Governance of Cloud Computing Services for the Life Sciences

Srdan Dzombeta, Persicon, Berlin

Vladimir Stantchev, SRH Hochschule Berlin

Ricardo Colomo-Palacios, Østfold University College, Norway

Knud Brandis and Knut Haufe, Persicon, Berlin

This analysis of the legal regulations for cloud computing in healthcare is based on the authors' expertise in cloud-based data processing for healthcare and life sciences organizations. The proposed implementation roadmap should help organizations govern health data processing and storage.

Novel computing infrastructures and approaches are often applied to improve processes in the healthcare and life sciences domains,[1] with some approaches going as far as incorporating virtual or mixed reality[2] as well as intelligent systems.[3] Cloud computing follows a similar path and is considered one the most important developments in IT.[4] In addition to the general benefits of cloud computing, there's a wide range of specific improvements that the cloud can bring to scientific organizations—particularly in the life sciences. As shown in recent works, these improvements can materialize in the areas of learning[5] and knowledge cocreation,[6] and are inherent to IT best practices, such as service-oriented architectures, Web services, and big data.[7,8]

However, security and privacy are often cited as major concerns when considering cloud computing adoption.[9] Although there are approaches that incorporate cloud computing in the context of patient data[10] and that aim to assess the general security requirements related to introducing the cloud,[11] both the research world and practitioners are still on the lookout for applicable approaches to govern cloud computing adoption in the area of healthcare.

Here, we present an approach that provides guidance for organizations in the life science domain that are adopting cloud computing and other outsourced IT services. We focus on Germany, because it's a jurisdiction with elaborate and restrictive regulations with respect to data protection, particularly in the area of healthcare.[12]

Overview of Legal Regulations

Almost every institution within the healthcare system—from doctor's offices to hospitals to medical insurance companies—must process personal patient data, including sensitive aspects of the patient's health status. In Germany, there is a wide range of applicable regulations that govern the protection of individual rights and the "informational self-determination rights" of patients. The universally applicable Federal Data Protection Act or Bundesdatenschutzgesetz (BDSG) defines health data as a special type of personal data with legally mandated increased protection requirements (section 9, paragraph 3 of the law. The collection, processing, and use of health data is generally allowed only for the purposes of preventive medicine and medical diagnosis, care, or treatment, or for the purpose of managing and administering health services. Such data can be processed only by medical personnel or by other people who possess the same appropriate confidentiality obligations (section 28, paragraph 7 of BDSG). However, a pre-assessment of the legality of this data processing should be conducted by the company's data protection official (section 4f BDSG), Section 5).

When operating IT systems that process health data, both the original organization (for example, the hospital, practitioner, or insurer) and the outsourcing company should implement appropriate technical and organizational precautionary measures, stemming from a list of eight *control requirements* (that is, specific areas that the organization should control with respect to information security, as noted in paragraph 9 and the related annex to paragraph 9 of BDSG. There's a similar requirement for *socially related data* (data that is processed in the context of social security benefits) in § 78a of the Social Codex

or Sozialgesetzbuch (SGB) and the related annex.

The legal framework of applicable laws stipulates only general requirements; each organization then must define and implement more specific measures. For example, an organization working with health-related data should apply general measures for protecting personal data (limited access, for example), but the organization should extend such measures to ensure secure data transmission (using encryption, for example). Furthermore, if the organization operates systems for more than one client (perhaps processing appointment data or analysis data for multiple general practitioners), then it should implement additional measures to separate each client's data. For hospital management systems in particular, there are specific recommendations for compliance.[13] Requirements that are similar to these recommendations also apply in cloud computing and outsourcing scenarios, because the providers are expected to satisfy the client organization's security requirements. These more specific requirements are derived from regulations for medical confidentiality, social data, and state-specific rules (each state—say as Bavaria, or Hamburg—has its own rules).

Keeping Medical Data Confidential

Medical confidentiality ensures the trusted relation between a doctor and a patient. In Germany, this relation is regulated in the Model Professional Code for Physicians in Germany or Muster-Berufsordnung für die deutschen Ärzte und Ärztinnen (MBO-Ä) with medical confidentiality specified in part II, paragraph 9 of the MBO-Ä (http://www.bundesaerztekammer.de/downloads/MBOen2012.pdf). A breach of confidentiality is considered a criminal offense, and such a breach can result from archiving patient data with a service provider without the patient's prior written consent. However, prior written consent should include specific data and legal information about the service provider, and obtaining such consent often isn't feasible.

