Partially Autonomous Information System Facilitating Performance-based Managed Entry Agreements in Slovakia

Aleš Tichopád[1]
[1] Department of Biomedical Technology, Czech Technical University in Prague, Kladno, Czech Republic,
ales.tichopad@fbmi.cvut.cz

***Abstract*—Performance-Based Managed Entry Agreements (PB MEAs) are agreements between payers and/or regulators on one and health technology businesses on the other end in which the individual patient's treatment success rate is monitored. Agreed reimbursement is determined by that rate. Without a successful response to treatment, reimbursement is reduced or completely absent. There is a high need for functional PB MEA systems across the developed economies. Satisfactory wide use has not yet been achieved. The reason is, among other things, technical obstacles and lack of adaptability of existing IT and data systems to the purpose of PB MEA. We present an autonomous cloud-based e-health information system to facilitate a transfer, data aggregation and analysis of real-world drug effectiveness data for the sake of PB MEA execution. The system makes use of a Pretty Good Privacy security feature for encrypting and decrypting and existing national e-health authentication cards.**

Keywords—managed entry agreements; PGP; drug market access; e-health

I. Introduction

A. The need to control health costs

Increase in spending on pharmaceuticals in the future is expected as highly innovative products with novel biological mechanisms enter markets. Reimbursement of all medicines for all patients can lead to inefficiencies and often have an unacceptable impact on health budgets. There is not always sufficiently convincing evidence of the benefits of medicines, or the benefits may vary widely from patient to patient. Consequently, reimbursement policy makers have attempted to control pharmaceutical spending through more or less sensitive instruments, ranging from preference for generic medicines, to temporary conditional reimbursement, to mechanisms to encourage co-payments, risk sharing with manufacturers, etc.

B. PB MEA

Managed Entry Agreements (MEAs) are arrangements that take into account uncertainty about the performance of technologies (especially drugs) while regulating their adoption to maximize their efficient use or limit their budgetary impact [1-4]. MEAs can be seen as a tool that enables patients to access new medicines, with the risk of uncertain benefit is shared between payer and pharma. Performance-Based Managed Entry Agreements (PB MEAs) are a sub-type of MEAs in which the individual patient's treatment success rate is monitored, and the amount of reimbursement is determined by that rate. Experience with PB MEAs remains limited because they often face challenges such as lack of data on the benefit [5-7]. Existing hospital information systems often do not provide sufficient flexibility to create payer-accessible observational infrastructure. National registries can be inflexible in their structure when it comes to a new drug to be monitored.

C. The technical need

In order for the BP MEA process to be implemented, there must be an authentic and secure transfer of patient identifiable clinical data between the provider and the HI or regulator. However, this is not the sharing of the complete patient record, but rather the recording and sharing of one or a few specific variables, such as, for example, PASI-100 score for psoriasis, tumor size, or disease progression information. Often these may be secondarily derived variables or indices. The very specific data required for PB MEA do not have predefined fields in outpatient and hospital information system forms and are recorded by the physician in the form of their own notes and often in a very unstructured way. Sometimes they are not recorded at all. Moreover, these data are not shared with payers. Claims for reimbursement are not usable for PB MEA purposes because they do not contain clinically relevant information. All of these systems could be modified. However, the necessary flexibility to adapt those systems for tens of PB MEAs per year and the fact that different systems exist at different sites make it difficult. Despite the reach abundance of data controlled by the Slovak National Health Information Centre (NHIC), the health data authority, the reason for the non-implementation of PB MEAs is the lack of a properly set up and highly flexible system for tracking the close therapeutic response of individual patients by the payer.

2022 E-Health and Bioengineering Conference (EHB) | 978-1-6654-8557-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/EHB55594.2022.9991597

978-1-6654-8557-9/22/$31.00 ©2022 IEEE

II. Deployed security, architecture and envirnoment

A. PGP Encryption

Pretty Good Privacy (PGP) is a security program for encrypting and decrypting and generally any transmitted data files and for authenticating email messages using digital signatures [9,10]. PGP was first designed and developed by Phil Zimmerman in 1991 and subsequently the PGP software was acquired by Symantec in 2010. OpenPGP is the most widely used standard for encryption. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) as a proposed standard in the defined format of RFC 4880. OpenPGP was originally derived from the PGP software, which was created by Phil Zimmermann. A growing area of application for PGP is file encryption. Because the algorithm used by PGP is essentially unbreakable, PGP offers a highly secure way to encrypt files at rest, especially when used in conjunction with threat detection and response [11]. However, such an advanced solution has not been implemented within the system presented here. Asymmetric encryption technology uses two different key type methods to encrypt and decrypt the transmitted data. It also uses two additional keys to sign and authenticate each data file. Thus, a prerequisite for successful encrypted transmission is the exchange of public keys between the two parties. The principle is as follows:

1. The sender encrypts the file using the recipient's public key.

2. The recipient decrypts the file using his private key.

3. To check the integrity and integrity of the transmitted data files, the sender uses his private key to sign the encrypted file.

