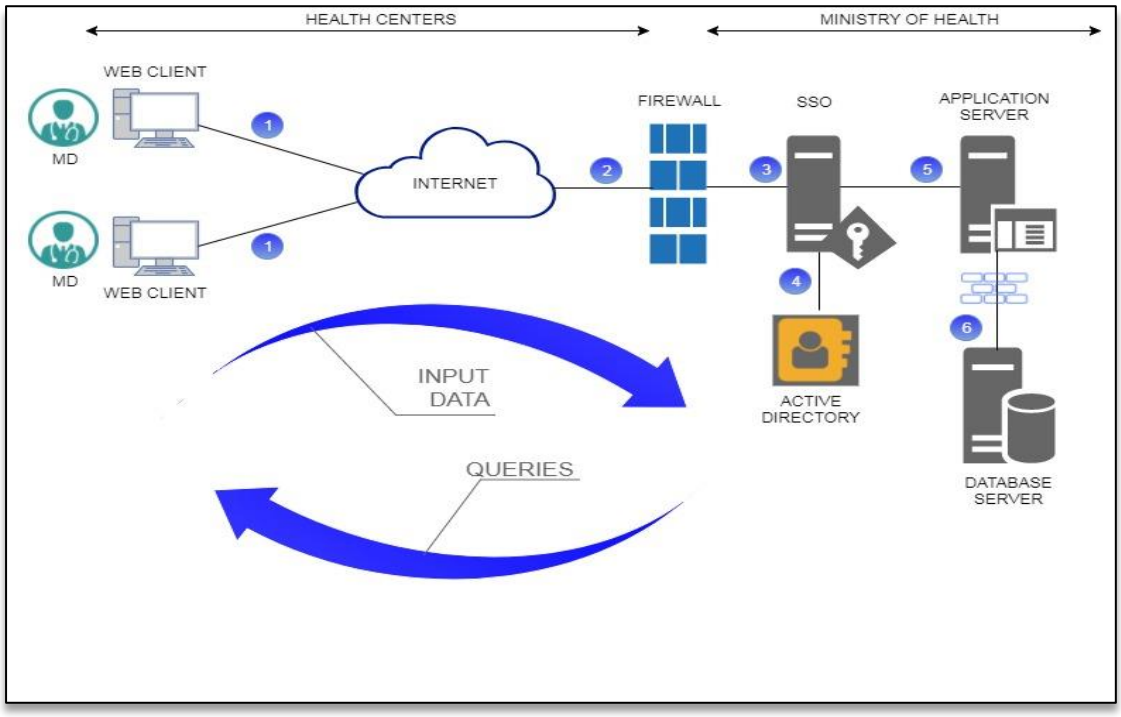
SUPPLEMENTARY FILE

HBR Security Framework Proposal

Suppl_Figure 1 displays the steps for visualizing a sequence for a secure framework regarding a doctor's (MD) navigation in the Hellenic Biomedical Registry (HBR).



Suppl_Figure 1. HBR framework proposal for secure MD's navigation .

Step 1: Medical doctors (MDs) of all Hellenic Health Units are able to register in HBR. Therefore, each MD submits the MD Registration Form (as Suppl_Figure 2 shows) via HBR platform online. He/She receives confirmation and credentials via two-factor authentication (2FA) from the Ministry of Health (governmental agency – administrator of HBR) [1,2]. This initial step ensures that the MD is informed about the security and management of sensitive patient's biomedical data and about the permission to use the software only for biomedical research purposes. Therefore, the MD Registration Form contains consent fields informing the MD for the HBR privacy policy and GDPR regulation awareness (as Suppl_Figure 2 shows).

Step 2, 3, 4: HBR administrators keep secure and update the HBR Active Directory regarding to the MDs' accounts. The MD (HBR end-user) navigates in the HBR using a secure Internet connection with Single Sign On (SSO) methodology over a security provide. Prior HBR real implementation, penetration testing procedures by governmental authorities are necessary to be executed.

