ΚΟΙΝΟΠΡΑΞΙΑ: ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ ΚΑΙ ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ

Project Title:

Deployment of Generic Cross Border eHealth Services in Cyprus

Agreement number: INEA/CEF/ICT/A2015/11S1451

Action No: 2015-CY-IA-0095

Τίτλος: Annex TE 1 NCPeH CY Technical deliverable – Part B

Release: v2.0

Αρ. Αναφ. Φακέλου: ΠΚ/2018/05/03

Λευκωσία 24 Ιουλίου, 2020

Βασικές Πληροφορίες Έργου

Πληροφορίες Έργου	
Τίτλος Έργου	**NCPeH CY**
Κωδικός Έργου	***2015-CY-IA-0095***
Ιδιοκτήτης Έργου	**Εθνική** Αρχή Ηλεκτρονικής Υγείας
Στοιχεία Επικοινωνίας Συντονιστή έργου	Καθ. Κωνσταντίνος Παττίχης Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου, Λεωφόρος Πανεπιστημίου 1 Αγλαντζιά Λευκωσία 2109 ΚΥΠΡΟΣ (+357) 22892697 (+357) 22892701 pattichi@cs.ucy.ac.cy

Ιστορικό αναθεωρήσεων

Αριθμός Έκδοσης	Ημερομηνία	Συγγραφείς	Εκδότης	Σχόλια
1	24/07/2019	Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου Φλουρής Ταντελλές	UCY & MOH	Πρώτο προσχέδιο
2	24/07/2020	Ιωάννης Κωνσταντίνου Ζήνωνας Αντωνίου Φλουρής Ταντελλές	UCY & MOH	Τελική Έκδοση

Θεώρηση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Θεώρησης
Δρ Βάσος Σκουτέλλας	Συντονιστής ελέγχου ποιότητας παραδοτέων	07/10/2020

Έγκριση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Έγκρισης
Καθ. Χρίστος Σχίζας	Πρόεδρος Εθνικής Αρχής Ηλεκτρονική Υγείας	08/10/2020

Executive Summary – Part B

This document refers to the NCPeH CY Information Security Framework. The goal of this document is to provide the directives and standards that have been implemented for the information security domain for the NCPeH CY system.

This document covers the following sections:

- B.1. Introduction
- B.2 Security Policy and Asset Classification Policy
- B.3. Access Control Policy
- B.4. Communications & Operations Policy
- B.5. Information System Acquisition, Development and Maintenance Policy
- B.6. Security Incident Management Policy
- B.7. Business Continuity Management Policy
- B.8. Human Resources Policy
- B.9. Physical and Environmental Security Policy
- B.10. IT Security Standard and Web Application Security Standard
- B.11. eHDSI Security Policies
- B.12. Public Key Infrastructure
- B.13. Backup Procedures and Policies

Furthermore, Annex IS 1 Information Security Policy and Procedures covers the Cyprus Government Information Systems Strategy and the corresponding policy and procedures followed for the NCPeH CY system implementation.

Table of Contents

B.1. Introduction

This document refers to the NCPeH CY Information Security Framework. The goal of this document is to provide the directives and standards that have been implemented for the information security domain for the NCPeH CY system. These directives and standards were adopted mainly from the Cyprus Government Information Systems Strategy to cover specifically the needs and implementations of the NCPeH CY system and infrastructure.

B.2 Security Policy and Asset Classification Policy

B.2.1 Security Policy

The Security Policy defines the following elements:

- approach to reach the required level of security for the NCPeH CY system;
- management and staff responsibilities regarding information security to ensure confidentiality, integrity and availability of information processed by NCPeH CY;
- a set of security policy statements governing the security goals of the governmental body operating the NCPeH CY.

The policies and the directions for all the above are documented in detail in the document "1 Annex IS 1 Information Security Policy and Procedures" section SUP.MR.PERS.1 - Recruitment Controls page 12, in section SUP.MR.PERS.2 - On-going Personnel Security page 18, in section SUP.MR.GOV.1 - Security Organizational Structure and Responsibilities page 65, in section SUP.MR.GOV.3 - Security Policy Characteristics and Accessibility page 73 and in section SUP.MR.GOV.4 - Security Culture, Awareness and Training page 77.

B.2.2 Asset Classification Policy

The Asset Classification Policy ensures that all NCPeH CY system information assets were/are identified, and an inventory of all-important assets is maintained. In addition, NCPeH CY system information is classified to indicate the need, priorities, and expected degree of protection.

The policies and the directions for all these are documented in detail in the document "1 Annex IS 1 Information Security Policy and Procedures" in section SUP.CGR1 - Asset Identification and Valuation page 98.

B.3. Access Control Policy

The Access Control Policy ensures implementation of controls for safeguarding and protecting access to the NCPeH CY system and its components and limiting the access only to those users or software applications that have a legitimate need to be granted access.

The policies and the directions for these are documented in detail in the document “1 Annex IS 1 Information Security Policy and Procedures” in section SUP.MR.PHS.1-A - Physical Security Zones page 27 and in SUP.MR.PHS.1-B - Application of Access Control page 37.