4. To verify the authenticity of the sender, the recipient uses the sender's public key to authenticate/confirm the sender.

B. Security architecture

The PGP security gateway (PGPSG) is a unique solution in the national eHealth environment installed in the internal infrastructure of healthcare providers (HCPs) and also in the internal infrastructure of health insurance companies (HIs). To secure the writing and reading of data, the PGPSG uses cryptographic operations based on the PGP protocol, which is based on asymmetric encryption. Demographic data is encrypted with the PHC and ZP public keys. It can only be decrypted using the PHR and GP private keys. This means that the demographic data can only be read by the PHR itself, who encrypted it, and the GP. It is not possible to decrypt this data on the server.

C. National Health Information Centre

NHIC is a state-funded organization founded by the Ministry of Health of the Slovak Republic. NHIC performs tasks in the area of informatisation of health service, administration of the national eHealth, standardisation of health informatics, health statistics and provision of library and information services in the field of medical sciences and health service. It administrates national health registries and national health administrative registries as well. The NHIC creates a fundamental environment and interface for the herein presented system.

III. Results

The system consists of four basic components: Database (DB), Server backend (BE) including API interfaces, Web portal (Frontend, FE) as a web browser environment and the PGP Security Gateway (Gateway) providing communication between the eHealth card, BE and FE part of the application, and providing data encryption and decryption using PGP keys and integration to eHealth by calling existing NHIC services (NHIS). The figure 1 shows the overall architecture diagram of the interaction between the modules as well as external entities (such as the health insurance company or the Ministry of Health).

A. Components

DB: The DB is a database built on MySQL 5.7+ technology. It is an opensource solution that does not require additional upfront costs to implement the application solution. The DB layer provides persistence of data in relational structures that can be accessed through SQL queries. Mirroring can be addressed within the DB to provide high accessibility and data replication. It is a separate layer that must be available to the BE part of the application.

BE: The BE is the backend part of the application that provides communication between the DB layer and the FE layer of the application through APIs and equally part of the application logic solution. A RESTful APIs are exposed in this part of the application for communication with the FE layer and the Gateway component. The communication at the transport layer level is secured by SSL protocol. The APIs themselves are protected by application security based on an authentication token, which is issued to the user upon successful login to the application. Access to individual application modules is secured by standard role-based access control (RBAC) access. The layer is implemented on PHP technology and Symfony 5+ framework. It is a separate layer that must communicate with the DB layer and FE layer of the application.

Web portal (or FE): The FE is a web portal serving as the frontend part of the application that mediates the interaction between the user and the application itself. It is a solution running in a web browser environment, based on the Vue 2+ JavaScript framework. FE consumes the REST API exposed by the BE part, so it is necessary for this layer of the application to be able to communicate with the BE part of the solution. The FE also communicates on localhost with the Gateway component of the application in the HCP (or generally any healthcare worker including e.g. nurses, HCW) client station environment. The FE runs in a browser environment on the user's localhost and provides the display of both clinical and patient demographic data. Communication at the transport layer level is secured by SSL protocol.

Gateway: The gateway is a standalone component that runs in the HCW's local station environment. The main role of this service is to ensure the separation of clinical data from patient demographic data that may identify the patient. Only the health care worker who entered the data into the system and the owners of the keys that were used to encrypt the data, such as the health insurer (HI) or another defined actor on the output with permission to read the encrypted data as well), can link the clinical data to the patient demographic data. The gateway also provides for the registration of the HCW and verifies him with the NHIC. Furter, it facilitates calling of NHIC services for the entry of data into eHealth in the predefined form. The Gateway is a service installed in the internal infrastructure of HCP and also in the internal infrastructure of other actors with the authority to read encrypted data if the project will require the disclosure of demographic data to the health insurance company or other actors in the output of the system. To secure the writing and reading of data, the Gateway uses PGP-based cryptographic operations, which is based on asymmetric encryption. The demographic data is encrypted with the public key of the health care provider and other actors with the authority to read the encrypted (demographic) data. It can only be decrypted with the private key of the PHR and the keys of other actors with the authority to read the encrypted (demographic) data. This means that only the owner of the private key that has been included in the encryption process can read the demographic data, i.e. the provider itself that encrypted the data and, for example, the HI. It is not possible to decrypt this data on the system server. The gateway also provides PGP key management through a dedicated interface in the FE, allowing the user to manage their PGP keys. The component is built on MS .Net 6 technology and has integrated CryptoController component as distributed by the NHIC.

