Healthcare-Related Data in the Cloud: Challenges and Opportunities

Valentina Casola
University of Naples "Federico II"

Aniello Castiglione
University of Salerno

Kim-Kwang Raymond Choo
University of Texas at San Antonio

Christian Esposito
University of Salerno

EDITOR:
KIM-KWANG RAYMOND CHOO

University of Texas at San Antonio
raymond.choo@fulbrightmail.org

THE MODERN HEALTHCARE SYSTEM IS DATA INTENSIVE. To efficiently care for their patients, various actors and entities (medical practitioners, nurses, allied health professionals, hospitals, clinics, hospices, and so on) often need to exchange significant amounts of information in real time.

Figure 1 is a schematic representation of data exchange between various actors and their mutual dependencies in an example healthcare system, where patients play a pivotal role.[1] In general, after a patient visits a healthcare provider (such as a general practitioner for an annual physical examination, a nurse practitioner to obtain a flu vaccine, or a radiographer for an x-ray), he or she will likely require additional medical services or attention over a period of time (for example, specialized medical examinations such as magnetic resonance imaging scans, or routine medical examinations such as blood tests, cholesterol checks, and blood-sugar checks).

We can broadly categorize healthcare as primary or secondary. Secondary healthcare providers, such as hospitals and other medical institutions, provide additional health services to complement those offered by general practitioners. Secondary healthcare can also be provided by pathologists working at laboratories and performing specific tests on patients. Both public and privately run healthcare providers generally have an administration and several other departments.

As Figure 1 illustrates, an extensive exchange of information takes place among primary and secondary healthcare providers. Without any loss of generality, we distinguish two communication flows: from primary healthcare providers to secondary healthcare providers, and from secondary healthcare providers to primary healthcare providers.

In the first communication flow, secondary healthcare providers retrieve patient data to provide the appropriate follow-up examination (such as specialist medical services and examinations). In the second communication flow, primary healthcare providers are notified whenever new information (such as medical records) relating to a given patient is available, thus facilitating a smooth handover. Also, at the administration level of a healthcare provider, there's a communication flow in which the administration collects relevant documents for a range of functions (such as billing). This flow is similar to the