B.4. Communications & Operations Policy

The Communications & Operations Policy covers key areas in the NCPeH CY system's day-to-day IT operations management. It focuses on operational procedures and responsibilities, service delivery, system planning, back-ups, media handling, exchanges of information and monitoring. It aims to ensure the correct and secure operation of NCPeH CY system information processing facilities.

The policies and the directions for the above are documented in detail in document “1 Annex IS 1 Information Security Policy and Procedures” in section SUP.MR.GOV.6 - Security Incidents Handling page 88, in section SUP.MR.INFOSEC.2-G - Backup and Recovery page 142, in section SUP.MR.INFOSEC.3-B - E-mail and Communication Activities Security page 155, in section SUP.MR.PHS.1-E - Secure Mobile Storage and Storage of Waste page 60 and in section SUP.MR.INFOSEC.2-E - Portable Computing page 128.

B.5. Information System Acquisition, Development and Maintenance Policy

This Policy ensures that information security is an integral part of information systems across the entire NCPeH CY system. It establishes the NCPeH CY system security practices during information system acquisition, development and maintenance, to prevent errors, loss, unauthorized modification or misuse of information.

The policies and the directions for the above are documented in detail in document “1 Annex IS 1 Information Security Policy and Procedures” in section SUP.MR.GOV.6 - Security Incidents Handling page 88, in section SUP.MR.INFOSEC.2-G - Backup and Recovery page 142, in section SUP.MR.INFOSEC.3-B - E-mail and Communication Activities Security page 155, in section SUP.MR.PHS.1-E - Secure Mobile Storage and Storage of Waste page 60, in section SUP.MR.INFOSEC.2-E - Portable Computing page 128 and in section B 11 of current document.

B.6. Security Incident Management Policy

This Policy aims to determine requirements and directions to ensure that events not complying with NCPeH CY Security Policy or its normal functioning are effectively addressed to re-establish secure operation and management of the system.

The policies and the directions for the above are documented in document in the Annex OP 1 Service Operation Plan, Section 3.4 Incident and Problem Management and Section 3.2 Emergency Changes Procedure.

B.7. Business Continuity Management Policy

This Policy mainly aims to establish adequate levels of prevention and resilience in NCPeH CY services to mitigate the impact of a potential disaster or other disruptions to business continuity (“disruption”).

The policies and the procedures for these are documented in the Annex OP 7 Business Continuity Procedures NCPeH.

B.8. Human Resources Policy

This Policy defines the security requirements for human resources. It aims to ensure that employees and contractors understand their responsibilities and obligations regarding the NCPeH CY security perspective.

The policies and the directions for these are documented in “1 Annex IS 1 Information Security Policy and Procedures” in section SUP.MR.PERS.1 - Recruitment Controls and SUP.MR.PERS.2 – On-going Personnel Security.

B.9. Physical and Environmental Security Policy

This Policy defines the security requirements to ensure the implementation of controls to secure the environment and the physical premises where the NCPeH CY system IT infrastructure and equipment are hosted.

The policies and the directions for these are documented in “1 Annex IS 1 Information Security Policy and Procedures” in section SUP.MR.PHS.1-A - Physical Security Zones page 27.

B.10. IT Security Standard and Web Application Security Standard

B.10.1 Coverage

NCPeH National Application development based on IT Security Standard – Web Application Security Standard of European Commission C(2018) 7283[1]. According to this standard information security is applied at all three layers of the platform: Application Layer, Host Layer and Network Layer. This approach is shown below:

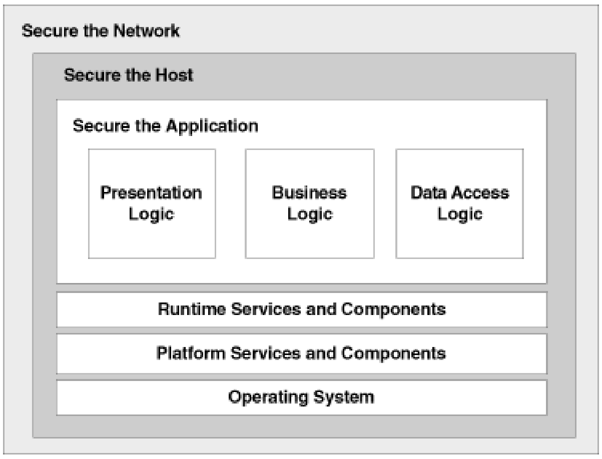

Figure 1: NCPeH CY Information Security Layers

This security standard covers the design, development and deployment of a web application. It establishes principles that developers should respect over the different phases of the web application lifecycle. Certain requirements have been suggested as recommended, and compliance with them may be evaluated on a case-by-case basis, based on risk assessment. Mandatory requirements, however, apply to any web application, regardless of its exposure, nature, functionalities or published information.

