

# “ MyHealth@EU”

## User Guide for Physicians



<https://www.neha.org.cy>



Χρηματοδοτείται από  
την Ευρωπαϊκή Ένωση  
NextGenerationEU



**Η υγεία μου @ ΕΕ**  
Υποδομή ψηφιακών υπηρεσιών ηλεκτρονικής υγείας  
για υπηρεσία της Ευρωπαϊκής Ένωσης

**Κύπρος — το αύριο**

ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ ΚΑΙ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ

This guide is intended for Healthcare Professionals, and specifically for physicians who use the National Contact Point for eHealth Portal, in order to access the Cross-Border eHealth Services.

## Table of Contents

Index Image .....	3
Use of the NCPeH Portal .....	5
Main Steps: .....	5
User Registration / Two-Factor Authentication.....	5
Access Management .....	15
Access to the National Contact Point.....	23
Provision of Services by Physicians.....	24
Patient Summary .....	24
Creation of a Patient Summary (PS).....	24
Retrieval of the Patient Summary of an EU Patient/Citizen - Patient Summary B (PS B) .....	30
ePrescription .....	33
Frequently Asked Questions (FAQ) .....	36
Frequently Asked Questions for Doctors Practicing in Cyprus.....	36
Do doctors in the destination country automatically have access to the patient’s health data? Do doctors need to report or inform that their patient is traveling? .....	36
In which language should I write the electronic prescription?.....	36
What information is included in the Patient Summary? .....	37
Frequently Asked Questions for Doctors Practicing in Another EU Country .....	38
How can I verify the identity of a European patient before accessing their Patient Summary?.....	38
How can I access the Patient Summary of a European patient?.....	38
In which language will the Patient Summary be accessible? What if it is in a language the doctor does not speak and the patient needs urgent care?.....	39
What happens when a patient is in an emergency and urgent medical care is needed, but their health data are not up to date? Who is responsible? .....	39
How will a foreign patient pay for the healthcare received?.....	39

# Index Image

Figure 1:National Contact Point for eHealth Portal.....	5
Figure 2: Login to the Provider’s Portal.....	6
Figure 3: CY Login. Please enter your credentials. ....	7
Figure 4:Official Government Website.....	7
Figure 5: Guidelines for new users .....	8
Figure 6: Instructions for Creating a «Cy Login» Account. ....	9
Figure 7: Access Management – “User Roles” & “Digital Certificate Issuance” .....	9
Figure 8:CY Login page. How to enable Two-Factor Authentication.....	11
Figure 9: CY Login page. Send a verification code to a valid phone number.....	12
Figure 10: CY Login page. Enter the 6-digit code you received on your phone.....	12
Figure 11: CY Login page. Choose an authentication method. ....	12
Figure 12: CY Login page. Configure Authenticator.....	13
Figure 13 : CY Login page. Two-factor authentication enabled. ....	13
Figure 14 : CY Login page. Choose a backup method. ....	14
Figure 15: CY Login page. Change or disable Two-factor authentication.....	14
Figure 16: Selecting “Providers’ Portal”.....	15
Figure 17: Selecting a Digital Certificate. ....	16
Figure 18: Provider Portal Login Screen .....	16
Figure 19: Login Interface for Healthcare Professionals on the Registry Portal.....	17
Figure 20: Instructions for Installing the Digital Certificate for Cross-Border eHealth Services .	17
Figure 21: Generating a New Digital Certificate .....	18
Figure 22: Delivery of the Digital Certificate Installation Code to the User’s Mobile Device via SMS.....	18
Figure 23: Digital Certificate Successfully Downloaded .....	18
Figure 24: Selection of the Installation Guide Based on the User’s Operating System .....	19
Figure 25: Digital Certificate Successfully Installed.....	21
Figure 26: Digital Certificate Installation Failed.....	22
Figure 27: National Contact Point Portal – Home Page Select “National Citizen” or “European Citizen.” .....	23
Figure 28: First Entry of Citizen Data for Patient Summary Creation or Electronic Prescription Issuance.....	25
Figure 29: Searching for a patient requires the physician or pharmacist to input the identity card number and date of birth. ....	25

Figure 30: Input of the One-Time Password (OTP).....	25
Figure 31: Menu of Cross-Border Electronic Health Services .....	26
Figure 32: Patient Summary Preview.....	26
Figure 33: Physician’s Declaration of Acceptance for the Legal Issuance of the Patient Summary Health Record.....	26
Figure 34: Creating/Editing the Patient Summary Health Record .....	27
Figure 35: Confirmation of the “Save” Action .....	27
Figure 36: Selection of the "European Citizen" button .....	30
Figure 37: Selection of the European Citizen’s Country Eligible for Cross-Border Services. ....	31
Figure 38: Enter the European Citizen Identification Method. ....	31
Figure 39: Patient Summary .....	32
Figure 40: New Electronic Prescription.....	33
Figure 41: Electronic Prescriptions History. ....	34

# Use of the NCPeH Portal

## Main Steps:

If the user has a verified profile on Cy Login and has enabled two-factor authentication (2FA), they can log in directly to the NCPeH portal. In all other cases, the user is considered new and must follow the steps outlined below.

## User Registration / Two-Factor Authentication

After logging into the Government Internet Security Gateway (Gov.cy), select “Health” from the list of e-Services. You will then see the option “Electronic Cross-Border Healthcare Services.”

By selecting this option, you will be directed to the platform National Contact Point for eHealth (NCPeH).

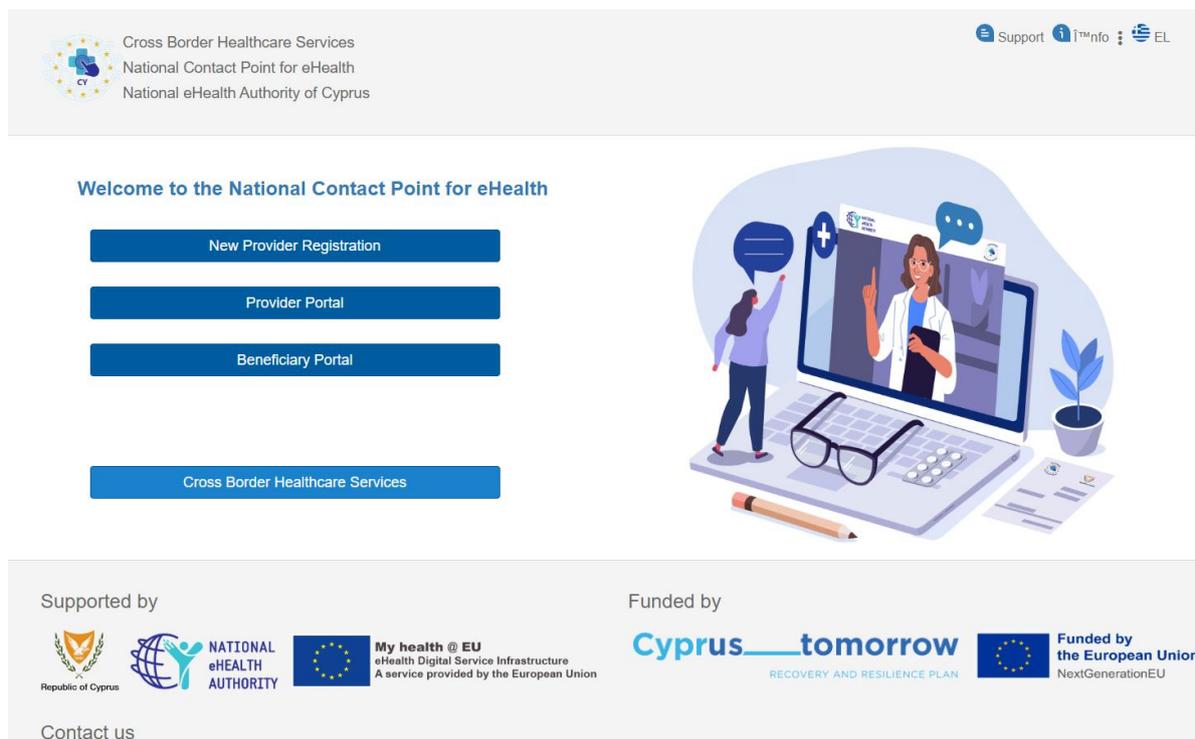


Figure 1: National Contact Point for eHealth Portal

Upon the user's transition to the cross-border healthcare platform, re-entry of login credentials will be required in order to access the available services.

The screenshot shows the top navigation bar with the logo of the National eHealth Authority of Cyprus and the text: "Cross Border Healthcare Services", "National Contact Point for eHealth", and "National eHealth Authority of Cyprus". On the right, there are links for "Support", "Info", and "EL".

The main content area features an illustration of a healthcare professional interacting with a large laptop screen. The screen displays a medical interface with a plus sign and a person's profile. A woman stands next to the laptop, pointing at the screen. A speech bubble is next to her. The laptop has a pair of glasses and a pencil on it. A small potted plant is on the right.

Below the illustration, the text reads: "Through their entrance to the platform, healthcare professionals have the ability to provide healthcare services that concern Patient Summary and Electronic Prescription/Dispensation." Below this text is a blue button labeled "Provider Portal".