 2325-6095/16/$33.00 © 2016 IEEE

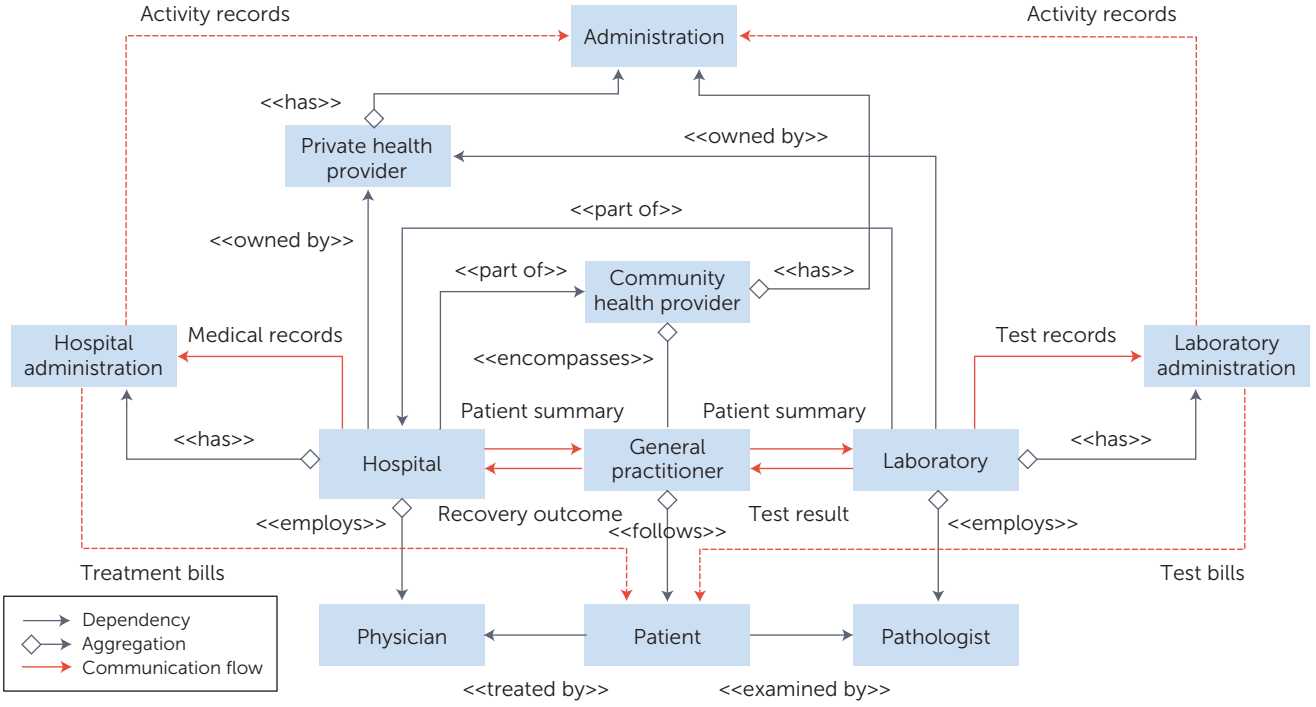

FIGURE 1. Overview of dependencies and communication flows in the healthcare domain.

second communication flow between primary and secondary healthcare providers. Such a communication flow is also of interest to the administration of the secondary healthcare structures and providers.

Healthcare providers have been shifting from paper-based record systems[2] to electronic medical record (EMR)[3] and electronic health record (EHR)[4] systems to improve patient care quality.[5,6] Internal and external patient mobility has also been increasing, for example, due to inter- and cross-country migration and the availability of cheaper treatment in other countries. In Europe, for example, the 1985 Schengen Agreement and the central principle within the European Union (EU) of freedom of movement for people, goods, and services (see Directive 2011/24/EU on patient rights in cross-border healthcare; http://eur-lex.europa.eu/eli/dir/2011/24/oj) also played a role in increasing external patient mobility.

Thus, we need an efficient and secure way to share medical data between various healthcare providers and other key stakeholders (including patients), regardless of geographical locations. Such a scenario, however, complicates the design and implementation of the underlying information and communications technology (ICT) infrastructure, which can comprise systems that aren't interoperable. For example, integrating all existing local (including legacy) systems to satisfy the following requirements remains a research and operational challenge:

- having a decentralized and distributed design,
- allowing asynchronous interactions,
- providing flexible data and service integration, and
- supporting security mechanisms with respect to privacy regulations.

Currently, there's an ongoing debate on the utilities and challenges of hosting and sharing of medical data in a cloud platform, despite the potential benefits of outsourcing health-related data to the cloud for storage, processing, and sharing (including cost optimization, ease of data management, flexibility, maintainability, and scalability).