Step 5, 6: Splitting off the application and database servers of the HBR, it improves the reliability of the system. At this point, the Virtualization Technology (a) increases the availability of the system, (b) ensures easier backup and disaster recovery, and (c) provides an easier route for administrators to install and maintain software, resulting to more efficient IT services. [3]-[5]

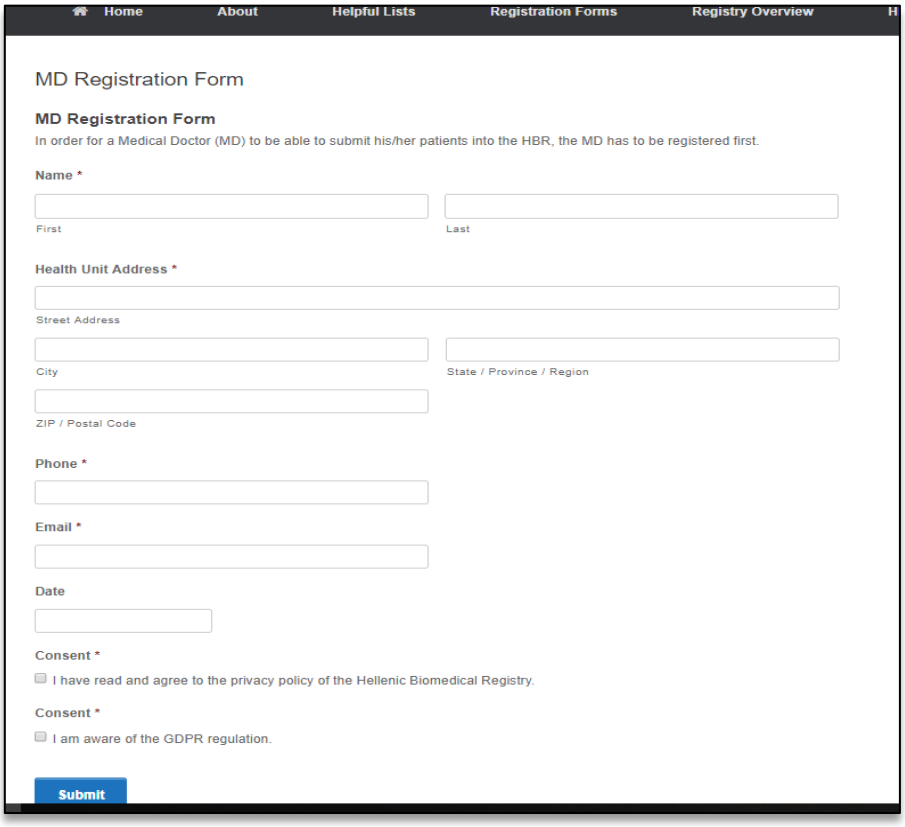
Input Data: The MD submits a Case Report Form (CRF), followed with a physically signed patient's application declaring his/her consent to participate in a clinical trial. This step ensures as far as possible the legitimacy of the patient's participation in a data recording system. Moreover, the following points must be mentioned:

- The MD adds/removes/alters patient's clinical and molecular information in the database.
- Only HBR governmental administrators have grants to delete the biomedical data of a patient (following GDPR regulation).
- The need for accurate patients' biomedical information resulting to the doctors' obligation to maintain all their registered patients' data updated. Based on this requirement, additional administrative support to each registered doctor might be necessary.

Output Data: All registered MDs are able to survey and query the database for scientific purposes.

MD Registration Form

Suppl_Figure 2 shows a screenshot from the HBR MD Registration Form webpage. The consent fields require opt-in action by the MD and are displayed before the submit button.



Suppl_Figure 2. MD Registration Form screenshot.

HBR General Information Security Policy & Measures

Regarding to our software development and virtual implementation, the general security policies are summarized as follows:

1. HBR modules is developed using WordPress® (free open-source CMS) and Microsoft® Visual Studio 2017 Community (free online/offline MS IDE distribution).
2. HBR security is based on *The Ultimate WordPress Security Guide – Step by Step (2019)* [6]**:**
    a. HBR requires credentials to login.
    b. MySQL Database is accessed only with administration grants.
    c. WordPress® modules and plugins are daily checked for updates.
    d. HBR contains plugins as a minimum-security policy:
        i. Ultimate Member
        ii. Sucuri Security for Auditing, Malware Scanner and Security Hardening
        iii. GDPR compliance plugin
        iv. Google Authenticator – Two Factor Authentication
3. Hospital Datasets were anonymized before we use them into our MySQL database schema.

REFERENCES

1. https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA, Last accessed in February 2019.
2. Fujii H, Tsuruoka Y. SV-2FA: Two-factor user authentication with SMS and voiceprint challenge response. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 2013, London, UK. DOI: 10.1109/ICITST.2013.6750207.
3. https://www.vmware.com/pdf/virtualization.pdf, Last accessed in February 2019.
4. https://education.emc.com/academicalliance/student/Virtualization%20WP.pdf Last accessed in February 2019.
5. https://www.sans.org/reading-room/whitepapers/metrics/security-data-visualization-36387, Last accessed in February 2019.
6. https://www.wpbeginner.com/wordpress-security/, Last updated in February 14th, 2019