B.10.2. Definitions

Term	Description
Anomaly Detection	Technique used to identify unpredicted or expected behavior.
Data	Data anonymization is a type of information sanitization whose

[1] https://ec.europa.eu/transparency/regdoc/rep/3/2018/EN/C-2018-7283-F1-EN-MAIN-PART-1.PDF

Anonymization	intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Content Management System	Software program or a set of related programs that are used to manage the structure and the design of digital content.
Cross Site Request Forgery	Attack where a malicious third-party website visited by the victim executes unwanted actions on the web application where the victim is currently authenticated to.
HTTP Strict Transport Security	Opt-in security enhancement that is specified by a web application using a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.
Perfect Forward Secrecy	Property of secure communication protocols in which compromises of long-term keys do not compromise past session keys.
Pseudonymization	Pseudonymization is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.
Sensitive non-classified Information	Information defined in the Commission Decision (EU, Euratom) 2015/443 that the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof.
Strong Authentication	Authentication based on the use of two or more independent authenticators as defined in the Password Technical Specification and Access Control and Authentication Standard.
Web Application Framework	Software framework designed to support the development of web applications including web services, web resources, and web APIs. Web application frameworks provide a standard way to build and deploy web applications. Web frameworks aim to automate the overhead associated with common activities performed in web development and provide a certain level of security by embedding and enforcing security mechanisms.
Web-Facing	Any system that is directly accessible from the Internet.
Session ID	Unique identifier that a website assigns to a specific user for some

	predetermined duration of time, or session, to keep track of visitor activity.

B.10.3. General Requirements

Adequate security practices adoption in the design, development and implementation of a web application are necessary to ensure it is secure by design.

S/N	Requirement	Implementation
1.	A risk assessment **shall** be conducted by the System Owner, in accordance with an IT Risk Management Methodology approved by the European Commission and its outcome (and any other relevant constituent) shall be part of the relevant Security Plan.	Mandatory
2.	A new web application **shall** use a robust and recognized development framework.	Mandatory
3.	The development team **should** use a development framework recommended by DIGIT.	Recommended
4.	A maintained version of the framework **shall** be used; by default, this should be the latest stable version of the framework.	Mandatory
5.	Unsupported or deprecated client-side technologies **shall not** be used.	Mandatory
6.	All client-side technologies not natively supported by browsers **shall** not be used.	Mandatory

B.10.4. Authentication

Authentication mechanisms prevent access by unauthorized users as well as leakage of information that could enable an unauthorized user to gain access.

B.10.4.1. Use of mutualized authentication services

S/N	Requirement	Implementation

7.	Web applications **should** use ARIADNI CY Login to enforce authentication with a strength that satisfies the risk analysis and/or the required level of security.	Recommended

B.10.4.2. Implement authentication controls to protect sensitive non-classified information.

S/N	Requirement	Implementation
9.	Web applications handling sensitive non-classified information **shall** use CY Login to enforce authentication with a strength that satisfies the risk analysis and/or the required level of security.	Mandatory
10.	Administration pages of an application containing sensitive non-classified information **shall** have stricter security requirements which may justify the need for a re-authentication and/or for a stronger authentication.	Mandatory
11.	Sensitive non-classified information, such as incorrect passwords, in case of failed login attempts, **shall** not be stored.	Mandatory

B.10.4.3. Protect privileged functionalities

S/N	Requirement	Implementation
12.	Administrator functionality and/or interfaces **shall not** be accessible to unauthorized users.	Mandatory
13.	Administration functionality and/or interfaces **shall not** be accessible from the Internet except for specific source IP addresses.	Mandatory
14.	Administration interfaces accessible from Internet **should** use a random path instead of the default path (e.g. /admin_7e63b9c132).	Recommended
15.	Default accounts **shall** be disabled.	Mandatory
16.	Administrators **shall** have a separate user and administrator role. Privileged functionalities **shall** only be available when the administrator is active.	Mandatory

B.10.4.4. Sanitize authentication error messages

S/N	Requirement	Implementation
17.	Information provided in authentication error messages **shall not** reveal technical details about the underlying security mechanisms.	Mandatory
18.	Information provided in authentication error messages **shall not** provide information about the existence of an account on the application.	Mandatory

B.10.4.5. Securely store and transmit credentials

S/N	Requirement	User Centric
19.	Security secrets used by the web application itself (e.g. passwords, API keys, encryption keys, etc.) **shall not** be included in the source code or online repositories so that if the source code is leaked these secrets do not become public.	Mandatory
20.	User passwords used to authenticate **shall** be stored in a secure way, being at least hashed using a strong cryptographic hash function[2] and the passwords **shall** be salted per user before hashing.	Mandatory
21.	Authentication controls **shall** be checked on the server side.	Mandatory
22.	Credentials used to authenticate **shall** be sent over HTTPS.	Mandatory

B.10.4.6. Protect renewal of credentials

S/N	Requirement	Implementation
23.	Modification of a user's credential **shall** require the user to enter the old password, new password and a confirmation of the new password. The password change functionality **shall** be accessible only by a secured logged-in session.	Mandatory
24.	Account/password recovery controls **should** make use of a time-based one-time authentication token. The validity period shall be based on the business needs with a max of 24h validity.	Recommended

25.	Initial credentials for the users of the application **shall** be unique and the users to modify their initial credentials.	Mandatory
26.	Recovery tokens and initial **should** be delivered over an encrypted side-channel to the affected users	Recommended

B.10.5. Session Management

Session IDs are protected both in storage and in transport to prevent account takeover through session ID exposure or predictability.

