**[Individual] Industry Application of the Technology**

**1. Select an industry (one) that has either been changed or likely to be changed with your chosen Tech.**

Cross-institutional sharing of healthcare data is a complex undertaking with the potential to significantly increase research and clinical effectiveness[1]. First and foremost, institutions often are reluctant to share data because of privacy concerns[7], and may fear that sending information will give others a competitive advantage[8]. Next, even if privacy concerns could be addressed, there is no broad consensus around the specific technical infrastructure needed to support such a task[9]. Finally, healthcare data itself is complex, and sending information across institutional boundaries requires a shared understanding of both data structures and meaning. Even assuming data can be shared efficiently and securely, these interoperability issues left unchecked will limit the utility of the data. Despite evidence that the value of healthcare data exchange is large[3], these issues, described below, remain significant barriers.

**Goals**

The main goal of this work is to describe an approach to effectively and securely share healthcare information within a data sharing network. We believe that a patient’s record should be consistent and available across institutional boundaries, and the terms of its access strictly dictated by the patient. As a secondary goal, this data should not only be shared, but shared in such a way that all interested parties can understand the structure and meaning, ultimately leading to improved data utility and patient care.

**Business Value**

Both the patient and the provider are positioned to benefit from a robust data exchange platform. Viewed from both perspectives, one may see that the quantifiable benefits gained by providers and organizations[5] are paralleled by greater convenience and better care outcomes for the patient.

**Patient Perspective:**

– Patients no longer need to coordinate the tedious and frustrating task of gathering records from various providers to send to their specialist. Instead, they would provide the specialist access to the blockchain, enabling them access to the data as they see fit.

– Patients retain control of their data without having to be data stewards – meaning, they no longer have to spend time and energy keeping their data managed and up to date. They also no longer need to manually reconcile the data when they visit multiple providers, which can be a non-trivial task.

– Ultimately, better and more available data leads to better care for the patient.

**Provider and Organization Perspective:**

– The true collaborative nature of creating and sharing data would eliminate many of the challenges of existing Health Information Exchange approaches.

– Healthcare organizations do not have to fight for a data-driven competitive advantage, because they all have access to the same information. This approach will enable organizations to collaborate on care coordination and outcomes-based care.

– Through existing trust/contracts with patients and partner hospitals/organizations, nodes can broadcast alerts or potential threats.

– Data can be shared for research activities including clinical trials, enabling larger and more diverse patient populations.

**2. Take into account of available information for your industry, i.e., not too new where there is no evidence.**

**1.1 Security**

Failing to secure the patient record has financial and legal consequences, as well as the potential to impact patient care. Securing the electronic medical record is a challenging task[6], and the ramifications of a breach are a strong disincentive to sharing data. For this work, we focus on both privacy and anonymity and how they apply to data sharing. Data privacy involves ensuring only authorized parties may access the medical record. This impacts any healthcare system, as patient privacy is not only an ethical responsibility, but a legal mandate[7]. Patient data is also an asset to the institution, and unauthorized access could compromise competitive advantages or reveal proprietary practices. Data anonymity may also be used to secure the record. In this way, identifiable information is left out, and only summary/partial data is shared. This can be acceptable, but is challenging, as it requires a large number of attributes with potential resource or patient care value to be removed from the record in order for it to be considered de-identified[8].

**1.2 Infrastructure**

A significant hurdle to sharing data is the agreement of the supporting technical architecture and infrastructure. Many attempts at data sharing require either (1) a centralized data source, or (2) the transmission of bulk data to other institutions. Both options introduce unique problems. Centralization increases the security risk footprint, and requires centralized trust in a single authority, while bulk data transmission forces institutions to yield operational control of their data.

**1.3 Interoperability**

Interoperability of healthcare records is the extent to which the clinical intent can be conveyed across institutional boundaries. Given the complexities of data in the healthcare domain, this is inherently difficult to achieve[9]. We examine interoperability within the context of two facets: Structure and Semantics, each necessary for the successful exchange of healthcare data[10]. Data structure, or the attributes and data elements use to convey information, is an important part of interoperability. Healthcare data is complex, and heterogeneous structures decrease the effectiveness of analysis and reduce understandability. To combat this, several industry-wide standards have been advanced[11]. While effective, there is no one authoritative standard, and aligning data encoded with disparate standards is a non-trivial task. Semantics refers to the use of terminologies and vocabularies to describe data meaning, or to codify the data. This codification of healthcare data is important to its interpretation, but is only effective if all parties agree upon the same codification schemes, or controlled terminologies[12]. Often, subsets of vocabularies are used to scope a particular domain of interest. These subsets, called Value Sets, may be used in conjunction with structural models to constrain the allowable codifications for attributes or attribute types.