The footer section contains logos for "Supported by" (Republic of Cyprus, NATIONAL eHEALTH AUTHORITY, My health @ EU) and "Funded by" (Cyprus—tomorrow, RECOVERY AND RESILIENCE PLAN, Funded by the European Union, NextGenerationEU). It also includes contact information: "Contact us" with links for <https://www.neha.org.cy>, phone number +357 22436038, email [info@neha.org.cy](mailto:info@neha.org.cy), and address 67<sup>th</sup> Limassol Avenue, 2121, Aglantzia, Cyprus. A small copyright notice is at the bottom: "Copyright © 2025 National eHealth Authority / Terms of Use / Privacy Policy".

Figure 2: Login to the Provider's Portal

Access to the National Contact Point for eHealth (NCPeH) is carried out through secure identification and authentication via the government web portal Gov.cy. The account on the portal constitutes a secure, personal digital account that provides access to various electronic services of the Republic of Cyprus.

 **CY Login**

**Sign in**

Username

Password

**Sign in**

---

No account? [Sign up](#)

[Forgot username?](#)

[Forgot password?](#)

OR

 [Sign in with Cyprus eID](#)

 [Sign in with eIDAS](#)

English

[Help](#) [Contact Us](#)

Figure 3: CY Login. Please enter your credentials.

Detailed instructions for creating an account on the Gov.cy portal, as well as for managing your personal profile, can be found at the following link on the official government website.



<https://cge.cyprus.gov.cy/cyloginregistration/register>

Figure 4: Official Government Website



### Welcome to the National Contact Point for eHealth

- New Provider Registration
- Provider Portal
- Beneficiary Portal
- Cross Border Healthcare Services



Supported by



Funded by



Contact us

Figure 5: Guidelines for new users

If you have created an account on CY Login and have activated two-factor authentication, please proceed to "Step 2: Access Management".

## User Registration / Two-Factor Authentication Activation

A prerequisite for using the application is that the citizen must have a verified CY Login profile with the Two-Factor Authentication feature activated. The CY Login service is the common access mechanism for government systems and services. Citizens who do not have a CY Login account can follow the steps below through the CY Login service. Two-Factor Authentication can also be activated through the application once Steps 1 and 2 have been completed.

### Step 1: Create / Activate Profile

- o Log in to the CyLogin Portal and start the registration process via the provided link.
- o Read the steps and begin the profile creation process.
- o Fill in the required information to create your profile.
- o Activate your profile (within 15 minutes) using the activation email.

### Step 2: Profile Verification

Profile verification can be completed through one of the following three options:

- o Using e-banking services of participating banks.
- o Via video call with a KEP (Citizen Service Center) officer, after scheduling an appointment.
- o By visiting a KEP/KEPO (Citizen Service Center/Citizen Point) in person, also by appointment.

### Step 3: Two-Factor Authentication Activation

- o The user logs into their CY Login account.
- o From the homepage, they select "Activate Two-Factor Authentication".
- o The user enters their mobile phone number and confirms it by entering the One-Time Password (OTP) received via SMS.
- o Selection of Verification Method Used
  - Via Authenticator App.
  - Via SMS Message.

Next Step

Figure 6: Instructions for Creating a «Cy Login» Account.

Step 2: Access Management

### Access Management

Healthcare professionals, specifically doctors and pharmacist-owners, are required to install the digital certificate on their computer (Microsoft Windows or Apple MacOS) for successful access to the platform.  
To proceed, please click the "Proceed" button to be assigned a user role as described below.

**User Role: Doctor**

- o Issuance of digital certificate.

**User Role: Pharmacy Owner – Pharmacist**

- o Issuance of digital certificate.
- o Management of pharmacists.
- o User registration within the pharmacy.

**User Role: Pharmacy Employee – Pharmacist**

- o User registration within the pharmacy.

Proceed

Figure 7: Access Management – “User Roles” & “Digital Certificate Issuance”

If you are a new user, once you have completed the creation and authentication of your profile on CYLogin, the next necessary step is to enable Two-Factor Authentication (2FA). Enabling Two-Factor Authentication significantly enhances the security of your account, as it adds an additional layer of protection beyond the password.

To enable Two-Factor Authentication (2FA) on your CYLogin account, first visit the official website <https://cylogin.gov.cy> and log in with your credentials. Once you have accessed the system, go to your profile, usually located in the top right corner of the screen, and select 'Settings' or 'Security Settings.' In this section, you will see the option 'Two-Factor Authentication (2FA).' Select the corresponding option to initiate the activation process. You will then be prompted to enter your mobile phone number. Immediately afterward, you will receive a One-Time Password (OTP) via SMS, which you must enter in the designated field on the screen to complete the verification and activation process.

Next, you will be asked to select the method by which you would like to receive the second factor for verification. The CYLogin service recommends using an authenticator app, as it provides a higher level of security. The two suggested options are Google Authenticator or Microsoft Authenticator.

Alternatively, you may choose to receive the code via SMS on your mobile phone. While both methods are acceptable, using an authenticator app is considered more secure and reliable for protecting your account.

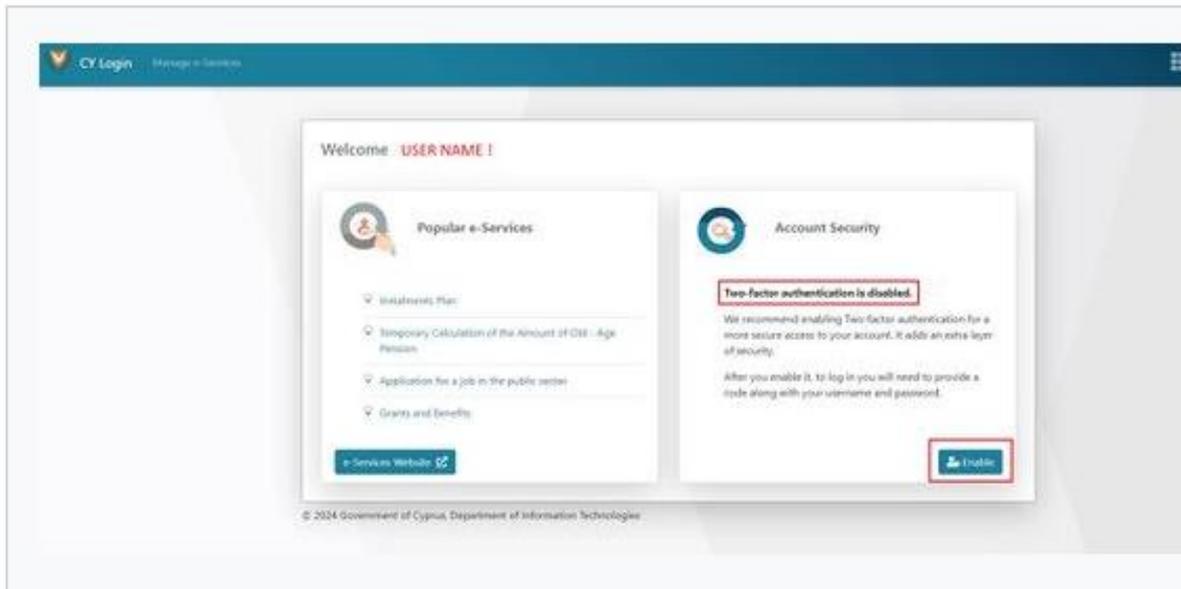


Figure 8:CY Login page. How to enable Two-Factor Authentication.

When using an authenticator app, a QR code will appear on your screen. Open the app on your mobile device and scan the QR code. If you are unable to scan it, you can enter the code manually. The app will generate a six-digit security code, which you must enter into CYLogin to confirm activation. If you choose SMS as your verification method, you must enter your mobile phone number and verify it by entering the One-Time Password (OTP) you receive via SMS.

Once you have correctly entered the six-digit code, click 'Confirm' or 'Complete.' If everything has been done correctly, a message confirming the successful activation of Two-Factor Authentication will appear

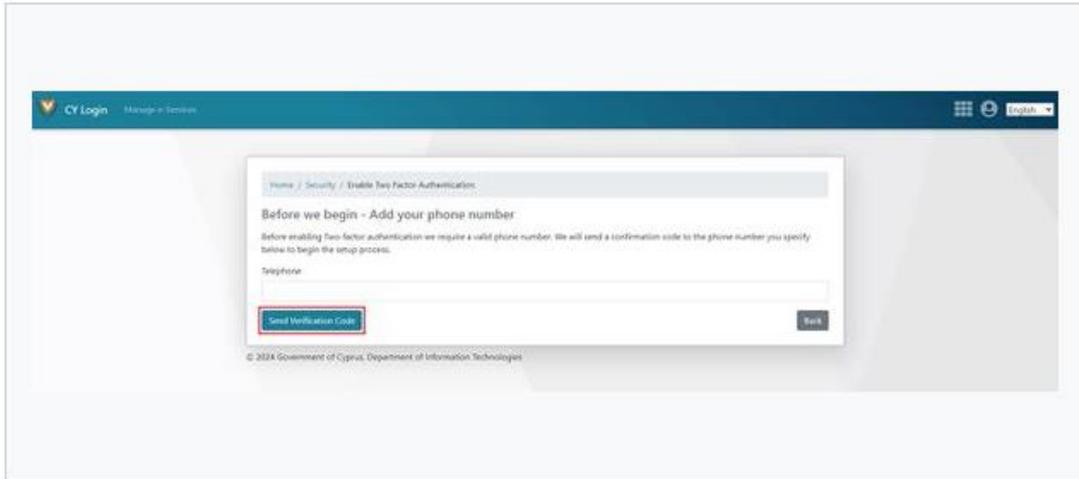


Figure 9: CY Login page. Send a verification code to a valid phone number.