B.10.5.1. Session IDs

S/N	Requirement	Implementation
27.	Session IDs **shall** be unique and contain at least 128 bits of entropy so that brute-forcing or guessing the session ID of an authenticated user is not feasible.	Mandatory
28.	Session IDs contents (or value) **shall not** contain meaningful data like username or e-mail address and other user's personal information.	Mandatory
29.	Sessions IDs **shall** never be displayed in URLs, logs, and error messages.	Mandatory
30.	Session IDs stored in cookies **shall** have the "Secure" flag set to prevent the browser from sending the cookie over an unsecured channel.	Mandatory
31.	Session IDs stored in cookies **should** have the domain attribute blank to avoid that the cookie is also sent to subdomains.	Recommended
32.	Session IDs stored in cookies **shall** have the path attribute set to the web directory path of the application that needs to receive the cookie rather than the root directory.	Mandatory
33.	Session IDs stored in cookies **shall** have the "HttpOnly" flag set, thus making it impossible for an attacker to access this cookie by client-side APIs such as JavaScript.	Mandatory

34.	Web application **shall** only accept cookies as a means for session ID exchange management and shall ensure that no other exchange mechanism is possible.	Mandatory

B.10.5.2. Session lifecycle

S/N	Requirement	Implementation
35.	Sessions **shall** be automatically terminated on the serve no longer active for a specified amount of time r when a user is	Mandatory
36.	Session idle timeouts **should** be no longer than 5 minutes for applications handling sensitive non-classified information and 30 minutes for the rest of the applications depending on a risk assessment	Recommended
37.	Sessions **shall** be automatically terminated when the user logs out of the web application.	Mandatory
38.	Sessions **shall** be automatically terminated on the client when the user closes the browser, by creating cookies without an expiration date	Mandatory
39.	Successful authentications **shall** generate a new session and therefore a new session ID.	Mandatory
40.	Web applications **shall** use the session management features implementation from the selected web development framework, rather than building such mechanism from scratch.	Mandatory

B.10.6. Access Control

Access control is used to allow access to those resources which are appropriate to that entity's identity and to prevent the intentional or unintentional execution of unauthorized actions in the application.

B.10.6.1. Enforce access controle

S/N	Requirement	Implementation
41.	Access control checks performed at client-side **shall** also be checked at server-side.	Mandatory

42.	Directory listing and browsing **shall** be disabled.	Mandatory
43.	File or directory metadata in the web applications **shall** be sanitized.	Mandatory
44.	The web application **shall** make use of anti-Cross Site Request Forgery (CSRF) tokens to prevent the user from executing unwanted actions on the web application they are currently authenticated to.	Mandatory

B.10.6.2. Minimize privileges

S/N	Requirement	Implementation
45.	All user accounts and resources (such as processes) **shall** only have the lowest level of rights needed to perform their tasks.	Mandatory
46.	Unapproved self-registered accounts **shall not** be allowed to post any public contents.	Mandatory
47.	Accounts supporting automated application functionalities **should** prevent interactive login, making it impossible to use these accounts for non-automated operations	Recemented

B.10.7. Input Validation & output sanitization

All input and output are handled securely to prevent any adverse effects when processed or rendered by the application.

B.10.7.1. Input validation checks

NCPeH CY system checks for dual input or for other input checks (e.g. limiting fields to specific ranges of input data) must be implemented to detect errors as: out-of-range values, invalid characters in data fields, missing or incomplete data, unauthorised or inconsistent control data, etc.

S/N	Requirement	Implementation
48.	Input validation controls **shall** be implemented for every web application which allows a user to input data.	Mandatory

49.	Input validation **shall** be performed at server-side.	Mandatory
50.	Input validation **should** also be performed at client-side in addition to server-side checks.	Mandatory
51.	Free text or numerical input fields must be replaced by enumerated whitelists where possible	Mandatory
52.	The system must incorporate validation checks in business rules, to avoid errors or inconsistencies in multiple routines	Mandatory
53.	Transactions which fail such checks must either be: rejected with a notification of the rejection sent to the submitter; corrected and resubmitted; or suspended pending further investigation	Mandatory
54.	Data validation must be performed at the server level to protect against malicious data coming from compromised clients	Mandatory

B.10.7.2. Prevent injection attacks

S/N	Requirement	Implementation
55.	The web application and all its backend services **shall** make use of a safe API that allows the use of a parameterized interface.	Mandatory
56.	If a parameterized API is not available, special characters **shall** be escaped using the specific escape syntax for that interpreter.	Mandatory

B.10.7.3. Render content safely

S/N	Requirement	Implementation
57.	Web applications **shall** use development frameworks mechanisms for rendering content safely and escaping reserved characters.	Mandatory

B.10.7.4. Input validation checks

Control of internal processing

Appropriate controls must be identified for the system to mitigate risks during internal processing. Architectural decisions on the functionality and implementation of these controls must be documented. The design and implementation of the system must ensure that the risks of processing failures leading to a loss of integrity are minimized;

Validation checks must be incorporated into System and related applications to detect any corruption of information through processing errors or deliberate acts. This must include:

