IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY | an informa business
Unlimited Validation Knowledge Awaits...
Published on *IVT Network* (http://www.ivtnetwork.com)

Assuring Data Integrity and Data Privacy Compliance when using Software-as-a-Service (SaaS) in the Life Science Sector

By **Eliane Veiga**  , **Nuala Calnan**

Jan 18, 2019 10:13 am EST

From the Editor-in-Chief:

This paper was part of Dublin Institute of Technology Regulatory Science Team requirements for granting the MSc. degree to Eliane Veiga. Congratulations, Eliane! Congratulations also to Dr. Nuala Calnan and Dr. Anne Greene of DIT!

Abstract

Data integrity (DI) and data privacy (DP) challenges have received increased regulatory attention in recent years. When considering GxP applications, a robust approach to risk-based computerized system lifecycle management requires well-defined processes, use of a qualified infrastructure, validated design and deployment of software, qualified personnel, rigorous change management and version control. With the increased adoption of cloud-based applications in the life science sector, cloud computing solutions such as *Software as a Service* (SaaS), offer many advantages including enhanced cost-effectiveness, ease of implementation, and flexible, highly scalable platforms. However, assuring data integrity and data privacy in the cloud requires a well-informed, proactive approach by the regulated organization in planning and maintaining control of their data once it is hosted on the cloud provider's site. This paper aims to examine the current regulatory expectations from the prospective of both data integrity and data privacy and proposes that when it comes to cloud computing, the most powerful tool organizations possess to assure data quality and security lies with their third party supplier contracts.

1. Introduction

Recent developments in technology and communications have led to a whole range of new cloud computing IT models, which are transforming the way by which global business is transacted. Curiously, SaaS as a business model has been available since the 1960s when it was referred to as a 'time sharing system' (Bratten, 2012). However, more recently it has become known as a method of software delivery where a third-party provider hosts an application which enable consumers to work and access their data using a variety of different technologies connected to the internet, from a variety of different locations (Singleton, 2018). SaaS solutions eliminate the need for companies to manage their applications across their own device network and also reduces the burden of managing their growing data volumes in their own data centers. This offers companies an opportunity to eliminate the high-cost of hardware acquisition, maintenance, software licensing, installation and in-house technical support (Rouse, 2018).

With the transition from traditional paper-based, manual records towards electronic systems, the GxP sector has been facing new and emerging data compliance challenges and has seen a rising number of regulatory actions taken by the international medicines regulators, primarily focused on data integrity. More recently, regulators and governments have become progressively vigilant regarding data security and personal data protection. With commercial transactions increasingly taking place across the internet the risk of hacking is now ever present.

In Europe, protection of data privacy is now regulated under the General Data Protection Regulation (GDPR), which came into force on the 25th May 2018.

The GDPR brings a few significant changes from the previous EU Data Protection Directive including;

- a redefinition of personal data and individual rights,
- specific distinctions between the roles and responsibilities of data controllers vs. data processors,
- new requirements on information governance and security,
- a new data privacy impact assessment (DPIA),
- clear requirements about data breach notifications,
- potential steep penalties for non-compliance.

The impacts of the new DI and DP regulations will affect many different industry sectors in many different ways. For those involved in the management and control of clinical research trials the new regulations potentially present a “perfect storm” for the development and approval of new medicinal products. The prevalence of new cloud-based technologies; coupled with technology advances in connected health; the proliferation and reliance on data analytics capabilities set within the context of globalization, present both opportunities and potential threats to the security and integrity of the data that must be carefully considered.

2. Research Background and Methodology

This research was undertaken by a Masters degree candidate within the Pharmaceutical Regulatory Science Team (PRST), a research team based at the Dublin Institute of Technology (DIT) in Ireland. The research sought to answer the following question:

What is the impact of the recent data integrity guidance and the new general data protection regulations on the delivery of cloud-based computing services for the regulated life science sector?

A detailed literature review of both the Data Integrity (DI) guidance and the new *General Data Protection Regulations* (GDPR) was conducted and a clinical trials user case-study was examined in detail to understand the qualified architecture and controls necessary to deliver a compliant *Software-as-a-Servic*e (SaaS) solution within the GxP environment.

The aim of this research is to establish the specific roles and responsibilities for a regulated company and their chosen third parties involved in a real-world clinical trial environment using a SaaS platform. Further, the research seeks to highlight the impact of the GDPR and Data integrity guidance on the use of cloud-computing solutions, providing key aspects to consider when implementing such platforms.