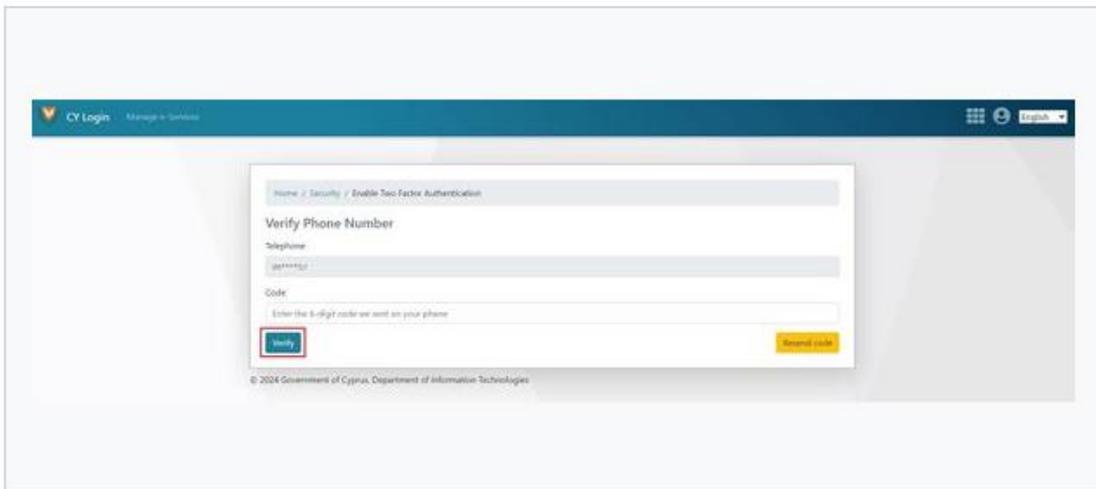


Figure 10: CY Login page. Enter the 6-digit code you received on your phone.

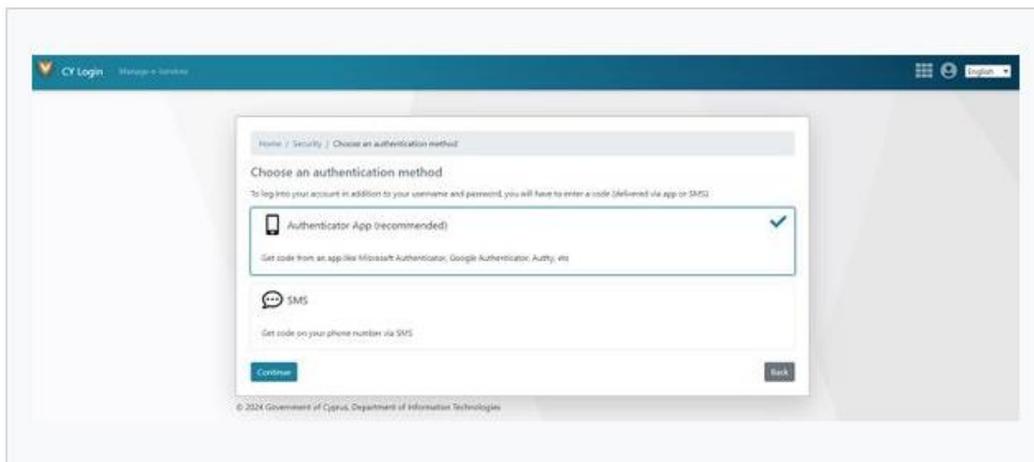


Figure 11: CY Login page. Choose an authentication method.

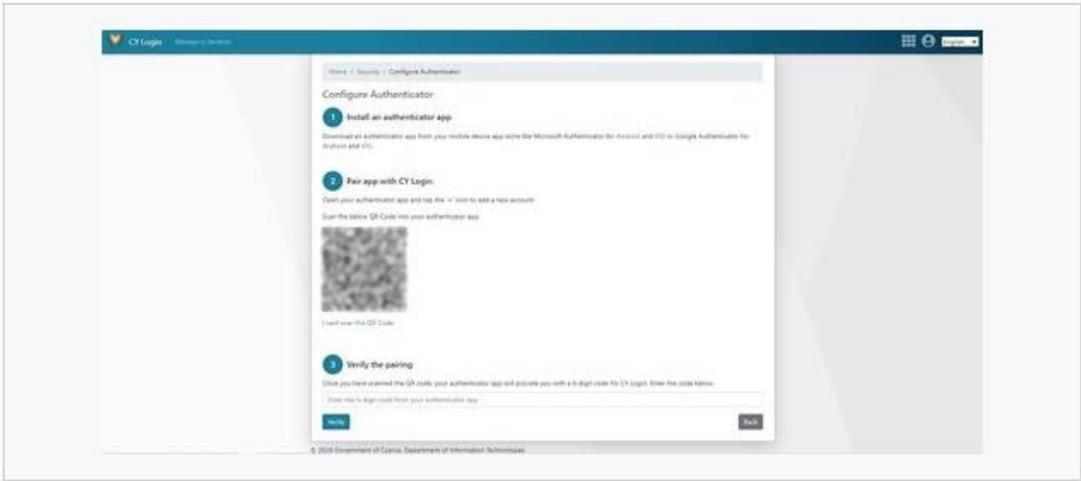


Figure 12: CY Login page. Configure Authenticator.

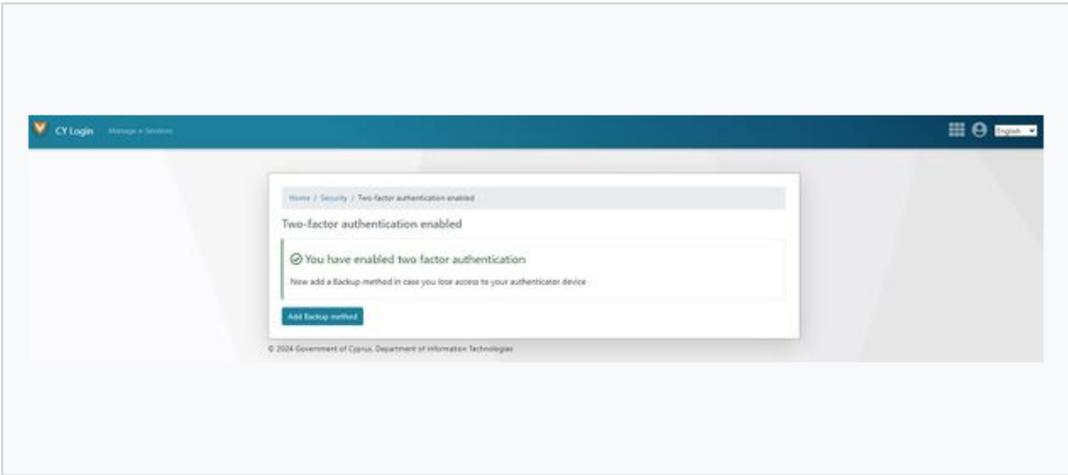


Figure 13 : CY Login page. Two-factor authentication enabled.

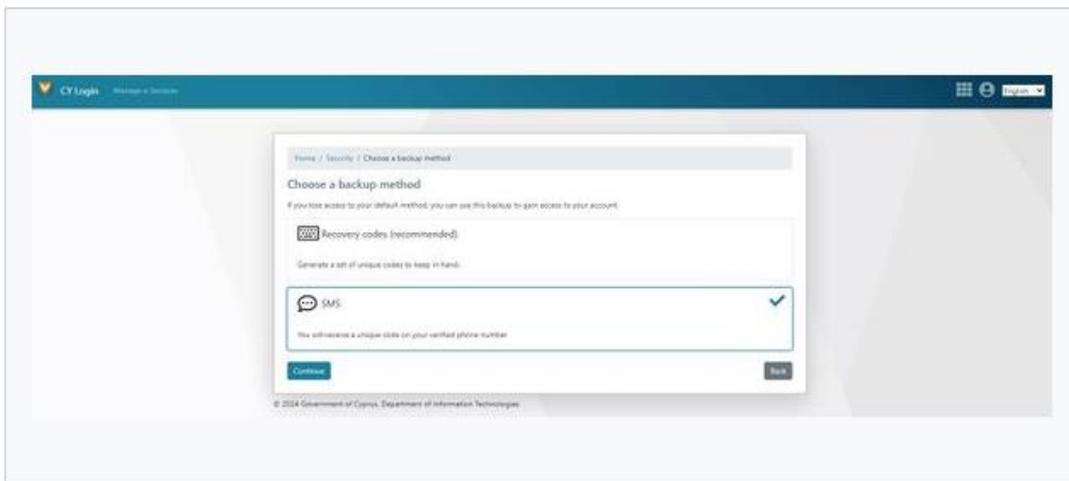


Figure 14 : CYLogin page. Choose a backup method.