Outputs: There are two types of outputs for end users who have to read these outputs either in aggregate form without identifying the individual (e.g. charts and summary statistics), or as individual data lines. Both of the end users access the results via the web browser on the FE web portal.

Email server: The SMTP email serves facilitates registration of HCPs into the system by sending and receiving registration emails.

B. Data flows and communication

The system is intended for HCWs who enter demographic and clinical data of patients treated with studied medication. At each visit HCP enters the clinical data required by the system. Demographic data or another identifying set of data are subsequently encrypted and sent to the BE part of the application and then preserved in the DB. The BE part of the application also ensures the preparation of the content of the XML message in the form of an examination record, into which it serializes in a defined form the clinical data stored in a structured way in the DB. These data are subsequently enriched with patient identification in the local Gateway component and sent to the NHIS by calling the specific service (figure 2) or the purpose of displaying encrypted demographic data, these encrypted data are sent to the local Gateway component, which decrypts them based on the presence of PGP keys in memory and provides them to the FE part running locally in the HCP browser, in case of a request to display them by an authorized actor (HCP or HI).

Before the actual use of the system, a HCP logins or registers to the system using an ePHI card and a reader provided by NHIS. ePHI card is a sufficient security means to verify the identity of the HCP. The Email server establishes the registration during the first instance.

IV. CONCLUSIONS

The system fulfils the requirements as defined with regard to the Slovak and European legislation in force and the user's normal requirements:

- Easy accessibility of the system for the needs of HCPs in whose health care the target groups of patients are
- Provide a friendly and simple user environment
- Secure data both during transport (in-transfer) and after persistence (at-rest)
- Secure sensitive demographic data through encryption
- Easy registration of users at the entry of the system (health worker)
- Use of existing and used security means for user authentication.
- As of the date of preparation of this manuscript, the implementation of this system in the Slovak environment has started at the National Centre for Health Information (NHIC), the national operator of the e-health system designated by the Ministry.
- Stress and safety tests in live operation have not yet been carried out.

ACKNOWLEDGMENT

The version published here is subject to continuous technological changes as its deployment in the national information infrastructure evolves.
The system has been developed by CEEOR s.r.o., and is currently being evaluated for implementation for use by the MoH and the NHIC.
The work has been supported by research grant SGS22 No. 133/OHK4/2T/17.