Protecting Social Data

Social data denotes all personally related data that concerns the social aspect of a person. The increased confidentiality requirements with respect to such data are defined in section 1, paragraph 35 of SGB I. A specific example of regulations in this area is the recently introduced electronic health card or elektronische Gesundheitskarte (eGK). Requirements concerning data protection in the context of the eGK are specified in Volume V of SGB, with particular regulations concerning encryption and access-control lists in § 291a SGB V.

To ensure compliance, the newly founded joint venture of German health insurers—Gematik—has specified an extensive security concept that will also be applicable to cloud computing and other outsourcing providers who will work with the eGK (see www.gematik.de/cms/de/spezifikation/abgekuendigte_releases/release_2_3_4/release_2_3_4_datenschutz/datenschutz/release_2_3_4_sicherheitskonzept.jsp [in German]).

Coordinating State-Specific Rules

Hospitals in Germany are particularly affected by state-specific rules with respect to data protection and information processing. A variety of state-specific hospital laws exist that often stipulate different requirements related to patient data processing.

Let us consider the Berlin State Hospital Law or Landeskrankenhausgesetz (LKG) of Berlin and the Health Data Protection Law of North Rhine-Westphalia (or Gesundheitsdatenschutzgesetz) as examples. They both include regulations regarding data transmission and disclosure. For example, hospitals in Berlin are only allowed to process patient data in-house or to outsource this processing to another hospital. Other providers can process patient data under the hospital's mandate only if they are prevented from mapping the data to a certain person or deriving personal information (section "24 Datenschutz" of LKG Berlin). In the case of North Rhine-Westphalia, there are explicit requirements that medical confidentiality should always be assured when processing data electronically.

Following a Mandate

Outsourcing in the context of cloud computing and other scenarios, such as IT service provision, typically constitutes the act of data processing under a mandate (Datenverarbeitung im Auftrag— or as BDSG calls it "Collection, processing or use of personal data on behalf of others") as stipulated by section 11 of BDSG. Consequently, the contractual relationship between the client and service provider involves specific data protection and information security requirements.

Specifying and Meeting Requirements

The contract should specify the type and scope of the intended data use, the client's control rights (such as the right to conduct independent audits on the premises of the service provider), as well as specific technological and organizational measures that the provider will implement to comply with section 9 BDSG.

The client thus must be careful when selecting the service provider, ensuring that the provider is capable of taking the appropriate technological and organizational measures (section 11, paragraph 2(4) of BDSG specifies that the client must carefully select the provider). This obligation to verify that the provider is taking the appropriate measure is known as the "control obligation," and it can be fulfilled in person or using experts, information security management system auditors, self-disclosure forms from the provider, as well as certificates or proofs of established data protection concepts from the provider. If the client fails to comply with this control obligation, the government or independent regulatory bodies can fine the client.

The obligation further continues during the actual data processing through regularly controls. The frequency of such follow-up verifications differs in accordance with the scope of data processing, the associated risks, the innovation cycle of related technologies, as well as the type of the processed data. Relevant cloud computing providers in Germany conduct yearly audits implemented by independent organizations and make the audit reports available to their clients (see www.pironet-ndh.com/site/pndh-website-site/node/269414/Lde [in German]).

Compared to these general requirements of data processing under a mandate by an outsourcing provider, the specific case of processing social data is regulated similarly but by a different law (section 80 of SGB X). There are several important differences between section 80 of SGB X and section 11 of BDSG that need to be considered. According to SGB X, client organizations are expected to use only providers from the public administration. A client can only use a private cloud computing provider if using a public provider will cause substantial problems to normal operations or if the private provider offers substantial cost benefits (both of which would be difficult to assess and verify formally).