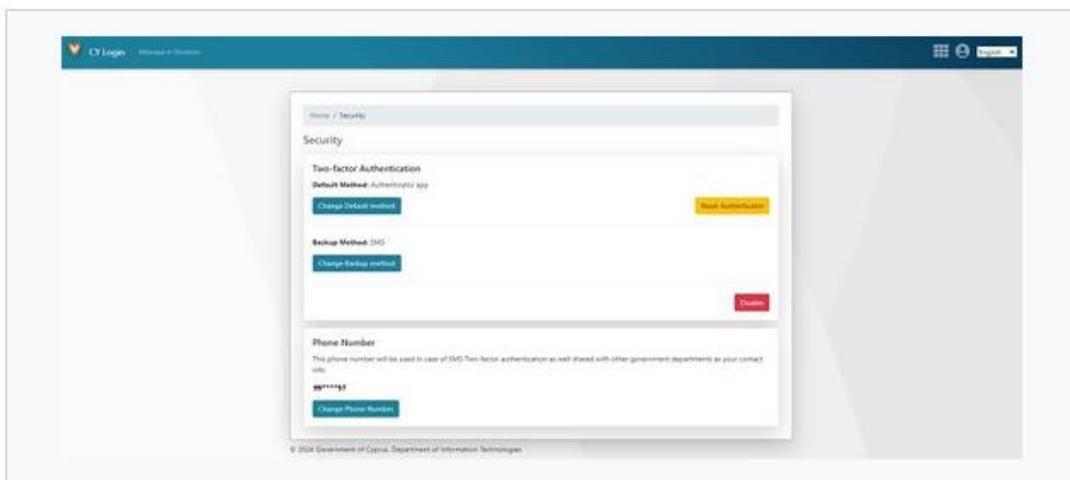


Figure 15: CYLogin page. Change or disable Two-factor authentication.

Once the default login process is completed, if you do not have access to the authenticator app, the CYLogin system provides alternative methods to proceed with your authentication. Upon signing in, you will be asked to choose one of the available alternative access methods in order to verify your identity. The available options are using a Recovery Code or receiving a code via SMS. The CYLogin system strongly recommends using Recovery Codes, especially in cases where access to the authenticator app is not possible.

## Access Management

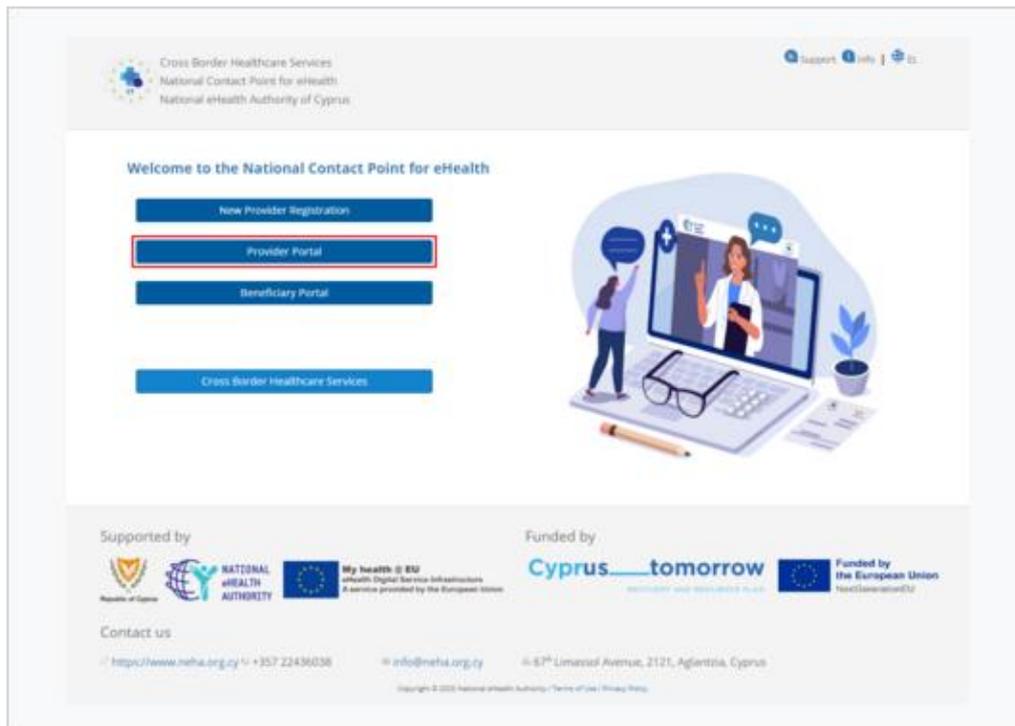


Figure 16: Selecting “Providers’ Portal”.

Upon logging into the NCP system, the physician must issue and download the Digital Certificate, which can only be stored on the specific computer where the login took place. This certificate is valid for two years and is required to ensure secure access to citizens’ data from other participating countries, within the framework of the cross-border operation of the NCP through Cyprus’s NCPeH (National Contact Point for eHealth).



## Digital Certificate Installation Guide

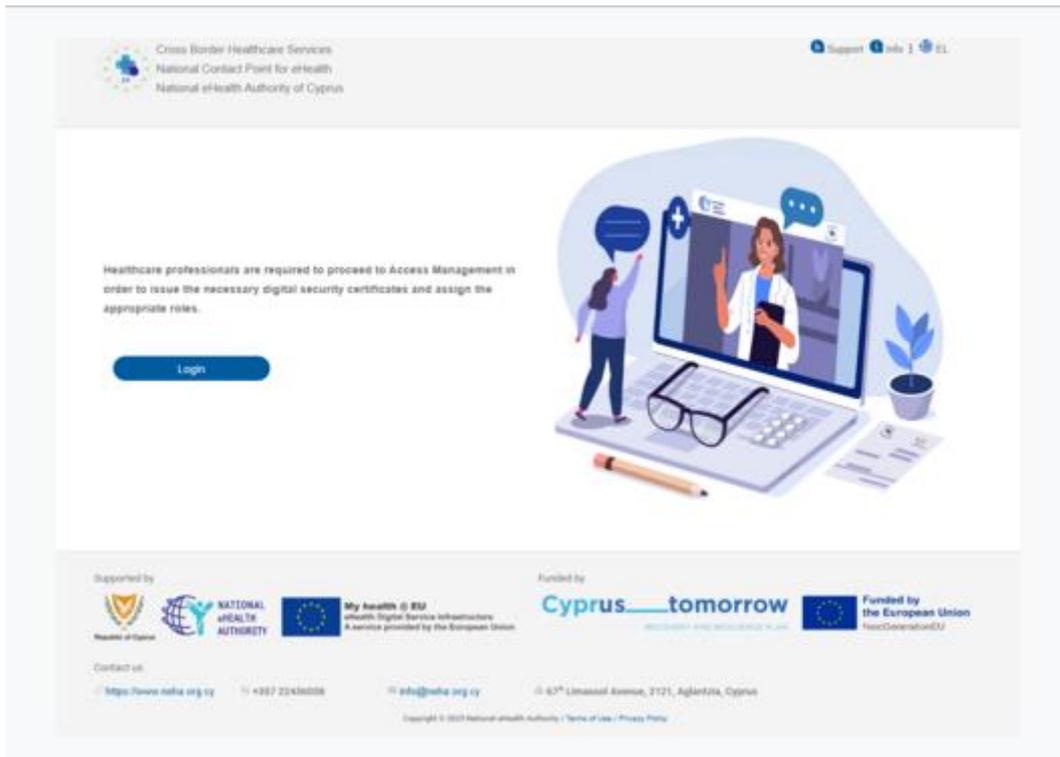


Figure 19: Login Interface for Healthcare Professionals on the Registry Portal

### Install Digital Certificate for Cross-Border Services

#### Instructions

The Cross-Border Digital Certificate is an electronic file used to verify a user's identity online. It confirms the authenticity of the user and ensures the security of communication. To access cross-border healthcare data, providers must follow a simple process involving the creation and importation of this Digital Certificate into their browser. This enables secure access to the NCPeH (National Contact Point for eHealth) portal.

[Download Digital Certificate](#)

[View Digital Certificates](#)

Follow these three steps to download a Digital Certificate:

1

(1) Click on the "Download Digital Certificate"

2

(2) Click "Yes" to the message "Create a Digital Certificate?"