3. Data Integrity – The Fundamentals

The UK Medicines & Healthcare products Regulatory Agency (MHRA) defines data integrity as ‘*the degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data lifecycle’* (MHRA, 2018). Assuring data integrity requires effective quality and risk management systems which enable consistent adherence to sound scientific principles and good documentation practices. The international regulators have defined an acronym (ALCOA) as the five elements necessary to assure data integrity throughout the data life-cycle. Even though ALCOA has been widely discussed in many publications, evidence from the US FDA warning letters and EU Statements of Non Compliance (SNCs) indicate that there still are many who do not understand the fundamentals of ALCOA. The following describes the basics of the five elements of DI (MHRA, 2016).

- (A) Attributable: Data should be recorded by the subject who performs the task. It is important to document this action to enable full transparency and traceability.
- (L) Legible: Means that all records must be readable and retained on durable media for the duration of the records retention period.
- (C) Contemporaneous: All activities must be recorded at the same time the action takes place.
- (O) Original: The original record is the first initial capture of the data. Regardless of whether the data is recorded on paper or electronically, information should be available for review in the same state as originally collected.
- (A) Accurate: Data must be accurately recorded. Therefore, educating staff about the importance of following approved procedures prior to recording their actions is essential to achieve data integrity.

More recent publications, including the WHO Guidance on Good Data And Record Management Practices, have expanded

these principles to describe ALCOA+ expectations, which puts additional emphasis on ensuring that data and records are *'complete, consistent, enduring and available'* (WHO, 2016).

3.1 Understanding the Data Lifecycle

The WHO guidance also bring the whole matter of data integrity back to first principles by reminding us that in order to ensure that an organization can undertake *'evidence-based and reliable decision-making, data governance should address data ownership, accountability and risk management for data process(es) right across the data lifecycle'* (WHO, 2016). A common pitfall for data integrity programs can arise when organizations focus their DI assessment and remediation efforts at an individual computerized system level and do not look at the issue from the perspective of how their critical records transition multiple platforms as they move around the data lifecycle.

The data lifecycle is defined by the MHRA as: *'All phases in the life of the data from generation and recording through processing (including analysis, transformation or migration), use, data retention, archive/retrieval and destruction'* (MHRA, 2018). ?Good data governance must be applied across the whole data lifecycle in order to provide assurance of data integrity.

Understanding the data quality implications across the data lifecycle becomes even more critical when cloud-based services are in use. Managing the risks at each of the data lifecycle boundaries requires carefully definition of roles and responsibilities for all stakeholders. Figure 1 illustrated the key phases of the data lifecycle.

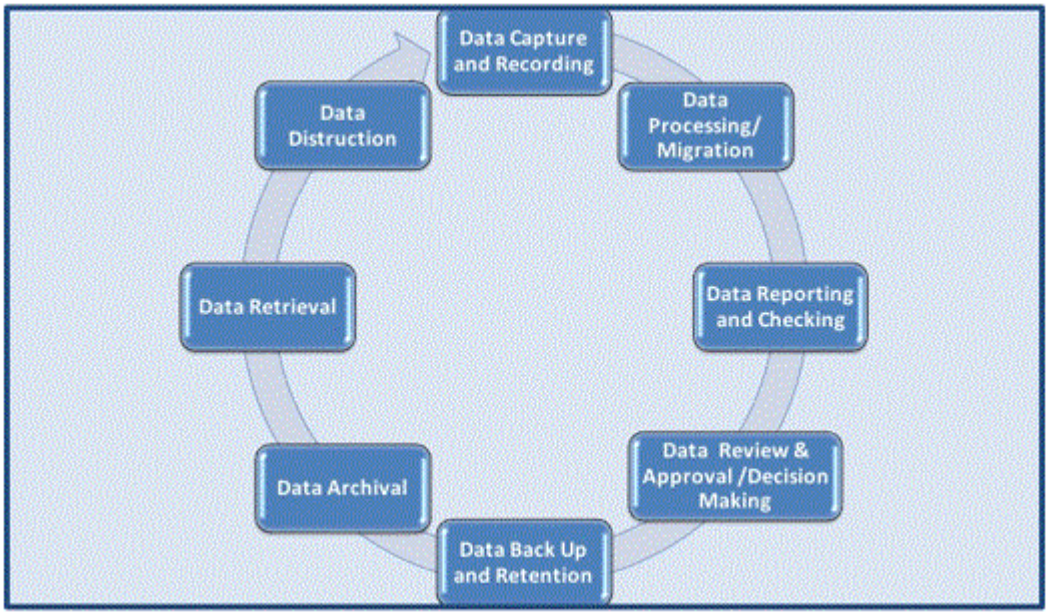

Figure 1: Phases of the Data Lifecycle

The MHRA guidance directly addresses data lifecycle considerations in cases where 'cloud' or 'virtual' services are used. Noting that attention should be paid to *'understanding the service provided, ownership, retrieval, retention and security of data',* (MHRA, 2018). Furthermore, caution should be taken of the physical location where the actual data is held, including the impact of any laws applicable to that geographic location.