Considering the Provider Location

When considering data processing under a mandate as stipulated by section 11 BDSG, organizations in the life sciences should ensure that the cloud computing providers process data exclusively within the EU or the European Economic Area (EEA). Due to the EEA-wide harmonization of data protection regulations in Directive 95/46/EC (especially considering current efforts to further increase levels of protection), cloud computing providers from the EU are expected to meet EU criteria even if they operate outside of the EU.[14] Nevertheless, we recommend that when drafting contracts with providers that operate outside of the EU, clients should specify that data processing outside the EU/EEA is not allowed.

Cloud computing providers located outside countries and jurisdictions of the EU/EEA can't conduct data processing under a mandate as stipulated by section 11 of BDSG. From the viewpoint of BDSG, data processing in such jurisdictions is considered data transmission, which requires specific authorization. Determining whether such transmission can be authorized is conducted in two steps.

First, it should be assessed whether the specific country already exhibits a proper data protection level (section 2(2), paragraph 4b of BDSG). The EU Commission itself conducts such assessments based on international treaties and has currently found proper levels for only a handful of countries, including Argentina, Australia, Guernsey, and Canada. The US is currently not among these countries, but based on US-EU Safe Harbor Framework (http://export.gov/safeharbor), certain certified providers are considered safe. If the general level of data protection isn't considered appropriate, data transmission can only be contractually specified using the preformulated EU standard contract clauses in verbatim. Furthermore, because these clauses only partially cover the requirements of the BDSG, it's recommended that the requirements of section 11, paragraph 2 of BDSG be covered in the contract.

Second, in addition to ensuring the appropriate data protection level of the country where the provider processes the data, the organization still needs a legal foundation for data transmission in a country outside the EU/EEA. The case of health-related data is specifically regulated in section 28 paragraphs 6–9 BDSG. Transmission of a person's data without explicit consent is possible under extremely limited conditions. For example, the processing of such data can only be conducted by people who are subject to the medical confidentiality requirement. This will be the case only if the provider is considered a so called "accomplice" ("Gehilfe" in German), which is a professionally active assistant of the doctor as defined in section 3(2), paragraph 203 of the Criminal Code or Strafgesetzbuch (StGB; www.iuscomp.org/gla/statutes/StGB.htm#203), which is not usually the case with a typical client-provider relationship.

Understanding the Risks of Security Breaches

Revelations about the extent of programs such as the PRISM surveillance program and others that are implemented to protect national security according to the US Patriot Act and the Foreign Intelligence Surveillance Act show that most of these surveillance methods constitute data access in the sense of BDSG. Regardless of the apparent legal conformity from the viewpoint of US laws, access to someone's medical data that comes from life science applications within the EU constitutes a grave violation of the fundamental rights of privacy and data protection of EU citizens.

The EU parliament has decided to further investigate PRISM and other data gathering activities (see www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN#). Because all US-based providers that were publicly identified as participating in PRISM are also signatories of the Safe Harbor agreement, there are reasonable doubts about the compliance of data processing by cloud computing providers in the US from the viewpoint of EU-based organizations. This is even more critical for the sensitive data that is processed in the life sciences.

Implementation Roadmap

When considering the already presented legal aspects and inherent risks of cloud-based data processing for organizations in the areas of healthcare and life sciences, it's evident that the organizations should define their requirements with respect to data privacy. The definitions should consider aspects such as the selection and evaluation process of possible cloud computing providers, specific detailed requirements about service-level agreements (SLAs), as well as specifically required organizational and technical measures to which the cloud computing provider should conform. This dramatically increases transaction costs in the cloud computing market, which is already marked by high levels of information asymmetry.[15]

Some existing automated approaches for matching demand and supply, even for the SLA phase,[16] are only of limited benefit, because they can't account properly for complex organizational measures. However, specific technical measures can be clearly stated in automated supply statements (for example, the service level objectives[12]) and can therefore be easily matched to automated requirements.

Recommendations for specific measures can be derived from relevant standards, such as the Baseline IT-Security or IT-Grundschutz standard by the Federal Office for Information Security or Bundesamt für Informationssicherheit (BSI; https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html). For example, the standard specifies "data protection with cryptographic methods." It also offers information about how to select the proper cryptographic methods, manage security keys, and reliably configure encryption modules. In addition, more generally applicable standards, such as ISO 27001 and ISO 291004 (see www.iso.org), can serve as a framework for managing information security and protecting data within the context of cloud computing and other outsourcing relationships.