3

(3) Click "OK" to close the message "An SMS was sent to the phone \*\*\*\*\*456"

Figure 20: Instructions for Installing the Digital Certificate for Cross-Border eHealth Services

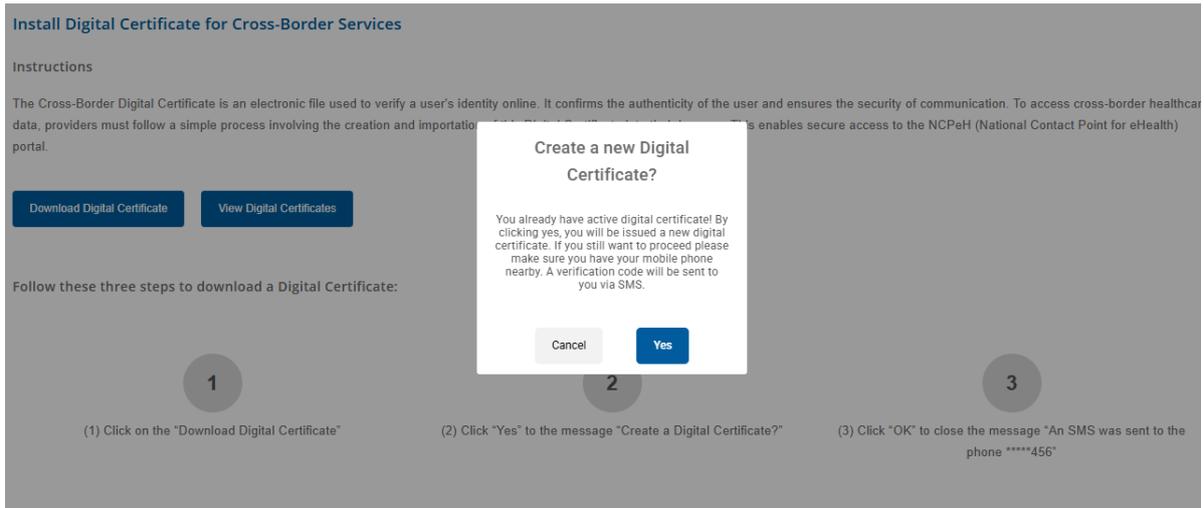


Figure 21: Generating a New Digital Certificate

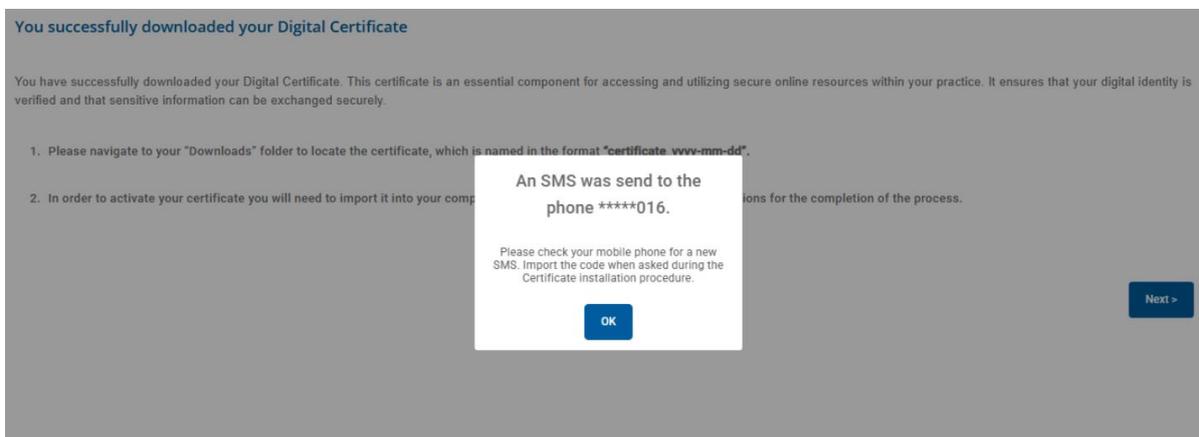


Figure 22: Delivery of the Digital Certificate Installation Code to the User's Mobile Device via SMS

### You successfully downloaded your Digital Certificate

You have successfully downloaded your Digital Certificate. This certificate is an essential component for accessing and utilizing secure online resources within your practice. It ensures that your digital identity is verified and that sensitive information can be exchanged securely.

1. Please navigate to your "Downloads" folder to locate the certificate, which is named in the format "certificate\_yyyy-mm-dd".
2. In order to activate your certificate you will need to import it into your computer. Click "Next" to follow the detailed instructions for the completion of the process.

Figure 23: Digital Certificate Successfully Downloaded

← Back

### Install your Digital Certificate

Please follow the instructions to import the certificate into your computer. Once completed, click the "Test Certificate" button to verify if the permission is active.



The image shows a web interface with two dropdown menus. The first dropdown menu is labeled 'Installation in Windows operating system' and the second dropdown menu is labeled 'Installation in MacOS operating system'. Both menus have a downward-pointing arrow on the right side.

Figure 24: Selection of the Installation Guide Based on the User's Operating System

## Digital Certificate Installation Process on MacOS

1. Locate and open the application "Keychain Access" either by using Spotlight Search or by navigating to Applications > Utilities in Finder.

**Note:** In newer versions of macOS, such as macOS Sequoia, when you try to open the Keychain Access application, the system may first launch the Passwords app and display a message with options. In this case, select "Open Keychain Access" to proceed to the correct application.

In this case, we select 'Open Keychain Access' to proceed to the correct application.

2. In the pop-up window that will appear with title "Manage your passwords" in "System Settings", click on the "Open Keychain Access" button.
3. While you are in the application "Keychain Access", navigate to the menu bar and click on File > Import Items.
4. Click the "Show Options" button.
5. Under "Destination Keychain" drop down, select "System".
6. Locate and select the .pfx file that you just downloaded from the NCP platform.

**Note:** Most likely to be found in "Downloads".

7. Click "Open".
8. Enter your user account password and click "Modify Keychain".

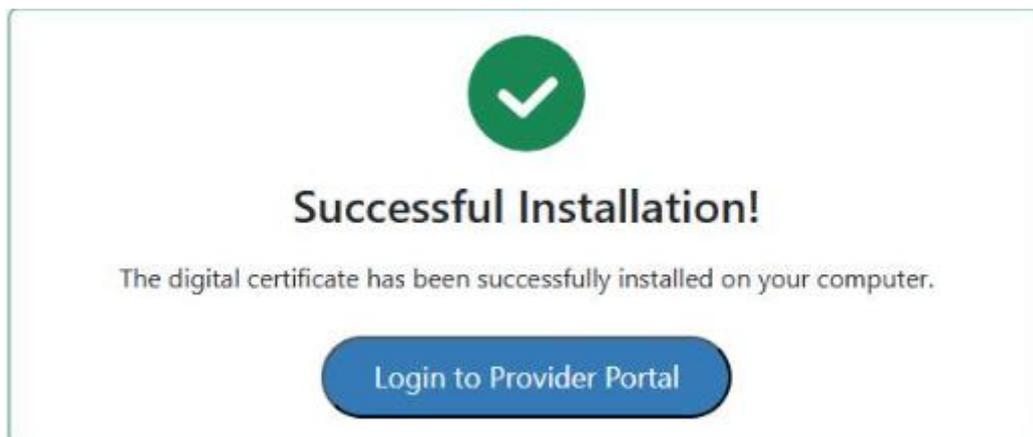
Note: This won't be needed, in case you entered your credentials while the application was launched.

9. Enter the password you received on your mobile phone when you requested a new certificate.
10. Click "Ok" button.
11. Enter your user account password and click "Modify Keychain".
12. Locate and select the certificate in the "System list".
13. Navigate to File > Get Info. To navigate to "Get Info" you can either use the menu bar or right click on the file .pfx.
14. Expand the "Trust" section.
15. Under the field "When using this certificate" drop down select "Always Trust".
16. Close the window and re-enter your user account password to save changes.
17. Click "Update Settings" for changes to be applied.
18. Navigate to File > Close to close the "Keychain Access" window.

## Installation on Windows

1. Find your new certificate file and double click on it.
2. Select Current User and click "Next"
3. Browse to certificate file.
4. Change the file type \*X.509 Certificate (\*.cer, \*.crt) σε Personal Information Exchange (\*.pfx, \*. p12).
5. Select the certificate file and click "Open".
6. Click «Next».

7. Enter the password you received on your mobile phone when you requested a new certificate.
8. Deselect Enable strong private key protection.
9. Click «Next».
10. Select Automatically select the certificate store on the type of certificate and click “Next”.
11. Click «Finish».
12. Click “OK” to close the import was successful message.



*Figure 25: Digital Certificate Successfully Installed*



### Digital Certificate Import Failed!

The digital certificate could not be properly imported into your internet browser.

---

This may be due to one of the following reasons:

- You have downloaded the digital certificate but have not yet imported it into your browser.
- You have deleted or cannot locate the digital certificate file on your computer.

Please repeat the process of downloading and importing the digital certificate.

[Download and Import a New Digital Certificate](#)

*Figure 26: Digital Certificate Installation Failed*

## Access to the National Contact Point

Upon logging into the Portal, you have the option to indicate whether the citizen you are assisting is a Cypriot national. In this case, you may proceed with creating or updating the Patient Summary (PSA), as well as issuing an Electronic Prescription (EP), depending on the purpose of the visit and the context of care provision.

If the individual is a citizen of another European country, you may proceed with retrieving their Patient Summary (PSB).