S/N	Requirement	Implementation
58.	Validating check digits in numerical fields;	Mandatory
59.	Validation of system-generated data including checking whether values calculated by the system are within expected ranges	Mandatory
60.	Checks on the integrity, authenticity of data downloaded/uploaded and verifying hash totals of records and files;	Recemented
61.	Free text or numerical input fields must be replaced by enumerated whitelists where possible	Mandatory
62.	The system must incorporate validation checks in business rules, to avoid errors or inconsistencies in multiple routines	Mandatory
63.	Checks to ensure that system processes are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved;	Mandatory
64.	Handling exceptions with meaningful error codes or messages preventing blocking situation and allowing debugging.	Mandatory

B.10.7.5. Message integrity

Controls must be applied to ensure the authenticity and integrity of NCPeH CY messages;

S/N	Requirement	Implementation
65.	Integrity checks must be performed on all such transmissions to ensure that the information has not been accidentally or deliberately corrupted;	Mandatory

66.	Issues detected through message integrity checks must include data modification, substitution or replay, or incomplete data;	Mandatory
67.	If integrity issues are detected, the system must log errors and take appropriate action, such as ignoring the system message; requesting the data again; informing the system admin;	Recommended
68.	Different types of message integrity controls must be employed to ensure different levels of assurance, including checksums or check digits; message digests or hashes; and digital signatures;	Mandatory
69.	Encryption methods used to maintain the integrity of information must be in line with the Certificate & Cryptographic Key Management Standard.	Mandatory

B.10.7.6. Output data validation

All system output must be validated to ensure that the data is correct and appropriate for the given circumstances. This may be through by:

S/N	Requirement	Implementation
70.	Plausibility checks to test whether the output data is reasonable;	Mandatory
71.	Reconciliation control counts to ensure processing of all data;	Mandatory
72.	Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;	Recommended
73.	Procedures for responding to output validation tests;	Mandatory
74.	Defining the responsibilities of all personnel involved in the data output process;	Mandatory
75.	Creating a log of activities in the data output validation process.	Mandatory

The system must only output data that is in line with the access privileges of an individual or information system requesting the data.

B.10.8. Communications

All communication between the client and the web server is protected to prevent modification or disclosure of sensitive non-classified information.

B.10.8.1. Secure traffic

S/N	Requirement	Implementation
76.	Communication between applications and underlying services **should** be encrypted.	Mandatory
77.	Communication of sensitive non-classified information between applications and underlying services **shall** be encrypted.	Mandatory
78.	Web application **shall** make use of encrypted traffic for the entire web session on every web page including content from third party domains, in compliance with the SSL/TLS Technical Standard.	Mandatory
79.	All sensitive non-classified information **shall** be kept out of the URL.	Mandatory
80.	The HTTP Strict Transport Security (HSTS) header **shall** be set on all requests and for all subdomains.	Mandatory
81.	The HSTS header **should** be pre-loaded into browsers with a long max- age flag (ideally one year).	Mandatory

B.10.8.2. Certificates

S/N	Requirement	Implementation
82.	Strong, non-deprecated algorithms, ciphers and protocols **shall** be used throughout the whole certificate hierarchy.	Mandatory
83.	Web facing applications **shall** use certificates delivered by a trusted Certificate Authority.	Mandatory
84.	Perfect Forward Secrecy **shall** be supported.	Mandatory

B.10.8.3. HTTP Secure Configuration

S/N	Requirement	Implementation
85.	The web application **shall** only accept the standard HTTP request methods (e.g. GET, POST). Other protocols or methods shall be blocked.	Mandatory
86.	All HTTP responses **shall** contain a Content-Type header with the correct MIME type	Mandatory
87.	HTTP headers **shall not** disclose version or any other internal information about the underlying system or technology	Mandatory
88.	Content Security Policy (CSP) header **shall** be used and strictly configured to prevent injections such as XSS or HTML injection	Mandatory
89.	The X-XSS-Protection header **shall** be used to protect against reflected XSS attacks.	Mandatory
90.	The X-Frame-Options header **shall** be used to protect against clickjacking attacks	Mandatory

B.10.9. Data Protection

Data is handled securely by the application to prevent leakage of data, including of sensitive non-classified information.

S/N	Requirement	Implementation
91.	Forms handling sensitive non-classified information **shall not** make use of autocomplete features for those fields of information and **shall** disable client-side caching.	Mandatory
92.	When filling out forms, sensitive non-classified information **should** be masked while typed. (e.g. *****)	Recommended
93.	Data stored in client-side cache **shall not** contain any sensitive non- classified information.	Mandatory
94.	Sensitive non-classified information **shall** only be sent over HTTPS.	Mandatory

95.	All sensitive non-classified information maintained in memory **should** be overwritten with zeros or random data once it is no longer necessary to be kept in memory	Recommended

B.10.10. Secure Handling of Resource

Input and content provided by the user is handled safely by the application to prevent application failure, data leakage or abuse of its functionalities.