The already discussed, preformulated EU standard contract clauses should be incorporated verbatim into the service contract. Significant attention should be paid to the detailed description of technical and organizational measures, because these constitute the contractually agreed upon security concept. The client organization serving the life sciences or healthcare fields should also consider continuity management in particular, because emergency and failover scenarios often lead to substantial security breaches. The volatility and frequent changes in the cloud computing market require detailed specifications about the proper and adequate handling of data in the case of the outsourcing contract's termination.

The sheer amount and diversity of the data protection requirements means that an integral part of organization-wide information security management systems must be the governance of cloud computing and outsourcing relationships. In this context, we propose extending existing information security management systems with a roadmap and an approach for processing data in the life sciences in cloud computing and other outsourcing scenarios. The approach considers four general phases and thus can be easily applied in the context of most IT-governance approaches.[17] The four phases are

- plan,
- select a cloud computing provider,
- negotiate contractual specified delivery mechanisms, and
- monitor and govern operation.

Figure 1 shows an overview of the proposed approach. It follows the same logic as the approach proposed in other work,[18] but we've adapted and extended it in several ways. The original approach

considers a specific lifecycle model (the service-oriented architecture, or SOA, lifecycle), while the approach proposed here considers four general phases that can be adapted to a variety of lifecycle-based approaches. Furthermore, the SOA-lifecycle approach considers dependability as an objective, while in our approach, we consider all compliance-related aspects of a cloud computing outsourcing project. Figure 1 also includes examples of objectives that are relevant for the specific phase. A more detailed list of objectives and activities is given in Table 1.

Figure 1. Overview of the proposed approach for processing data in the life sciences in cloud computing and other outsourcing scenarios. It considers four general phases and can be adapted to a variety of lifecycle-based IT governance approaches. Table 1 provides details about every phase.

Table 1. Roadmap for assessing cloud computing providers by organizations in the healthcare and life sciences domains.

Roadmap	Question
Plan	1. Which data is affected by the outsourcing decision: health-related, social, or medically confidential?
	2. Which legal frameworks are applicable: Federal Data Protection Act or Bundesdatenschutzgesetz (BDSG); Social Codex or Sozialgesetzbuch (SGB); State-specific data protection laws or Landesdatenschutzgesetze LDSG); State-specific hospital laws or Landeskrankenhausgesetze (LKG); Criminal Code or Strafgesetzbuch (StGB); or others?
	3. Which existing risks are associated with the outsourcing decision: data availability, confidentiality, or integrity?
	4. Which requirements exist concerning data protection: appropriate security architecture, data encryption and cryptography, identity and rights management, control possibilities, monitoring and security incident management, contingency plans and measures, and others?
	5. Which barriers are present? No data storage outside Germany, outside the EU or European Economic Area (EEA), or outside some other area?
Select the provider	6. Is the provider compliant with legal and data protection requirements?
	7. Where does the provider store data (EU/EEA or other jurisdiction)? If other, does an appropriate protection level exist? If the US, is the provider Safe Harbor certified? If corporate structures of the provider reside outside the EU (for example, internal providers residing outside EU), how are they involved in the data processing?
	8. Does the provider have an information security management system (ISMS) concept?
	9. How was the ISMS concept assessed concerning appropriateness of technical and organizational measures and how is the result of the assessment documented?
	10. Does the provider have current and internationally established certifications (for example, ISO 27001)?
Negotiate	11. Is the cloud computing service precisely and clearly formulated?
	12. Are appropriate control rights for the cloud user organization and corresponding obligations for the cloud provider being specified?
	13. Are there clauses that govern the contingency operation and the return of data in the case of bankruptcy of the cloud provider?
	14. Is there a mandate for data processing ("Vereinbarung zur Auftragsdatenvereinbarung," see section 11, paragraph 2 of BDSG and section 80, paragraph 2 of SGB X)
	15. When operating in non-EU jurisdictions, are the EU standard clauses or Binding Corporate Rules part of the agreement?

	16. Are there specific, relevant service-level agreements? Do they outline the availability and dependability requirements, response and restoration deadlines, computing power, and support details?
	17. Are there specific contingency regulations for the case of catastrophic failures?
Monitor and govern	18. Are controls being conducted regularly? Are there assessments of the agreed-upon technical and organizational measures?
	19. Are the security concepts being regularly assessed? Are they current, and do they correspond to the current state of the art?