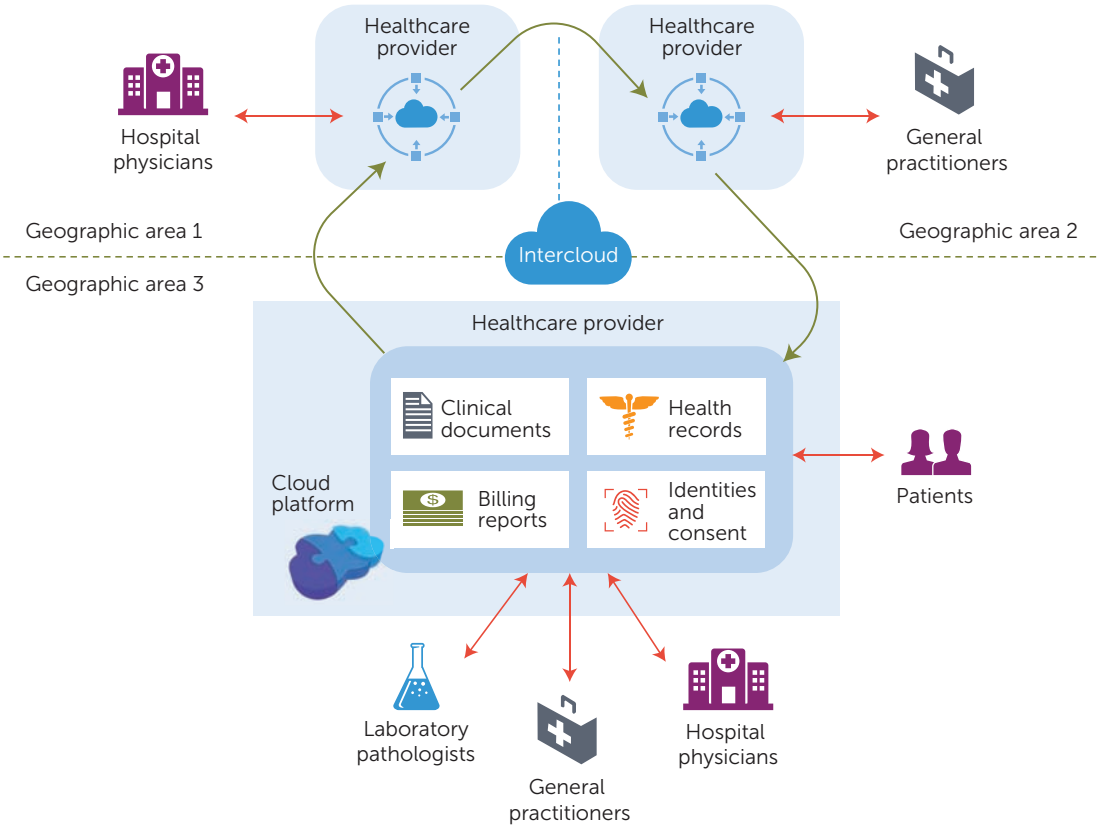

FIGURE 2. Cloud-based medical data management.

Figure 2 illustrates how cloud computing can be adopted within the healthcare domain for medical data management. Each healthcare provider has access to or hosts a cloud platform, which can be used to store, process, and share data among patients, healthcare personnel, and other relevant stakeholders (such as centers for disease control and prevention if an outbreak is detected). Such a platform can also host services for managing the identities of all registered users, patient consent, and patient health records and reports. The cloud platform can also support the healthcare provider's administrative processes, such as generating and updating billing reports and disbursing funds. To meet patients' mobility needs, public and private cloud platforms used by different healthcare providers can be federated using an intercloud infrastructure to share patient data, generate billing records, and so on.[7]

As with all technologies, cloud deployments in the healthcare industry are vulnerable to threats posed by both external attackers and employees or vendors associated with the cloud service provider (that is, insider threats). Security researchers have attempted to solve such challenges, for example, by using cryptographic solutions such as privacy-preserving cloud solutions.[8] In recent work, for example, a team of computer security researchers presented a framework for handshake schemes in mobile healthcare social networks.[9] They constructed an efficient cross-domain handshake scheme that allows symptoms matching within mobile healthcare social networks. This allows patients who have matching symptoms and are registered with one or more healthcare providers to mutually authenticate each other and establish a secure communication session. The authors implemented a prototype of the scheme using an An-

droid app.[9] Another work presents a cryptographic scheme designed to provide fine-grained database field search on healthcare clouds.[10] The scheme lets an authorized user (such as a healthcare provider or medical researcher) securely and efficiently search for values in the fields of the table of the relevant EHRs.

Lack of control over the outsourced data is another key concern.[11] Various data privacy and healthcare-related legislation regulate sensitive data, such as medical records. For example, the upcoming EU Data Protection Directive states that any personal data generated within the EU is subject to the European law and data can only be shared with a third party if its owner is notified. Again, personal data can't leave the EU, unless it's sent to a country that provides an adequate level of protection (for example, by participating in potential new EU-US data sharing agreements).

Moreover, restrictions on personal data storage and access differ even among states within the same country or region. Within the EU, for example, some countries, like France and Denmark, have broad restrictions, whereas others, like Italy and Germany, have no or limited restrictions for certain types of data. Furthermore, regulations in different countries can conflict, such as the regulation concerning data owners and the regulation concerning datacenter locations. In the United States, the 2001 Patriot Act allows US intelligence agencies to access personal data managed by US companies, without notifying data owners. This is in clear violation of the EU directive, should cloud service providers or healthcare providers decide to abide by the US Patriot Act. In theory, a solution could be to restrict EU datacenters to be located in a European country, but in practice, such a requirement (or restriction) is seldom part of the service-level agreements (SLAs) offered by (major) cloud service providers.

Introducing security-related SLAs is another promising approach to the provisioning of innovative and secure cloud services, including in the healthcare domain. There are, however, several challenges associated with the provision of cloud services based on security SLAs. For example, how do we represent security in such a way that it's understandable by both users and providers, as well as quantifiable and measurable? We also need to ensure that we can automate the provisioning process even in a multicloud environment to avoid vendor lock-in, and continuously monitor the delivered services to enforce the security SLAs.

EU projects, such as Secure Provisioning of Cloud Services based on SLA management (SPECS, www.specs-project.eu),[12] Multicloud Secure Applications (MUSA, www.musa-project.eu),[13] and SLA-Ready (www.sla-ready.eu), are actively researching the definition of security SLA models that can be easily used by customers to express their security requirements and by providers to manage the security services and policies granted to their users. Existing security SLA models primarily provide standard security controls and have innovative security metrics that enable cloud service providers to realistically measure and guarantee security. However, it's still early and both researchers and standardization bodies are still studying the effectiveness of such security SLA models.[14]

THIS IS A FIRST STEP TOWARD THE ADOPTION OF PER-SERVICE SECURITY SLAS, INCLUDING IN THE HEALTHCARE INDUSTRY. Research opportunities include the design of effective security SLA models that will fulfill specific user requirements, such as data geolocation, and compliance with the relevant legislation (for example, the Health Insurance Portability and Accountability Act of 1996 for US healthcare providers) and international standards.