This process of obtaining and sharing medical records is ineffective for the following reasons:

• It is slow since copies of medical data must be prepared, delivered, and picked up by patients. The law allows providers up to 30 days to supply medical records to patients, although some providers may only take 5-10 business days to prepare non-critical health records [22].

• It is insecure because data copies may be lost or stolen during their physical transmission by patients from one location to another.

• It is incomplete since as patient health history may be fragmented because their data is stored in disparate and siloed systems. There is no single source that stores all the medical records of an individual, so patients must therefore be responsible for keeping track of when and where they received health services in order to request copies of their medical history.

• It lacks context since today’s healthcare systems are provider-centric instead of patientcentric, thereby preventing patients from taking control of their own health records and having knowledge of what is done to their data or who has accessed their data [23].

**3. Each group member to have a different industry:**

A key problem in production healthcare systems today is the lack of secure links that can connect all independent health systems together to establish an end-to-end reachable network [9] while protecting healthcare professionals with some level of anonymity (privacy). Although data standards like HL7 [10] and FHIR [11] provide basic interoperability for data exchange between trusted systems, this level of interoperability is limited to the implemented standards and requires data mapping between systems in most if not all cases. Maintainability of these systems is also hard to achieve since an interface change on one system requires other parties in the trusted network to adapt the change as well.

**3.1 Detailed discussion of 2 real world IT examples**

**3.1.1 Patient-Controlled Cancer Data Sharing**

Cancer diagnoses and treatment plans are rarely black-and-white, i.e., they involve many considerations due to the complexity of tumor cases and the number of available treatment options [Multidisciplinary Cancer Care: The Benefits of a Tumor Board. (n.d.). Retrieved March 01, 2018, from <https://www.maacenter.org/blog/multidisciplinary-cancer-care-the-benefits-of-a-tumorboard>]. Getting fresh perspectives from different specialists can help narrow down the options and may shorten the time from (suspected) diagnosis to treatment for a cancer patient. In the U.S. today, most hospitals have included at least one tumor board, which is a multidisciplinary team of medical, surgical, radiation oncologists, and other specialists and care providers, to review and discuss individual cancer patient’s condition and treatment options in depth [2]. Despite the increasing effort to encourage cancer care collaboration among oncologists, patients and families remain passive in the decision-making process. A largescale enterprise hospital may involve specialists from a wider range of disciplines, whereas a smaller-scale care center may have limited resources to expand their tumor boards. The quality of life that is important to cancer patients may be neglected due to patient disengagement.

In reality, patients may wish to reach out to a new provider for a second opinion on their medical conditions and/or treatment plan. To share critical data today, patients have to obtain copies of their medical reports from their current provider, which may include their family history, visit history, prescriptions, current diagnoses and treatment options, and so on. All reports will then be delivered physically to the new provider. In this technologically advanced society, patients with critical conditions should be least involved in the manual data sharing process and have the critical data shared in a timely manner to prevent delays in treatment. A patient-controlled data sharing feature is missing from the existing health systems for cancer patients to promptly request a second opinion and also selectively share information. Instead of creating a new trusted “middle man” that mediates the establishment of trust relationships between providers/hospitals, Blockchain technology offers the opportunity for trustless exchange and disintermediation that allow existing trust relationships to be aggregated and propagated across various organizations and providers. This approach is similar to the patient referral process, except the referrals are not limited to a single provider’s network. Instead, they could be expanded across different regions, states, and even countries. A Blockchain-based system can also capture existing trust relationships between patients and providers, allowing patients to decide which provider(s) can share their data.

**3.1.2 Personal Health Records**

Unlike the current standard practice of using provider-centric EHRs to maintain and manage patient data, personal health records (PHRs) are applications used by patients, the true data owners, to access and manage their health information. The ultimate goal for PHRs is to help patients securely and conveniently collect, track, and control their complete health records compiled from various sources, including provider visit data, immunization history, prescriptions records, physical activity data collected from Smartphone devices, and many more. PHRs enable patients to control how their health information is used and shared, verify the accuracy of their health records, and correct potential errors in the data [53]. Enterprises and technology companies, such as Apple and Microsoft, have begun exploring centralized solutions with their Apple Health [40] and Microsoft HealthVault [54] products. Centralized approaches do not resolve the data sharing problem at its core, however, and may therefore face similar hurdles as existing disparate EHR systems. Blockchains, in contrast, allow distribution of control to individuals via decentralization enabled by consensus algorithms. By creating a widely accessible and secure data distribution service that connects to existing health systems, patients can easily aggregate their medical history without requesting a copy from every provider they have visited. Connections to personal smart devices are also possible as Blockchains remove the “distrust” between healthcare professionals and third party health tracking apps and services. Furthermore, permission-based data distribution can be set up with smart contracts to guarantee that patients (1) remain in control of their data access, (2) are aware of the origin of aggregated data sources, and (3) are informed when their data is accessed by providers. Data origin and access history are made transparent to the patients through immutable audit logs to always keep patients up-to-date of when and by whom their health information is retrieved.