Cloud systems still face some obstacles to their adoption.[19] Specific doubts remain that externally controlled cloud services can be adequately protected, and industry-specific offerings are being assessed to ensure security and privacy.[20] Health systems are crucial when considering technological developments, and the importance of the cloud for the health sector has been underlined by previous studies in countries such as China.[21] In the regulation field, literature has analyzed cloud services in several environments including general studies on EU data privacy regulations,[22] general records management,[23] and US federal electronic health record regulations[24] along with studies devoted to analyzing transborder health data in cloud settings.[25]

As healthcare as a sector presents an increasing share of the GDP in almost every country, and its current share of GDP is already high in most developed countries, we can expect that efforts to improve the quality and reduce the costs of healthcare will increase. This is also the case with applications within the broader area of life sciences, where similar pressures exist. Innovations in IT are a tremendous driver for such developments, as demonstrated by the example of genome sequencing, where IT innovation has driven down the costs from US$48,000 to $1,000 within the last five years (http://en.wikipedia.org/wiki/Full_genome_sequencing). We expect important developments in the area of the governance of cloud computing scenarios in this area in the near future, in order to create a meaningful bridge between complex and restrictive information security and data privacy regulations, on the one side, and a high pace of IT innovation, on the other.

References

1. V. Stantchev et al., “Optimizing Clinical Processes with Position-Sensing,” *IT Professional*, vol. 10, no. 2, 2008, pp. 31–37.
2. V. Stantchev, *Enhancing Health Care Services with Mixed Reality Systems*, Springer, 2009.
3. V. Stantchev, “Intelligent Systems for Optimized Operating Rooms,” *New Directions in Intelligent Interactive Multimedia Systems and Services—2*, vol. 226, E. Damiani et al., eds., Springer, 2009, pp. 443–453.
4. M. Armbrust et al., “A View of Cloud Computing,” *Comm. ACM*, vol. 53, no. 4, 2010, pp. 50–58.
5. F.J. García-Peñalvo et al., “Informal Learning Recognition through a Cloud Ecosystem,” *Future Generation Computer Systems*, vol. 32, 2014, pp. 282–294.
6. M. Conde et al., “Knowledge Co-Creation Process Based on Informal Learning Competences Tagging and Recognition,” *Int’l J. Human Capital and Information Technology Professionals*, vol. 4, no. 4, 2013.
7. V. Stantchev and M. Malek, “Addressing Web Service Performance by Replication at the Operating System Level,” *Proc. 3rd Int’l Conf. Internet and Web Applications and Services*, 2008, pp. 696–701.
8. F.J. García-Peñalvo, M.A. Forment, and M.D. Lytras, “Some Reflections about Service Oriented Architectures, Cloud Computing Applications, Services, and Interoperability,” *J. Universal Computer Science*, vol. 18, no. 11, 2012, pp. 1405–1409.
9. K. Petruch, V. Stantchev, and G. Tamm, “A Survey on IT-Governance Aspects of Cloud Computing,” *Int’l J. Web and Grid Services*, vol. 7, no. 3, 2011, pp. 268–303.
10. C. O. Rolim et al., “A Cloud Computing Solution for Patient’s Data Collection in Health Care Institutions,” *Proc. 2nd Int’l Conf. eHealth, Telemedicine, and Social Medicine*, 2010, pp. 95–99.
11. R. Zhang and L. Liu, “Security Models and Requirements for Healthcare Application Clouds,” *Proc. 3rd IEEE Int’l Conf. Cloud Computing*, 2010, pp. 268–275.