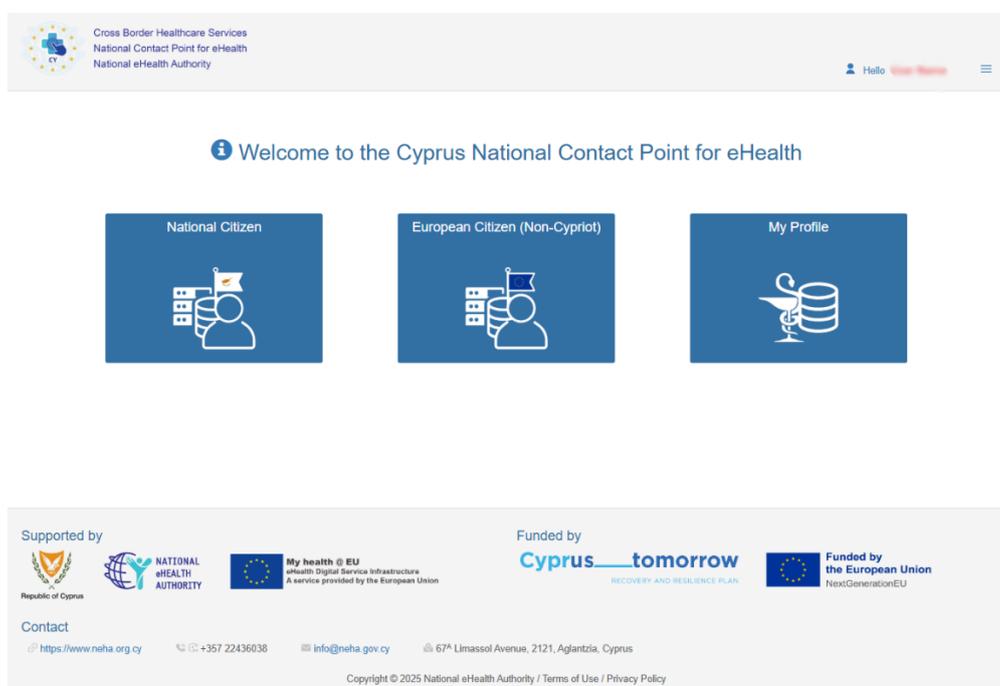


Figure 27: National Contact Point Portal – Home Page  
Select “National Citizen” or “European Citizen.”

# Provision of Services by Physicians

## Patient Summary

### Creation of a Patient Summary (PS)

The Patient Summary (PS) is created for Cypriot citizens who plan to travel to countries within the European Union and wish to have access to Cross-Border eHealth Services. The purpose of this process is to ensure that, in the event of a medical emergency during travel, healthcare professionals in other EU member states can have immediate and secure access to the citizen's essential medical information. The Patient Summary is made available to healthcare providers in EU countries and can be used directly if medical care is required during the citizen's stay abroad. It is essential to inform the citizen that their health data will be processed in the country of travel.

The citizen visits their Personal Doctor and informs them of their intention to travel abroad. Once the doctor completes the identification and authentication process as a user within the National Contact Point system, they proceed with the creation and submission of the Patient Summary (PS). A prerequisite for creating and/or updating the PS is the citizen's consent. This consent is provided through the entry by the doctor of a One-Time Password (OTP), which the citizen receives on their mobile phone.

Next, once the doctor has logged into the system, they follow the procedure below:

- The doctor searches for the patient using their ID card (ADT or ARC) and date of birth,
- The doctor is prompted to enter the One-Time Password (OTP) sent by the NCP system to the patient,
- From the available options "View / Edit", the doctor selects "Edit."
- An intermediate page is then displayed, asking the doctor to acknowledge that they will be the author of the Patient Summary (PS). This step applies if the doctor has not previously edited data for this patient or if the patient's PS does not already exist,
- The doctor gains access to add/edit or create the Patient Summary (PS),

- The doctor either saves or discards entry. If neither action is taken, the data is automatically deleted after 24 hours.

Please provide patient demographics data.

ID:  Name:  Surname:  Date of Birth:  Gender:

Address \* (number, address, postal code, city)  Country \*

Email  Mobile Phone Number \*

After the submission of patient demographics, it is necessary to verify the patient's phone number through an One-Time Password (OTP).  
Please fill in all mandatory fields (\*)

Figure 28: First Entry of Citizen Data for Patient Summary Creation or Electronic Prescription Issuance

Enter Patient Personal Identifiers

Fields marked with an asterisk ( \* ) are mandatory.

Type of Identification Document \*  Identification Document Number \*  Date of Birth \* (Correct format (dd-mm-YYYY))

Figure 29: Searching for a patient requires the physician or pharmacist to input the identity card number and date of birth.

Please provide the One-Time Password to verify patient consent

One-Time Password

Figure 30: Input of the One-Time Password (OTP)



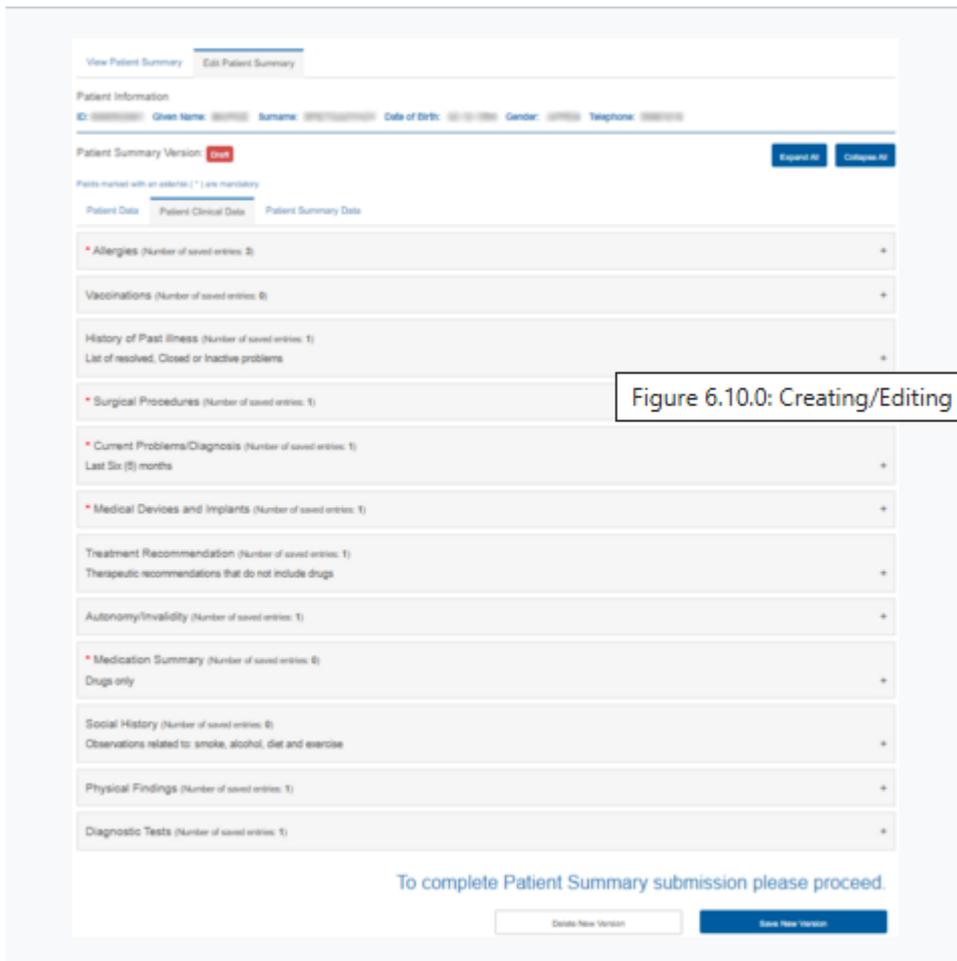


Figure 6.10.0: Creating/Editing t

Figure 34: Creating/Editing the Patient Summary Health Record

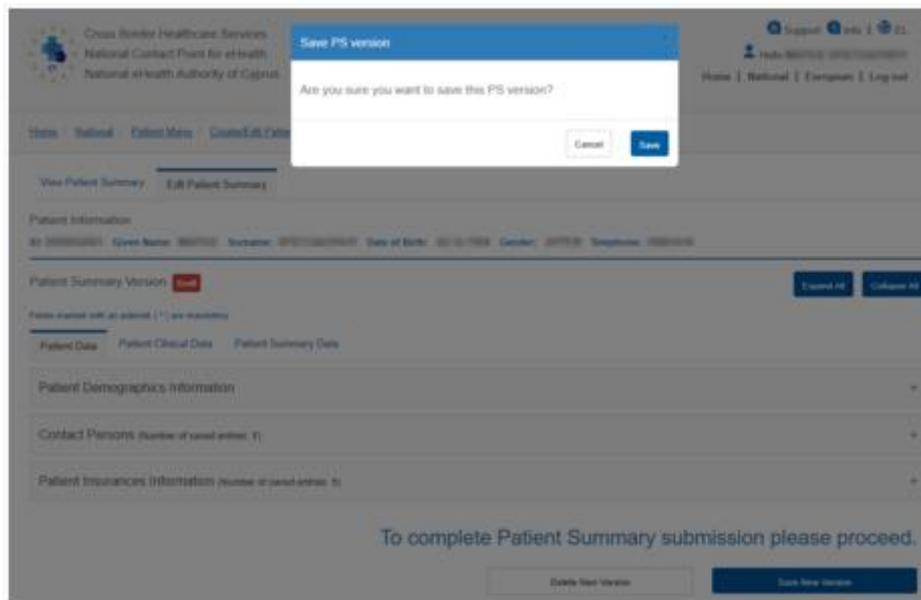


Figure 35: Confirmation of the "Save" Action

## Contents of the Patient Summary

The data included in the Patient Summary (PS) are as follows:

- Data of the doctors who provide medical information in the patient's PS:

i) Identification details: full name, unique identifiers

ii) Contact details: work/clinic address, mobile phone number

iii) Professional details: specialty, registration number

- Patient Data

According to the current setup, the patient's medical data is entered manually by the personal doctor. The ultimate goal and next stage is the automation of the data collection process for the Patient Summary through integration with other source systems/databases — medical data via the GESY platform, and demographic data through integration with the Civil Registry and Migration Department database.

