	
10.3.2	System acceptance	Yes				■	
10.4	**Protection against malicious and mobile code**						
10.4.1	Controls against malicious code	Yes					■
10.4.2	Controls against mobile code	Yes					■
10.5	**Back-up**						
10.5.1	Information back-up	Yes					■
10.6	**Network security management**						
10.6.1	Network controls	Yes					■
10.6.2	Security of network services	Yes					■
10.7	**Media handling**						
10.7.1	Management of removable media	No	Patient information at IPS are not available on removable media.				
10.7.2	Disposal of media	No	Patient information at IPS are not available on removable media.				
10.7.3	Information handling procedures	No	Patient information at IPS are not available on removable media.				
10.7.4	Security of system documentation	Yes				■	
10.8	**Exchange of information**						
10.8.1	Information exchange policies and procedures	Yes					■
10.8.2	Exchange agreements	Yes			■		■
10.8.3	Physical media in transit	No	Patient information at IPS are not available on removable media.				
10.8.4	Electronic messaging	Yes				■	■
10.8.5	Business information system	Yes					■
10.9	**Electronic commerce services**						
10.9.1	Electronic commerce	Yes				■	
10.9.2	On-line transactions	No	No transactions are taking place in the systems of IPS.				
10.9.3	Publicly available information	No	IPS processes no publicly available healthcare information.				

Nr.	Control objectives and controls NEN7510:2011	Applicable & Implemented Y/N	Substantation (when not applicable)	LR	CO	BR/BP	RRA
10.10	**Monitoring**						
10.10.1	Audit logging	Yes				■	
10.10.2	Monitoring system use	Yes				■	■
10.10.3	Protection of log information	Yes				■	
10.10.4	Administrator and operator logs	Yes				■	
10.10.5	Fault logging	Yes				■	
10.10.6	Clock synchronization	Yes				■	
11	**Access Control**						
11.1	**Business requirement for access control**						
11.1.1	Access control policy	Yes					■
11.2	**User access management**						
11.2.1	User registration	Yes				■	■
11.2.2	Privilege management	Yes				■	■
11.2.3	User password management	Yes				■	■
11.2.4	Review of user access rights	Yes				■	■
11.3	**User responsibilities**						
11.3.1	Password use	Yes				■	■
11.3.2	Unattended user equipment	Yes				■	■
11.3.3	Clear desk and clear screen policy	Yes				■	■
11.4	**Network access control**						
11.4.1	Policy on use of network services	Yes				■	■
11.4.2	User authentication for external connections	Yes				■	■
11.4.3	Equipment identification in networks	Yes				■	■
11.4.4	Remote diagnostic and configuration port protection	Yes				■	
11.4.5	Segregation in networks	Yes				■	■
11.4.6	Network connection control	Yes				■	■
11.4.7	Network routing control	Yes				■	■
11.5	**Operating system access control**						
11.5.1	Secure log-on procedures	Yes				■	■
11.5.2	User identification and authentication	Yes				■	■
11.5.3	Password management system	Yes				■	■
11.5.4	Use of system utilities	Yes				■	■
11.5.5	Session time-out	Yes				■	■
11.5.6	Limitation of connection time	Yes				■	■
11.6	**Application and information access control**						
11.6.1	Information access restriction	No	IPS does not perform the management of application systems of healtcare companies.				
11.6.2	Sensitive system isolation	Yes			■	■	■
11.7	**Mobile computing and teleworking**						
11.7.1	Mobile computing and communications	Yes					■
11.7.2	Teleworking	Yes					■
12	**Information Systems Aqcuisition, Development and Maintenance**						
12.1	**Security requirements for information systems**						
12.1.1	Security requirements analysis and specification	Yes				■	■
12.2	**Correct processing in applications**						
12.2.1	Input data validation	No	IPS does not perform the management of application systems of healtcare companies.				
12.2.2	Control of internal processing	No	IPS does not perform the management of application systems of healtcare companies.				
12.2.3	Message integrity	No	IPS does not perform the management of application systems of healtcare companies.				
12.2.4	Output data validation	No	IPS does not perform the management of application systems of healtcare companies.				
12.3	**Cryptographic controls**						
12.3.1	Policy on the use of cryptographic controls	Yes					■
12.3.2	Key management	Yes				■	
12.4	**Security of system files**						
12.4.1	Control of operational software	Yes				■	■
12.4.2	Protection of system test data	No	It is not possible to use patient data as test data.				
12.4.3	Access control to program source code	Yes			■	■	
12.5	**Security in development and support processes**						
12.5.1	Change control procedures	Yes				■	
12.5.2	Technical review of applications after operating system changes	Yes				■	
12.5.3	Restrictions on changes to software packages	Yes				■	
12.5.4	Information leakage	Yes			■	■	■
12.5.5	Outsourced software development	Yes				■	
12.6	**Technical Vulnerability Management**						
12.6.1	Control of technical vulnerabilities	Yes				■	
13	**Information Security Incident Management**						
13.1	**Reporting information security events and weaknesses**						
13.1.1	Reporting information security events	No	IPS can not report information security events to patients.				
13.1.2	Reporting security weaknesses	Yes				■	
13.2	**Management of information security incidents and improvements**						
13.2.1	Responsibilities and procedures	Yes				■	
13.2.2	Learning from information security incidents	Yes				■	
13.2.3	Collection of evidence	Yes				■	
14	**Business Continuity Management**						
14.1	**Information security aspects of business continuity management**						
14.1.1	Including information security in the business continuity management process	Yes				■	■
14.1.2	Business continuity and risk assessment	Yes				■	■
14.1.3	Developing and implementing continuity plans including information security	Yes				■	■
14.1.4	Business continuity planning framework	Yes				■	
14.1.5	Testing, maintaining and reassessing business continuity plans	Yes				■	■
15	**Compliance**						
15.1	**Compliance with legal requirements**						
15.1.1	Identification of applicable legislation	Yes		■			■
15.1.2	Intellectual property rights (IPR)	Yes		■			■
15.1.3	Protection of organizational records	Yes		■	■	■	■
15.1.4	Data protection and privacy of personal information	Yes		■	■		■
15.1.5	Prevention of misuse of information processing facilities	Yes		■			■
15.1.6	Regulation of cryptographic controls	Yes		■			■
15.2	**Compliance with security policies and standards, and technical compliance**						
15.2.1	Compliance with security policies and standards	Yes				■	
15.2.2	Technical compliance checking	Yes				■	
15.3	**Information systems audit considerations**						