References

1. C. Esposito, M. Ciampi, and G. De Pietro, "An Event-Based Notification Approach for the Delivery of Patient Medical Information," *Information Systems*, vol. 39, Jan. 2014, pp. 22–44.
2. T. Schabetsberger et al., "From a Paper-Based Transmission of Discharge Summaries to Electronic Communication in Healthcare Regions," *Int'l J. Medical Informatics*, vol. 75, nos. 3–4, 2006, pp. 209–215.
3. M. Steward, "Electronic Medical Records," *J. Legal Medicine*, vol. 26, no. 4, 2005, pp. 491–506.
4. K. Häyrinena, K. Sarantoa, and P. Nykänenb, "Definition, Structure, Content, Use and Impacts of Electronic Health Records: A Review of

the Research Literature," *Int'l J. Medical Informatics*, vol. 77, no. 5, 2008, pp. 291–304.
5. R. Hillestad et al., "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs," *Health Affairs*, vol. 24, no. 5, 2005, pp. 1103–1117.
6. R. Hauxe, "Health Information Systems—Past, Present, Future," *Int'l J. Medical Informatics*, vol. 75, nos. 3–4, 2006, pp. 268–281.
7. C. Esposito et al., "Interconnecting Federated Clouds by Using Publish-Subscribe Service," *Cluster Computing*, vol. 16, no. 4, 2013, pp. 887–903.
8. C. Esposito, A. Castiglione, and K.-K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated Clouds," *IEEE Cloud Computing*, vol. 3, no. 1, 2016, pp. 12–17.
9. D. He et al., "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network," *IEEE Trans. Dependable and Secure Computing*, in press, doi: 10.1109/TDSC.2016.2596286.
10. C. Guo et al., "Fine-Grained Database Field Search Using Attribute-Based Encryption for E-Healthcare Clouds," *J. Medical Systems*, vol. 40, 2016, article 235.
11. *Cloud Computing Risk Assessment*, European Union Agency for Network and Information Security (ENISA), 2009; www.enisa.europa.eu/publications/cloud-computing-risk-assessment.
12. M. Rak et al., "Security as a Service Using an SLA-based Approach via SPECS," *Proc. IEEE Int'l Conf. Cloud Computing Technology and Science* (CloudCom), 2013, pp. 749–755.
13. E. Rios et al., "Towards Self-Protective Multi-Cloud Applications: MUSA-A Holistic Framework to Support the Security-Intelligent Lifecycle Management of Multi-Cloud Applications," *Proc. 5th Int'l Conf. Cloud Computing and Services Science*, 2015, pp. 551–558.
14. V. Casola et al., "Providing Security SLA in Next Generation Data Centers with SPECS: The EMC Case Study," *Proc. 6th Int'l Conf. Cloud Computing and Services Science*, 2016, pp. 138–145.

VALENTINA CASOLA *is an associate professor of computer science at the University of Naples Federico II, Italy. Her research interests focus on security methodologies to design and evaluate distributed systems, including cyberphysical infrastructures, cloud systems, and Web services. Casola has a PhD in electronic engineering from the Second University of Naples. Contact her at casolav@unina.it.*

ANIELLO CASTIGLIONE *is an adjunct professor of computer science at the University of Salerno, Italy, and the University of Naples "Federico II," Italy. His research interests include security, communication networks, information forensics and security, and applied cryptography. Castiglione has a PhD in computer science from the University of Salerno, Italy. He's a member of several associations, including IEEE and ACM. Contact him at castiglione@ieee.org.*

KIM-KWANG RAYMOND CHOO *holds the Cloud Technology Endowed Professorship at the University of Texas at San Antonio. His research interests include cyber and information security and digital forensics. Choo has a PhD in information security from Queensland University of Technology, Australia. He's a fellow of the Australian Computer Society and a senior member of IEEE. Contact him at raymond.choo@fulbrightmail.org.*

CHRISTIAN ESPOSITO *is an adjunct professor of computer programming at the University of Naples "Federico II", Italy, and the University of Salerno, Italy, where he's also a research fellow. His research interests include information security and reliability, middleware, and distributed systems. Esposito has a PhD in computer engineering from the University of Naples "Federico II," Italy. Contact him at esposito@unisa.it.*