The same procedure applies when the patient wishes to update their Patient Summary (PS). The doctor chosen by the patient will be authenticated through the process described above and, using the patient's demographic information and OTP, will locate the existing Patient Summary in the system. The doctor will then modify or update it as needed by selecting "Update Patient Summary."

As mentioned above, in order to create or update the Patient Summary (PS), the doctor must, in addition to the patient's ID/ARC number and date of birth, also enter the One-Time Password (OTP) sent by the NCP system to the patient at that moment. This process ensures that:

- I.No Patient Summaries (PSs) are created or updated without the patient's knowledge or consent, and
- II.The Patient Summary is created or updated only by the doctors selected by the patient.

## Data Security and Privacy

The Patient Summaries (PS) will be stored in the system in encrypted form, and access will be granted only after entering the One-Time Password (OTP) sent by the system to the registered phone number.

The privacy and security of the information are ensured through the following encryption mechanisms and hashing algorithms:

1. The NCP does not store the citizen's identification data within the system. Instead, it stores a hash identifier generated from the document type, document number, the person's date of birth, and an alphanumeric value securely registered in the system. These data are irreversible.

2. The patients' medical data are stored in encrypted form using symmetric encryption (AES-256). The decryption key is protected in such a way that it cannot be shared with the application programming interface (API) that accesses the encrypted data, unless a valid One-Time Password (OTP) for the specific patient (hash identifier) is provided. In that case, the decryption key is retrieved from the secure keystore and temporarily loaded into memory to decrypt the data.

Therefore, no one (including the officers of the NCP) has access to or can decrypt the data without the unique One-Time Password (OTP).

The procedure described above ensures the data subject's right of access in accordance with Article 15 of the GDPR. In this way, each patient will have access to their own Patient Summary, prescriptions, and other related documents contained within the NCPeH (beneficiary portal) through their account on the "GOV.CY" web portal.

The patient will be able to receive notifications regarding the creation or update of their Patient Summary, access by healthcare professionals to their record, requests submitted by the National Contact Point (NCP) of another Member State for its retrieval, as well as the transmission of the record to the corresponding NCP of that Member State.

It is noted that these notifications will be sent via SMS to the phone number registered during the creation of the Patient Summary.

Regarding the retention period, it is ensured that Patient Summaries will be retained for 15 years from the date of the last update and will then be automatically deleted, unless the patient requests their deletion earlier. It should also be noted that Patient Summaries of citizens traveling from other EU countries are not stored under any circumstances.

## Retrieval of the Patient Summary of an EU Patient/Citizen - Patient Summary B (PS B)

A citizen insured in another EU member state who is currently in Cyprus visits a doctor and informs them that their Patient Summary exists in their home country's cross-border eHealth system. All doctors in Cyprus have the ability to retrieve the patient's medical summary using the NCPeH CY application, after first being authenticated through the government portal Gov.cy.

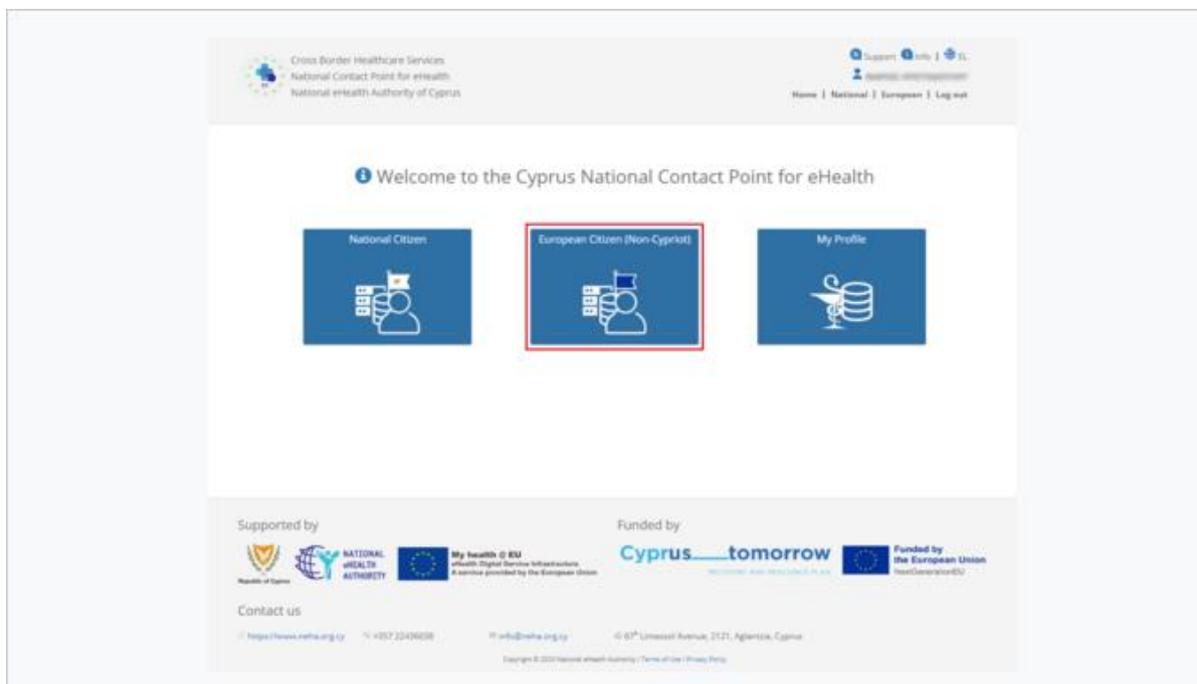


Figure 36: Selection of the "European Citizen" button



Figure 37: Selection of the European Citizen's Country Eligible for Cross-Border Services.

The doctor accessing the NCPeH application selects the cross-border functionality on the platform, indicating that they will operate as an NCPB. They then select the patient's country and submit a request to retrieve the Patient Summary (PS B) of the EU patient/citizen, after entering the patient's unique identifiers, as defined by each member state for NCP purposes.

Figure 38: Enter the European Citizen Identification Method.

Through the cross-border portal of NCPeH CY, the request is forwarded to the system of the patient's home and insurance country, from which the Patient Summary (PS B) is retrieved in XML and PDF formats. The files containing the Patient Summary (PS B) are transferred directly to the doctor's computer without being stored on the central infrastructure of the NCPeH.

The doctor does not have the ability to edit the patient's data and can only view it for NCP purposes.

Patient					
Prefix	Family Name	Given Name			
Primary Patient Identifier					
Gender	Female	Date of Birth			
▶ See details					

Creation Date of the Document	2025-08-26	Last Update of the Information	2025-08-26	Original Document Language	Croatian-CROATIA
-------------------------------	------------	--------------------------------	------------	----------------------------	------------------

Clinical Sections	
Allergies and adverse reactions Document	
▶ Original narrative	
▼ Translated coded	
No information about allergies	
Problem list - Reported	
▶ Original narrative	
▼ Translated coded	

Figure 39: Patient Summary

## ePrescription

The treating/prescribing doctor or healthcare provider in Cyprus logs into the NCPeH CY application, selects the cross-border e-prescription (eP) functionality, and issues a prescription by creating an electronic prescription.

**Add Prescription**

Search of Medicinal Product (at least 2 characters)

Brand Name  Active Substance  ATC Code

ATC Code

G	GENITO URINARY SYSTEM AND SEX HORMONES
GD4	UROLOGICALS
GD4C	DRUGS USED IN BENIGN PROSTATIC HYPERTROPHY
GD4CA	Alpha-Adrenoreceptor Antagonists
GD4CA01	Alfuzosin

Active Substance

ALFUZOSIN

Product Name

NATRAL OD TABLET, PROLONGED-RELEASE 10MG

Strength

10MG

Pharmaceutical Dose Form

TABLET, PROLONGED-RELEASE

Is substitution of Brand name allowed?