S/N	Requirement	Implementation
96.	Data (e.g. files, variables) submitted by a user to the web application **shall not** be used as input for operating system commands.	Mandatory
97.	Files uploaded by users **shall not** be stored under the web directory (webroot) of the webserver.	Mandatory
98.	Uploaded files **shall** be scanned by antivirus software.	Mandatory
99.	The web application **shall not** execute files uploaded by the user.	Mandatory
100.	All URL redirects **shall** be validated at the input time.	Mandatory
101.	If URL redirects based on a pre-defined list (e.g. whitelist) of allowed domain is not possible, a warning **shall** be shown firstly to the users notifying them that they are going off of the site, and a link shall be clicked by them for confirmation.	Mandatory

B.10.11. Error & Exception Handling

Error messages must not contain information that can be used to compromise the application or reveal sensitive non-classified information.

S/N	Requirement	Implementation
102.	Information provided in error messages **shall** be generic: it shall not reveal technical details about the underlying security or any other system internal mechanisms, except for a unique identifier which can be used in troubleshooting.	Mandatory

B.10.12. Logging

Logging is the act of keeping records of events that occur in an operating system or software applications. Logging enables anomaly detection as well as investigation and response to incidents.

S/N	Requirement	Implementation
103.	The web application **shall** log all necessary information (e.g. access control decisions) needed to begin a thorough investigation.	Mandatory
104.	Authentication attempts, both successful and failed, **shall** be logged.	Mandatory
105.	Access to sensitive non-classified information **shall** be logged.	Mandatory
106.	Changes to web application configuration, including changes to privileges assigned to users and security parametrization, **shall** be logged.	Mandatory
107.	Logs **shall not** include sensitive non-classified information.	Mandatory
108.	Logs **shall not** be accessible to unauthorized users.	Mandatory
109.	Controls **shall** be in place to prevent that logs are overwritten or tampered with.	Mandatory

B.10.13. Host & Network Security

Host and network supporting the application have to be secure to prevent host-level attacks and network-level attacks resulting in a compromise of the application through the host. As far as the network is concerned, this section describes a high-level approach for the network security. Network Security Standard provides more in-depth details.

B.10.13.1. Host Security on Premise or in Private Cloud

All hosts shall be configured based on hardened security baselines reflecting best security configuration practices.

S/N	Requirement	Implementation
110.	Communication between components (e.g. web application server - database server) **shall** require an authenticated connection, using an account with the least privileges necessary to operate.	Mandatory
111.	The application and all underlying components and middleware **shall** run with minimal privileges and **shall** not use (default) administration accounts shipped with systems.	Mandatory
112.	All hosts and software supporting the web application **shall** be updated timely after publication of security patches.	Mandatory
113.	All hosts and software supporting the web application **should** be updated timely after publication of functional patches	Recommended
114.	All management platforms that allow interaction with the hosts and software supporting the web application – including cloud consoles or similar management platforms – **shall** adhere to at least the same set of requirements as the actual web application and its supporting software	Mandatory
115.	Access to such management platforms **shall** be considered as privileged access, and the accounts for this **shall** adhere to applicable requirements of the Password Technical Specification and the Access Control and Authentication Standard	Mandatory
116.	Cloud Service Providers **shall** be able to support all the security requirements applicable to the web application	Mandatory

B.10.13.2. Network Security

S/N	Requirement	Implementation
117.	External facing web applications **shall** be deployed in demilitarized zone (DMZ) to permit only limited connectivity to specific hosts in the internal network, reducing the attack surface.	Mandatory
118.	External facing web application containing sensitive non-classified information **shall** be protected by a Web Application Firewall.	Mandatory

B.10.14. Deployment

Proper security testing prior to implementation in production prevents the deployment of vulnerable applications. Development releases should be digitally signed by the development team to ensure there is no modification after the final acceptance and waiting for deploying in the production environment.

B.10.14.1. Debug mode

S/N	Requirement	Implementation
119.	Debug mode **shall** be disabled in production.	Mandatory

B.10.14.2. Acceptance and Security Testing

S/N	Requirement	Implementation
120.	For web applications handling, sensitive non-classified information, pseudonymization and/or anonymization of data **shall** be assured in the test environments.	Mandatory
121.	For web applications handling sensitive non-classified information, pseudonymization and/or anonymization of data **should** be assured in the acceptance environments.	Recommended
122.	In accordance with the priority levels as described in IT Vulnerability Management Security Standard every web application **shall** undergo regularly a web application vulnerability assessment to identify common vulnerabilities.	Mandatory
123.	Important vulnerabilities based on a vulnerability assessment **shall** be fixed prior to going into production.	Mandatory
124.	If the web application handles sensitive non-classified information, a penetration test **should** be executed to find vulnerabilities in the web application.	Recommended
125.	Test environments **shall not** be publicly accessible.	Mandatory

B.11. eHDSI Security Policies[2]

B.11.1. SR1: Data flows must be adequately protected, as specified in international standards.

Data flows protected according to the policies descripted in section B.10.8 Communication security standard. Specifically, NCPeH system has three different data zones.

