CM7 System Access Modifications Documentation

1. IP Restriction Implementation

- **Purpose:** Enhance security by limiting CM7 admin access to specific IP addresses
- **Implementation Method:** Using Hostinger's IP restriction features

2. URL Separation

- **Admin Portal:** Dedicated URL for administrative access
- **User Portal:** Separate URL for end-user interface **Benefits:**
- Enhanced security through separation
  - Better resource management Improved user
  - experience
  -
- the login interface for patients remains on domain xx.pl and we allow them to login via Google
- the interface for staff login is on cm7med.pl
- **It was not explicitly mentioned that the administrative interface will not be indexed - it is worth adding, for example, robots.txt, noindex in metadata and other crawl protection.**

The administrative interface (`cm7med.pl`) is strictly protected against search engine indexing and discovery. Measures implemented:

- `robots.txt` contains `Disallow: /` to block crawlers.
- HTML meta tag: `<meta name="robots" content="noindex, nofollow">`.
- The domain is not linked from any public page or sitemap.
- Optionally, domain name is obscure (e.g. `panel-login.cm7med.pl`) or not registered in public DNS.

3. New Login Page Implementation

- **Features:**
  - Modern user interface
  - Enhanced security measures
  - User-friendly design **Security**
- **Measures:**
  - Two-factor authentication capability
  - Add Captcha
  - Password strength requirements
  - Login attempt limitations

3. No mention that the new site will only be accessible via VPN - this is important.
No mention of the lack of a public DNS - the domain should be difficult to guess or even accessible only internally.
It's worth adding that all access is secured by VPN, not just login.

The administrative login site is not publicly advertised. It is technically accessible **only for whitelisted IP addresses**configured via Hostinger's VPS Firewall.
The system logs all login attempts (successful and failed), and unauthorized IP access attempts trigger alerts for the administrator.
If necessary, IP addresses are automatically revoked after a predefined time window (e.g., 5 hours) using server-side scripting or cron jobs.

3a. Login with SMS code (Two-factor authentication).

When logging in, after entering a username and password, the system requires the entry of a one-time SMS code.

The code is automatically sent to the phone number assigned to the employee's account by the receptionist or super administrator.

Rules of operation:

The phone number is entered when the account is created.

The SMS code has a limited validity period (e.g. 5 minutes).

Limit of attempts to enter the code (e.g. 5) - when exceeded, the system blocks the possibility of logging in for a specified period of time.

If necessary, the possibility to resend the code (with a limit of, for example, 1 time per minute).

Security and privacy:

Phone numbers are stored in the database in encrypted form.

Communication with the SMS service is done through an encrypted API (SMSAPI).

Ability to change phone number only by authorized administrator.

📌 **Additional suggestions:**

Consider implementing SMS fallback - if the code doesn't arrive, the user can request an alternative code (e.g., email with a link with limited validity).

Protect the API endpoint responsible for sending SMS from abuse (rate limiting).

- if someone doesn't want SMS then they can confirm OTP by email. For sending codes and messages there is to be a graphic visualization of sending these SMS with cm7med.co.uk logo and everything related to dashboard for staff will be sent from email admin@cm7med.pl

In addition to SMS verification, users can opt for OTP verification via email. All messages (SMS or email) include a branded visual (logo of `cm7med.co.uk`) and are sent from the trusted sender: `admin@cm7med.pl`.
All SMS and email endpoints are protected with rate-limiting to prevent abuse and spamming.

3D. Access Monitoring and Logging

The system continuously logs the following:

- IP addresses of all login attempts
- Timestamps and username (or user ID)
- Type of access (SMS, email, failed login)
- Events of adding/removing IP from firewall

Suspicious behavior (e.g., repeated access attempts from unknown IPs) triggers immediate alerts for the administrator.

4. Online Consultation Requirements

- Required Additional Fields:
  - National ID number PESEL
  - Residential address
  - Date of birth

- **Checkboxes:**

  There should still be 2 that are when choosing a stationary consultation plus add 2 additional checkboxes only for online consultations. In total, there should be 4 checkboxes for online consultations.

  This is the current content of checboxes, you will have to change it on July 4th!