Yes  No

**Packaging**

Package Description\*

PACK WITH 30 TABLETS IN BUSTERS

Number of packages\*

1

**Posology**

Quantity\*

1

Units per Intake\*

TABLET

Frequency of Intake\*

1

Frequency of Intake Unit\*

day

Route of Administration

ORAL USE

Duration of treatment\*

1

Duration Units\*

month

Onset Date Tuesday, October 7, 2025

07-10-2025

**Instructions to patient**

**Advices to dispenser**

Clear form Cancel Save

Figure 40: New Electronic Prescription.

Αρχικό / Εθνικό / Μενού Ασθενή / Δημιουργία/Επεξεργασία Συνταγογράφησης

Πληροφορίες Ασθενή

Ταυτότητα: [ID] Όνομα: [Name] Επώνυμο: [Surname] Ημερομηνία γέννησης: [DOB] Φύλο: ΘΗΛΥ Τηλέφωνο: [Phone]

Ηλεκτρονικές Συνταγές (μόνο για διασυνδριακές υπηρεσίες υγείας) + Προσθήκη Συνταγής

Φίλτρο Κατάστασης: All

Αναγνωριστικό Συνταγής	Ημερομηνία Έκδοσης Ασφάλειας	(Κωδικός ATC) Περιγραφή	Κατάσταση	Ενέργειες
CY202507030000020	03/07/2025	(J02AC01) fluconazole 50MG	Active	[Icons]

Δημιουργός: [User]

**Περιγραφή**

Εμπορική Ονομασία: FLUCOZAL CAP-SULE, HARD 50MG  
 Δόση: 50MG  
 Μορφή Δόσης Φαρμάκου: CAPSULE, HARD  
 Συσκευασία: 1 x (PACK WITH 14 CAPS IN BLISTER(S))

Κωδικός ATC: J02AC01  
 Ενεργό συστατικό: fluconazole

**Θεραπεία**

Ποσότητα: 1 CAPSULE  
 Συχνότητα Λήψης: EVERY 1 DAY(S)  
 Οδός Χορήγησης: ORAL USE

Διάρκεια Θεραπείας: 7 day  
 Ημερομηνία Έναρξης (ChangeMonthYear): 03/07/2025

Συμβουλές προς τον Φαρμακοποιό: Advice on how to take the box is intended for both  
 Οδηγίες προς τον Ασθενή: one capsule after lunch for both the husband and the wife

Find Previous 1 Next Last Αντικείμενα ανά σελίδα: 5

Figure 41: Electronic Prescriptions History.

A similar procedure is followed as when creating/updating the Patient Summary (PS), as described below:

- The doctor searches for the patient using their ID/ARC number and date of birth.
- The doctor is prompted to enter the One-Time Password (OTP) sent by the NCP system.
- The patient’s prescription history is displayed, showing which prescriptions are active or inactive.
- The doctor selects “Create New Electronic Prescription.”
- The doctor gains access to enter the new electronic prescription.
- The doctor either saves or discards the prescription.

The selection of medicines will be made from a predefined list of drugs with specific codes that are standardized at the European level, as provided by the pharmaceutical authorities. These codes refer not to the brand but to active substances, dosage forms, etc. During the electronic prescription process, specific rules and restrictions are applied. The system allows only one medicine per prescription, meaning that multiple medicines require separate prescriptions. The treating doctor should be aware that:

A medicine legally prescribed in Cyprus as part of the official pharmaceutical list may be classified as prohibited or controlled in another European country. In particular, for controlled substances (e.g., opioids, sedatives, psychotropic drugs), legislation can vary significantly between EU member states. If a doctor in Cyprus issues an electronic prescription for a controlled substance:

The patient is responsible for ensuring that the medicine is permitted in the destination country and that the prescription can be legally dispensed in accordance with that country's legislation.

The cross-border prescription is stored locally within the NCPeH CY infrastructure for retrieval by a pharmacist in another EU member state who is authorized to dispense it. At the same time, it is always printed and signed as required by the applicable national law. When the prescription is dispensed abroad (eDispensation/eD), the information is returned to the system via the respective cross-border system of the member state where it was executed and recorded in the NCPeH CY database, ensuring that the dispensation is tracked in the cross-border system.

# Frequently Asked Questions (FAQ)

## Frequently Asked Questions for Doctors Practicing in Cyprus

Do doctors in the destination country automatically have access to the patient's health data? Do doctors need to report or inform that their patient is traveling?



Authorized Healthcare Professionals in the destination country can access a patient's health data only if the data are available for cross-border electronic health services. In some countries, citizens are required to give explicit consent, while in others, cross-border electronic health data exchange may be permitted by law and does not require any action from the patient. In any case, pharmacists and doctors in the treatment country can access a patient's health data only if it has been made available for cross-border electronic exchange by the country of residence. Additionally, in some destination countries, doctors and pharmacists may need the foreign patient to sign an additional privacy statement to comply with local legislation and be authorized to process the patient's data. Doctors in the country of residence should, depending on the member state, inform their patients about the possibility of making their health data available for cross-border electronic health services when they travel. This can be done either through personal guidance by the doctor or via access to a national health portal. It is not necessary to declare that the patient will travel. National portals differ from country to country, so doctors should check the information provided by their national contact point for eHealth regarding communication and availability of cross-border electronic health services. If they have not received training or guidance, they should contact their national contact point for eHealth to obtain the necessary information.

### In which language should I write the electronic prescription?

You must enter the prescription in the language of your country of residence. When the patient requests medication in the country of travel, the pharmacist will receive the prescription both in the original language and in the language of the destination country.

The translation is performed automatically through the underlying digital infrastructure, facilitating the pharmacist's understanding and execution of the prescription.

## What information is included in the Patient Summary?

- Warnings and Allergies
- Medical History (vaccinations, past health issues, surgeries performed more than six months ago)
- Current Medical Condition (ongoing health issues, medical devices and implants, current medications, treatment recommendations, surgeries within the last six months)
- Social History
- Pregnancy History (if relevant)
- Physical Findings
- Diagnostic Tests

It is not mandatory for all this information to be available. This means that there may be cases where only part of the data is accessible. For example, if certain information is not present in the electronic systems or cannot be translated into the language of the destination country, it may not be available. In addition, there may be specific details missing for the patient (e.g., allergies), which could make the Patient Summary partially inaccurate or incomplete.

Refer to the training provided by your National Contact Point for eHealth on how to read the information in the Patient Summary. If you have not received training, please contact your National Contact Point for eHealth to obtain the necessary guidance.

## Frequently Asked Questions for Doctors Practicing in Another EU Country

### How can I verify the identity of a European patient before accessing their Patient Summary?



Each country has specified the types of identification documents a patient may present when requesting a cross-border electronic health service (Patient Summary or Electronic Prescription). As healthcare professionals, it is essential to consult the National Contact Point for eHealth (NCPeH) of the country from which the prescription or Patient Summary originates.

Patient identity verification is done through the presentation of the appropriate identification document. Using the NCPeH web portal, you select the country of issuance of the European citizen's Patient Summary and are informed about the required documents and necessary details needed to search for the patient.

### How can I access the Patient Summary of a European patient?

Once you have authenticated via the Gov.cy portal and verified the patient's identity, you can request access to the patient's data provided by the underlying digital infrastructure by entering the patient's unique identifiers, as defined by each member state for NCP purposes. Before accessing the European patient's Patient Summary, it is necessary to inform the patient that their health data will not be processed in Cyprus.

If access to the patient's Patient Summary is not possible, an error message will appear with clear information about the reason. One common reason is that the patient did not request their Patient Summary before leaving their country of permanent residence. In such cases, you should advise the patient to contact their doctor upon returning to their home country to continue their usual care.

**In which language will the Patient Summary be accessible? What if it is in a language the doctor does not speak and the patient needs urgent care?**

When a doctor accesses the Patient Summary, they will receive the information both in the patient's language and in their own language. The underlying digital infrastructure automatically handles the translation. However, some information may be missing from the Patient Summary if it is not available in the patient's home country or could not be translated. If, for any reason, the doctor cannot understand the information in the Patient Summary, they should follow the usual procedures for patient care, as they would normally, without relying solely on the Patient Summary.

**What happens when a patient is in an emergency and urgent medical care is needed, but their health data are not up to date? Who is responsible?**

In case of an emergency, if access to the Patient Summary is not possible because the patient's data are unavailable (for example, if the patient forgot to provide authorization in their home country before departure), emergency services will provide the best possible medical care even without access to the patient's health information. If any issue arises from the care provided, the responsibility lies with the country where the treatment is delivered.

**How will a foreign patient pay for the healthcare received?**

If an EU citizen receives necessary healthcare using the European Health Insurance Card (EHIC), the same charges and payment procedures apply as for insured citizens of the country providing the care. If it is not possible to use the EHIC or the S2 form (pre-authorization form), patients must pay upfront and can request reimbursement once they return to their home country.

(\*) References:

European Commission – “My Health in the EU” (Digital exchange of electronic prescriptions and Patient Summaries)

#DigitalHealth, [ec.europa.eu/health/ehealth/digital\\_health\\_en](https://ec.europa.eu/health/ehealth/digital_health_en)