1. **Portal Zone:** There is an encrypted channel using SSL mechanism that ensures users' identification, authentication and authorization.
2. **Application zone** is directly connected with Data Zone within the same datacenter, on the same rack. These zones of the NCPeH CY system are inside the protected environment of the governmental network as depicted in the figure 1 below.
3. **TESTA Zone** is installed within the Governmental Network and is directly connected with other TESTA NCP Healthcare Providers. Moreover, through firewall TESTA Zone communicates with Patient Summary A, ePrescription and eDispense Zone for purposes where Cyprus is acting a country A.

Furthermore, data flows diagrams are descripted in Annex TE 1 NCPeH CY Technical deliverable Part A Section A.5 Data Flows Description.

B.11.2. SR2: End users must be clearly identified by national infrastructure before being able to enter the system.

Users are clearly identified by national infrastructure. There are two ways of Authentication depending to the way the end users access the system.

Access NCPeH CY inside Governmental Network:

[2] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Section+I+-+Security+Policies?preview=/37752833/110494996/eHDSI_Section_I-Security_Policies_v3.0.0_OR.pdf

End users are authenticated from NCP Active directory which has been deployed, maintained and supported by the NCPeH CY team. The procedures for end user registration is described in Annex OP 2 Operations and Organisational Structure, Appendices I and II.

Access NCPeH CY from the internet:

There are 3 steps for end users' authentication from the internet:

Step 1: 2 way SSL. End user must install a client certificate issued from UCY. The user obtains this certificate during her/his registration. Without this certificate the user will not be able to access the NCPeH CY portal.

Step 2: Ariandi authentication. End user must be authenticated through the national authentication gateway (SSO) Ariadni.

Step 3: NCP Active Directory authentication and authorization. The user is identified and authorized according to his/her role that is registered to the NCPeH active directory.

For more information please refer to Annex TE 1 NCPeH CY Technical deliverable – PART A, Sections A3.a.i and A3.a.ii

B.11.3. SR3: Mutual authentication between End Users and the national infrastructure's identity providers is needed when connecting to the system.

Access NCPeH CY from the internet:

There are 3 steps for end users' authentication from the internet:

Step 1: 2 way SSL. End user must install a client certificate issued from UCY. The user obtains this certificate during her/his registration. Without this certificate will not be able to access the NCPeH CY portal.

Step 2: Ariandi authentication. End user must be authenticated through the national authentication gateway (SSO) Ariadni.

Step 3: NCP Active Directory authentication and authorization. The user is identified and authorized according to his/her role that is registered to the NCP active directory.

For more information please refer to Annex TE 1 NCPeH CY Technical deliverable – PART A, Sections A3.a.i and A3.a.ii

B.11.4. SR4: End user identification and authentication procedures in place must have been audited according to the security audit policy.

End user identification and authentication audit procedures are described in Annex TE 1 NCPeH CY Technical deliverable Part A in section A4 System Components Description paragraph d. Audit Trail Service.

B.11.5. SR5: The security audit policy must be implemented. The types of security audit procedures to be applied are defined by eHOMB

To ensure the registration of all activities, every NCP event is logged and the following events referring to the Data Exchanges of eHealth DSI Architecture are recorded:

- HP Authentication
- Patient Identification and Authentication
- HP Authorization
- Medical data Query and Retrieve
- Medical Data Update (Dispensation notification)

All these events are logged independently for the result (successful or not) of the corresponding action.

Moreover, the NCP secure audit system logs the following system and network infrastructure events:

- NCP / Security Service startup/shut down;
- Usage of secure Audit log (other than audit log record creation);
- Access policy change (ie. Network, file system);
- User account event (ie. Create account);
- Configuration changes;
- Partial failure;
- PKI event;

- Timing synchronization;
- Authentication (NCP, Technical Staff) failure and success.

Audit police is described in Annex TE 1 NCPeH CY Technical deliverable Part A in section A4 System Components Description paragraph d. Audit Trail Service.

B.11.6. SR6: Mutual Authentication between national contact point providers (NCPs) of different countries is needed, when initiating a trans-European (cross border) information flow.

Mutual authentication is established between different countries:

1. Inside TESTA network: Point to Point connection with other TESTAng EU NCPs
2. Two-way SSL is enabled in NCP-A Server which is responsible for connecting to national infrastructure.

Secure Communication between other NCPeHs is descripted in Annex TE 1 NCPeH CY Technical Deliverable Section 4 System Components Description paragraph f National Contact Point Subparagraph vi Secure Communication with other NCPeH.

B.11.7. SR7: Non-repudiation procedures must be implemented between the User-Originator and the User-Receiver of documents and messages.

Non-reputation procedures are descripted in Annex TE 1 NCPeH CY Technical Deliverable section A4. System Components Description paragraph f National Contact Point, subparagraph vii OpenNCP Audits, 2 Non-Repudiation audits.

B.11.8. SR8: All eHealth DSI actors in a Country B must ensure that any medical document is forwarded only to the user that has been authorized to access the document.

1. See SR2 above

2. All requests, for medical documents, from NCP-B are initiated from users who are authorized to access these documents, thereby ensuring that any medical document is forwarded only to the user that has been authorized to access the document.

There are specific permissions (epSOS EED SAML Binding) assigned to logged in users to be able to assess what is permitted:

PHYSICIAN PERMISSIONS: PRD-006, PRD-003, PRD-004, PRD-005, PRD-010, PRD-016, PPD-032, PPD-033P. These permissions are defined in OpenNCP Properties

B.11.9. SR9: The software used to implement the NCP gateway must conform to the technical specifications of eHealth DSI architecture and common components.