12. G. Hornung and C. Schnabel, “Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination,” *Computer Law and Security Rev.*, vol. 25, no. 1, 2009, pp. 84–88.
13. L. Hasse, “Umsetzung der ‘Orientierungshilfe Krankenhausinformationssysteme’ in Thüringen” [“Implementation of the Guidance ‘Hospital Information Systems’ in Thuringia”], *Datenschutz Datensicherheit-DuD*, vol. 36, no. 8, 2012, pp. 560–560 [in German].
14. “Directive 95/46/EC of the European Parliament and of the Council,” *Official J. European Communities*, 24 Oct. 1995; http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
15. V. Stantchev and G. Tamm, “Reducing Information Asymmetry in Cloud Marketplaces,” *Int’l J. Human Capital and Information Technology Professionals*, vol. 3, no. 4, 2012, pp. 1–10.
16. V. Stantchev and G. Tamm, “Addressing Non-Functional Properties of Services in IT Service Management,” *Non-Functional Properties in Service Oriented Architecture: Requirements, Models and Methods*, IGI Global, 2011, pp. 324–334.
17. V. Stantchev and L. Stantcheva, “Extending Traditional IT-Governance Knowledge Towards SOA and Cloud Governance,” *Int’l J. Knowledge Society Research*, vol. 3, no. 2, 2012, pp. 30–43.
18. V. Stantchev and M. Malek, “Addressing Dependability throughout the SOA Life Cycle,” *IEEE Trans. Services Computing*, vol. 4, no. 2, 2011, pp. 85–95.
19. R. Colomo-Palacios et al., “Human and Intellectual Capital Management in the Cloud: Software Vendor Perspective,” *J. Universal Computer Science*, vol. 18, no. 11, 2012, pp. 1544–1557.
20. S. Liu, “New Perspectives for IT,” *IT Professional*, vol. 14, no. 1, 2012, pp. 2–4.
21. N. Kshetri, “IT in the Chinese Healthcare Industry,” *IT Professional*, vol. 15, no. 1, 2013, pp. 12–15.
22. N. Kshetri and S. Murugesan, “Cloud Computing and EU Data Privacy Regulations,” *Computer*, vol. 46, no. 3, 2012, pp. 86–89.
23. J. JPC Rodrigues et al., “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems,” *J. Medical Internet Resources*, vol. 15, no. 8, 2013.
24. E.J. Schweitzer, “Reconciliation of the Cloud Computing Model with US Federal Electronic Health Record Regulations,” *J. Am. Medical Informatics Assoc.*, vol. 19, no. 2, 2012, pp. 161–165.
25. J.J.M. Seddon and W.L. Currie, “Cloud Computing and Trans-Border Health Data: Unpacking U.S. and EU Healthcare Regulation and Compliance,” *Health Policy and Technology*, vol. 2, no. 4, 2013, pp. 229-241.

Srdan Dzombeta *is a member of the executive board of Persicon. His research interests lie in the field of internal control systems and cloud systems. Dzombeta has a degree in business administration and a master of laws. Dzombeta studied at the Technical University of Berlin, the University of California at Los Angeles, and the University of Saarland. Contact him at srdan.dzombeta@persicon.com.*

Vladimir Stantchev *is the executive director of the Institute of Information Systems at SRH Hochschule Berlin, Germany, where he is also a research professor. His major research interests are in the areas of IT governance, cloud computing architectures, IT strategy, as well as methods for service and software engineering. Stantchev is a member of the ACM, IEEE (Computer Society, Communication Society, and Standards Association), and the German Informatics Society GI e.V. Contact him at stantchev@computer.org.*

Ricardo Colomo-Palacios *is full professor in the Computer Science Department of the Østfold University College, Norway. His research interests include applied research in applied information systems including aspects like cloud governance and big data environments. He received his PhD in computer science from the Universidad Politécnica of Madrid. Contact him at ricardo.colomo-palacios@hiof.no.*

Knud Brandis *is a member of the executive board of Persicon. His research interests are in the areas of information security and risk management. Brandis earned his Master of Business Administration in financial management at the University of Wales, UK. He is also a visiting lecturer at the University of Applied Sciences Brandenburg for the master’s program “Information Security Management,” a lecturer*

in the IT service management according to ITIL topic at the Baden-Wuerttemberg University, and a lecturer in the consulting topic at the Academy of Economics and Law. Contact him at knud.brandis@persicon.com.

***Knut Haufe** is a manager at Persicon. His research is focused on preparation of certification audits according to ISO 27001- or ISO 27001-based BSI IT baseline protection, a topic in which he also advises leading organizations in the fields of public administration (especially EU paying agents), technology, and utilities. Haufe has a master's degree in commercial law. Contact him at knut.haufe@persicon.com.*