**3.2 The discussion should also compare and contrast the 2 IT related examples in relation to the topic.**

**4. Discussion should focus on relating to the innovation concepts (can refer to the group’s innovation concepts).**

Reference:

[1] En.wikipedia.org. (2018). *Disruptive innovation*. [online] Available at: https://en.wikipedia.org/wiki/Disruptive\_innovation [Accessed 25 Apr. 2018].

[2] Peterson, K., Deeduvanu, R., Kanjamala, P. and Boles, K., 2016. A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare* (Vol. 1, pp. 1-10).

[3] Jan Walker, Eric Pan, Douglas Johnston, Julia Adler-Milstein, et al. The value of health care information exchange and interoperability. Health Affairs, 24:W5, 2005.

[4] Randolph C Barrows and Paul D Clayton. Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association, 3(2):139–148, 1996.

[5] Centers for Disease Control, Prevention, et al. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. MMWR: Morbidity and Mortality Weekly Report, 52(Suppl. 1):1–17, 2003.

[7] Chris Clifton, Murat Kantarcioˇglu, AnHai Doan, Gunther Schadow, Jaideep Vaidya, Ahmed Elmagarmid, and Dan Suciu. Privacy-preserving data integration and sharing. In Proceedings of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, pages 19–26. ACM, 2004.

[8] Yaorong Ge, David K Ahn, Bhagyashree Unde, H Donald Gage, and J Jeffrey Carr. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. Journal of the American Medical Informatics Association, 20(1):157–163, 2013.

[9] Paul C Tang, Joan S Ash, David W Bates, J Marc Overhage, and Daniel Z Sands. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. Journal of the American Medical Informatics Association, 13(2):121–126, 2006.

[8] US GPO. CFR§ 164 security and privacy. 2008. http://www.access.gpo.gov/ nara/cfr/waisidx 08/45cfr164 08.html. Accessed: 2016-08-06.

[9] Charles N Mead et al. Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap? Journal of Healthcare Information Management, 20(1):71, 2006.

[11] A Begoyan. An overview of interoperability standards for electronic health records. USA: Society for Design and Process Science, 2007.

[12] James J Cimino et al. Desiderata for controlled medical vocabularies in the twenty-first century. Methods of Information in Medicine-Methodik der Information in der Medizin, 37(4):394–403, 1998.

[13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[22] Olivier Bodenreider, Duc Nguyen, Pishing Chiang, Philip Chuang, Maureen Madden, Rainer Winnenburg, Rob McClure, Steve Emrick, and Ivor DSouza. The NLM Value Set Authority Center. Studies in Health Technology and Informatics, 192:1224, 2013. [23] Steffan D Norberhuis. MultiChain: A cybercurrency for cooperation. PhD thesis, TU Delft, Delft University of Technology, 2015.

9 Zhang, P., Walker, M., White, J., Schmidt, D.C., and Lenz, G.: ‘Metrics for assessing Blockchain-based healthcare decentralized apps’, Proceedings of 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), October 12-15, 2017, Dalian, China

10 Dolin, R.H., Alschuler, L., Beebe, C., Biron, P.V., Boyer, S.L., Essin, D., Kimber, E., Lincoln, T., and Mattison, J.E.: ‘The HL7 clinical document architecture’, Journal of the American Medical Informatics Association, 2001, 8, (6), pp. 552-569

11 Bender, D., and Sartipi, K.: ‘HL7 FHIR: An Agile and RESTful approach to healthcare information exchange’, in Editor (Ed.)^(Eds.): ‘Book HL7 FHIR: An Agile and RESTful approach to healthcare information exchange’ (IEEE, 2013, edn.), pp. 326-331

40 IOS - Health. (n.d.). Retrieved March 01, 2018, from https://www.apple.com/ios/health/ 41 Zhang, P., White, J., Schmidt, D.C., Lenz, G., and Rosenbloom, S.T.: ‘FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data’

42 Multidisciplinary Cancer Care: The Benefits of a Tumor Board. (n.d.). Retrieved March 01, 2018, from <https://www.maacenter.org/blog/multidisciplinary-cancer-care-the-benefits-of-a-tumorboard>

53 Tang, P.C., Ash, J.S., Bates, D.W., Overhage, J.M., and Sands, D.Z.: ‘Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption’, Journal of the American Medical Informatics Association, 2006, 13, (2), pp. 121-126

54 Microsoft HealthVault. (n.d.). Retrieved March 01, 2018, from https://www.healthvault.com/en-us/