NCP gateway is described in Annex TE 1 NCPeH CY Technical deliverable Part A in section A4 System Components Description paragraph f. National Gateway.

B.12. Public Key Infrastructure

UCY has implement a Public Key Infrastructure (PKI) which is managed centrally by a framework which distributes, maintains, and revokes public keys to verify end users and build trust between end users in public zone and NCPeH CY system. This PKI consists of hardware, software, peopleware and procedures which implement and enforce the following concepts/services/components:

- Digital certificates: association between a public key and identity in NCPeH CY system (National portal and their users). It contains algorithms to compute digital signature, and validity period to prove Identity authenticity;
- Organizational Certificate Authorities CA checks to verify information provided by the requester of digital certificate and signs the certificate with its private key for distribution to users;
- Certificate Factory procedure creates Certificates based on the information received the Certificate Authority Service. This Factory produces the CRL's.
- Revocation Authority: a service which authorized parties can request the revocation of certificates and which verified revocation requests to the certificate authority service.
- Certificate Revocation List CRL: an instrument for checking the continued validity of certificate for which the CA has responsibility.

B.13. Backup Procedures and Policies

NCPeH CY team haσ implement backup procedures and policies for securing NCPeH system from failures and disasters. Specifically

- There are 4 physical servers (with hyper V for virtualization)
- Production environment deployed on three physical servers (see figure 2 NCP 1, NCP 2, NCP 3) in High Availability configuration.
- The 4th physical server is running the testing environment (see figure 2 NCP 4).
- There is a Sinology (https://www.synology.com) Primary NAS which has Nakivo backup software installed, (https://www.nakivo.com/). Nakivo makes backup VMs every 6 hours.
- Backups are stored in Primary NAS and every 24 hours are transferred to a secondary NAS which is installed in another building (1 km away)

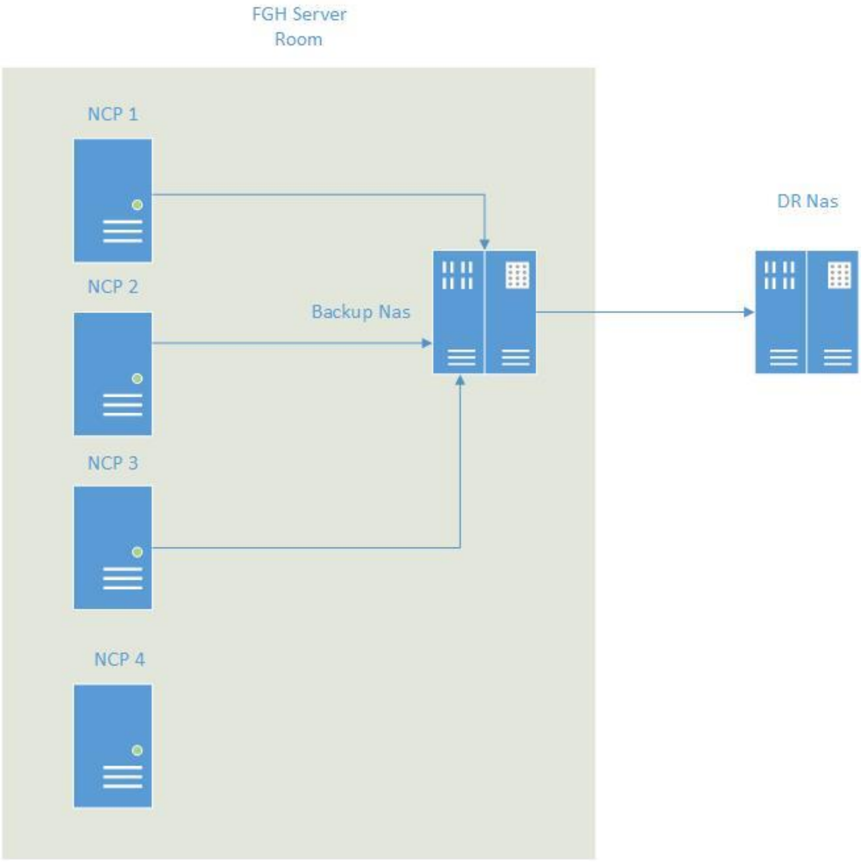

Figure 2: Backup procedures and policies

B.13.1 Backup Scenarios

B.13.1.1 Scenario 1. Failure in one physical server

NCPeH CY production environment is deployed in a High Availability setup and configurations in two physical servers. If one of the three servers have a problem NCPeH CY system will be continuously working.

B.13.1.2 Scenario 2. Failure in two physical servers

NCPeH CY production environment is deployed in three physical servers. If two servers have failure, the NCPeH CY system will be deployed in one server based on the latest VMs backups stored in Primary NAS and will recover.

B.13.1.3 Scenario 3. Fire in Ammochostos Hospital

NCPeH CY production environment is destroyed from fire. NCPeH is stored in secondary NAS and will be recovered when hardware will be available.