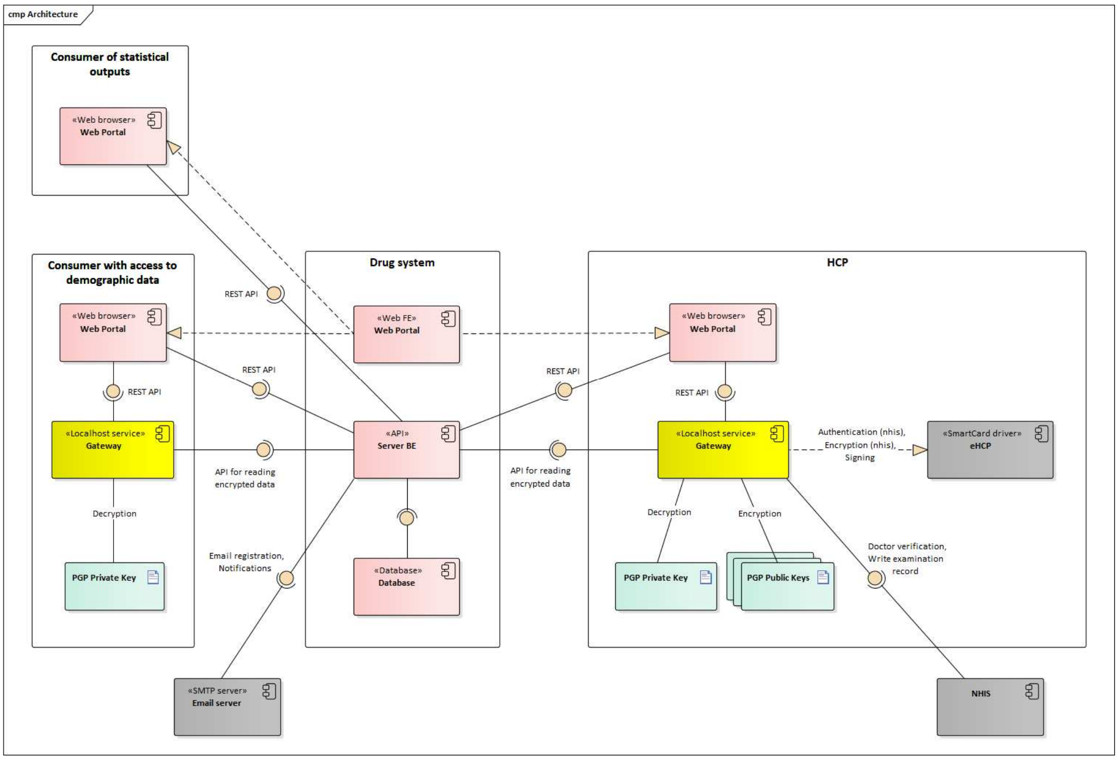

Fig. 1. System architecture and interactions.

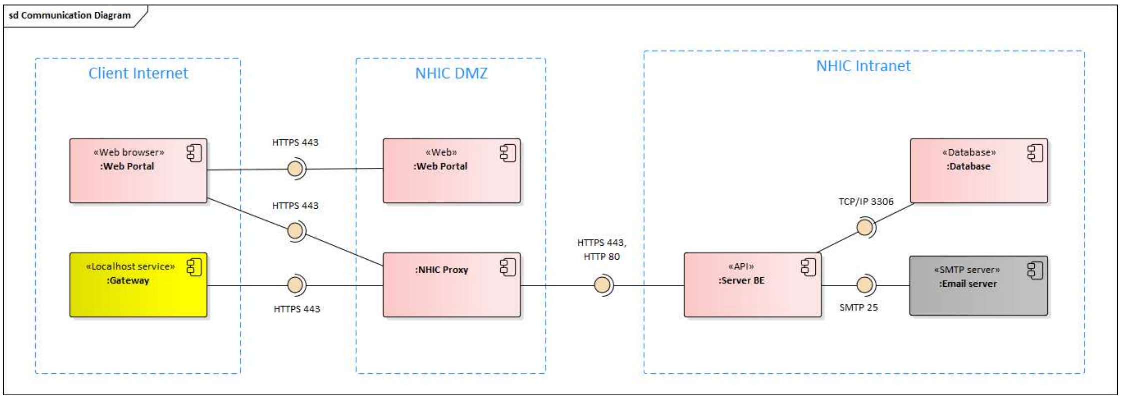

Fig. 2. System communication diagram between the client and the NHIC.

References

[1] M. Klemp, KB. Frønsdal, K. Facey. What principles should govern the use of managed entry agreements? Int J Technol Assess Health Care, 27, 2011, pp. 77-83.

[2] E. Andersson, J. Svensson, U. Persson, P. Lindgren. Risk sharing in managed entry agreements—A review of the Swedish experience. Health Policy, 124, 2020, pp. 404-410.

[3] JC. Bouvy, C. Sapede, S. Garner. Managed entry agreements for pharmaceuticals in the context of adaptive pathways in Europe. Front Pharmacol. 9, 2018, pp. 1-8.

[4] M. Dabbous, L. Chachoua, A. Caban, M. Toumi. Managed Entry Agreements: Policy Analysis From the European Perspective. Value in Health. 23, 2020, pp. 425-433

[5] M. Wenzl, S. Chapman. Performance-based managed entry agreements for new medicines in OECD countries and EU member states: How they work and possible improvements going forward. OECD Health Working Papers. 2019.

[6] CY. Lu, C. Lupton, S. Rakowsky, ZUD. Babar, D. Ross-Degnan, AK. Wagner. Patient access schemes in Asia-pacific markets:Current experience and future potential. J Pharm Policy Pract. 8, 2015, pp. 1-12.

[7] JJ. Carlson, S. Chen, LP. Garrison. Performance-Based Risk-Sharing Arrangements: An Updated International Review. PharmacoEconomics. 35, 2017, pp. 1063-1072.

[8] A. Reuter, A. Abdelmaksoud, K. Boudaoud, M. Winckler. Usability of End-to-End Encryption in E-Mail Communication. Front Big Data. 14, 2021.

[9] J. Petters. What is PGP Encryption and How Does It Work? Varonis. 2020. p. 1. Available: https://www.varonis.com/blog/pgp-encryption

[10] G. Kelly, B. McKenzie. Security, privacy, and confidentiality issues on the internet. Journal of Medical Internet Research, 4, 2002.