- **Zapoznałem(-am) się z Regulaminem i Polityką Prywatności i akceptuję ich postanowienia**. * (we already have a regular consultation so this one stays)
- **Wyrażam zgodę na otrzymywanie powiadomień SMS i e-mail dotyczących mojej wizyty (np. przypomnienia, zmiany terminu** (we already have a regular consultation so this one stays)
- ***Wyrażam zgodę na przetwarzanie moich danych osobowych w celu realizacji konsultacji medycznej online zgodnie z RODO."*** *(new only for online consultation)*
- ***Zgadzam się na przeprowadzenie konsultacji medycznej w formie zdalnej i akceptuję związane z tym ograniczenia i warunki świadczenia usług (****new only for online consultation)*

5. Enhanced Security Features

- Add reCAPTCHA v3 to all registration forms
- Implement required checkbox on Contact page form

  - Generate site & secret keys via Google reCAPTCHA v3.
  - Insert client-side script in `<head>`.
  - On the backend, verify the token with Google API and evaluate score.
  - If score < 0.3 — reject the submission or require additional verification.

- **Contact form:**

  - Add a required checkbox (e.g., "I consent to data processing").
  - Prevent form submission if the checkbox is not checked.

- **Extra recommendations:**

  - Log reCAPTCHA score and user IP.
  - Optionally show reCAPTCHA v2 if score is low.

- Rate-limit form submissions per IP (e.g., max 10/hour).

6. Doctor Profile Optimization

- Individual doctor pages with URL format:

  https://centrummedyczne7.pl/lekarze/first-last-name Google
- indexing optimization with meta descriptions
- Direct booking link functionality from search results

SEO requirements for these pages:

- **Meta title** and **meta description** must be generated dynamically based on the doctor's profile data (full name, medical specialty, years of experience, consultation types, and prices).

  Example of a dynamically generated `meta title`:

  Name/ Surname – [SPECIALIST} General Surgery Specialist with |EXPERIENCE| 20 Years of Experience | Centrum Medyczne 7

- Example of a dynamically generated `meta description`:

  Book an appointment with Dr. Michał Sz, a general surgery specialist with 20 years of experience. Online consultations from 150 zł – available now at Centrum Medyczne 7.

- Each doctor profile page must include:
  - An **H1 heading** with the doctor's full name
  - **Visible information** such as specialization, experience, consultation types, and pricing
  - **Structured data markup** (Schema.org `Physician`) dynamically populated with the same data
  - A **canonical tag** pointing to the static URL
  - A clear **appointment booking link** (Call to Action)

Objective:
Ensure that Google correctly identifies and indexes the page as a personal profile of the doctor, optimized for name and specialty-based queries.

7. New Dashboard Reporting Feature

- Access Control:
  - Available to reception staff and super admins
  - Doctors limited to viewing own reports
- Report Features: Date range selector
  - Patient full name
  - Appointment date and time
  - Doctor's full name
  - Service details and pricing
  - Document generation metadata
  - Total earnings calculation
- Export Options: PDF and Excel formats

To implement these changes, please select the specific sections you'd like to modify and then request AI assistance through the menu.

Access Control:

- Available to **reception staff** and **super administrators**
- Doctors have access **only to their own reports**

Report Features:

- Custom **date range selection**
- **Patient's full name**
- **Appointment date and time**
- **Doctor's full name**
- **Details of the service provided** and its **price**
- **Metadata** regarding the time of report generation
- Automatic **calculation of total revenue** within the selected period

Additional Technical Requirements:

- The feature should appear as a **separate menu item** on the left sidebar of the dashboard
- The report view should support **export to PDF or CSV**
- Each entry should be **clickable**, opening detailed appointment information

Implementation Timeline

- [ ] Configure IP restrictions in Hostinger (remember that I have to easily grant access from a given IP and, for example, after 2 hours I can remove this access to cm7med.pl)
- [ ]
- [ ] Set up separate URLs for admin and user portals
- [ ] Design and implement new login page

Test all new security features

Document final configuration details

Note: All changes should be thoroughly tested in a staging environment before deployment to production.

As previously agreed, the following items were included in the original project scope and therefore must be implemented free of charge**:**

1. Configuration of the payment gateway
2. Customization of email templates (e.g., OTP messages) – all emails must be configured in **Polish**, appear **professionally styled**, and use a **consistent template**
3. Implementation of a system for sending login credentials to patients
4. Adjustments to the patient account area and fixing any potential issues
5. Optimization of images used in links (especially on the homepage)
6. Upload of Terms of Service and Privacy Policy documents (we'll provide them by July 4th)
7. Replacement of interior photos in the "About Us" section (photos are in preparation)
8. Conversion of images to WebP format and improvement of image quality (current images load slowly and appear low quality)
9. Page speed improvements (some elements still load too slowly)
10. Blocking the ability to open images in a new tab or download them
11. Improving image indexing in Google (e.g., clinic photos should be indexed properly)
12. 2–3 small adjustments to texts and images on the site

The project and final payment are considered complete only once everything is fully functional, error-free, and all content – including emails – is properly translated into Polish.