4. Data Privacy – The Fundamentals

The General Data Protection Regulation (GDPR) came into force in the EU on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive. The GDPR emphasises transparency, security and accountability by both *data controllers* and *data processors,* while at the same time standardising and strengthening the right of European citizens to data privacy.

A detailed report published by law firm White & Case, on the impacts and implications arising from the EU GDPR, states that it is difficult to overstate the importance of the GDPR, noting that:

- First, it is very wide-ranging, and will impact almost every organization that is based in the EU, as well as every organization that does business in the EU, even if based abroad.

- Second, the GDPR is extremely serious. For too long, EU legislators have felt that organizations do not take their data protection responsibilities seriously enough, and so the GDPR dramatically increases the **maximum penalties for non-compliance to the greater of €20 million, or four percent of worldwide turnover**—numbers that are specifically designed to attract C-Suite attention.
- Third, the GDPR raises the bar for compliance significantly. It requires greater openness and transparency; it imposes tighter limits on the use of personal data; and it gives individuals more powerful rights to enforce against organizations. Satisfying these requirements will prove to be a serious challenge for many organizations. (White & Case, 2017)

In a GxP environment, the resonance between the DI regulatory guidance and the requirements set out under GDPR is perhaps best understood when reviewing the definition for a “data breach". The GDPR defines it as ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.’ The responsibility lies firmly with the data controller to ensure that it has appropriate processes and templates in place for identifying, reviewing and (to the extent required) promptly reporting data breaches. (White & Case, 2017).

4.1 What is Personal Data and Sensitive Personal Data?

The GDPR defines personal data as *‘any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person’*.

Sensitive Personal Data are defined as *‘personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.’*

From a life science sector perspective the new EU data protection regulation has a significant impact on the management of sensitive personal / health data, such as that typically associated with clinical trials for medicinal products.

4.2 What is the impact of the new data protection regulations for life science companies?

Specifically, from a healthcare and cloud-based solutions prospective, the GDPR brings some significant changes from the previous data protection directive, including (Intersoft Consulting, 2018):

- Definition of “Sensitive personal data”

Under GDPR different categories of personal data have been defined. Sensitive data is one of the categories of personal data established by GDPR which comprises of “biometric data”, “genetic data” and “data concerning health or sex life and sexual orientation”. Processing of sensitive data has become much stricter under the new regulation.

- The obligation on both data controller and processors

Controllers and processors have been allocated shared, stricter responsibilities under the GDPR. The data controller may be described as *‘the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.’* (Data Protection Commissioner, 2018).

Under GDPR, the data controller must implement organizational and technical measures to demonstrate compliance of the processing activities undertaken on their behalf. Furthermore, data controllers have the responsibility for selection and oversight of their service providers (data processors). The GDPR defines such a data processor as *‘a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller’.*

The compliance burden is now shared between processors and controllers. One of the significant requirements that GDPR imposes for processors is that if they intend to hire another processor to assist with data management, e.g. a cloud computing supplier, the data controller must approve this appointment prior to commencement. This requirement is intended to protect personal data from transfer to a third party, even to another country, without the controller’s prior authorization.

- Appointment of a Data Protection Officer (DPO)

A data protection officer (DPO) is responsible to conduct a company-wide risk/impact assessment. Where the core activities of the controller and processor involves processing large volumes of sensitive data (e.g. health related data) both controllers and

processors should appoint an individual trained on data protection to carry out and monitor internal measures to ensure the organization is compliant with the regulation. Under GDPR, DPOs must be facilitated to execute their tasks independently.

- Data Protection Impact Assessment (DPIA)

Controllers must now apply a data protection impact assessment (DPIA), especially when new technologies and /or suppliers are being used. The DPIA is a tool that should help controllers and processors to identify data protection gaps prior to commencement of data processing and should provide measures and safeguards to protect the personal data. Additionally, the controller should look for the DPO's advice regarding when the DPIA should be carried out.

5. Cloud Computing -The Fundamentals

Cloud computing provides on-demand access to larger computing power, storage, web-based applications and various IT resources, via the internet, with 'pay-as-you-go' pricing options. With cloud-based computing, users can access their data using the web from anywhere in the world. Cloud-based services reduce the overhead burden of maintenance and the heavy lifting of procuring and housing hardware infrastructure such as servers etc. It offers scalable solutions for both services and computing power and the cloud-based application(s) can be upgraded anytime based on the requirements of the customer. (Amazon, 2018)

5.1 Cloud Computing: The main options and associated accountability

The various cloud computing service configuration options and their associated accountability are outlined in Figure 2, as follows:

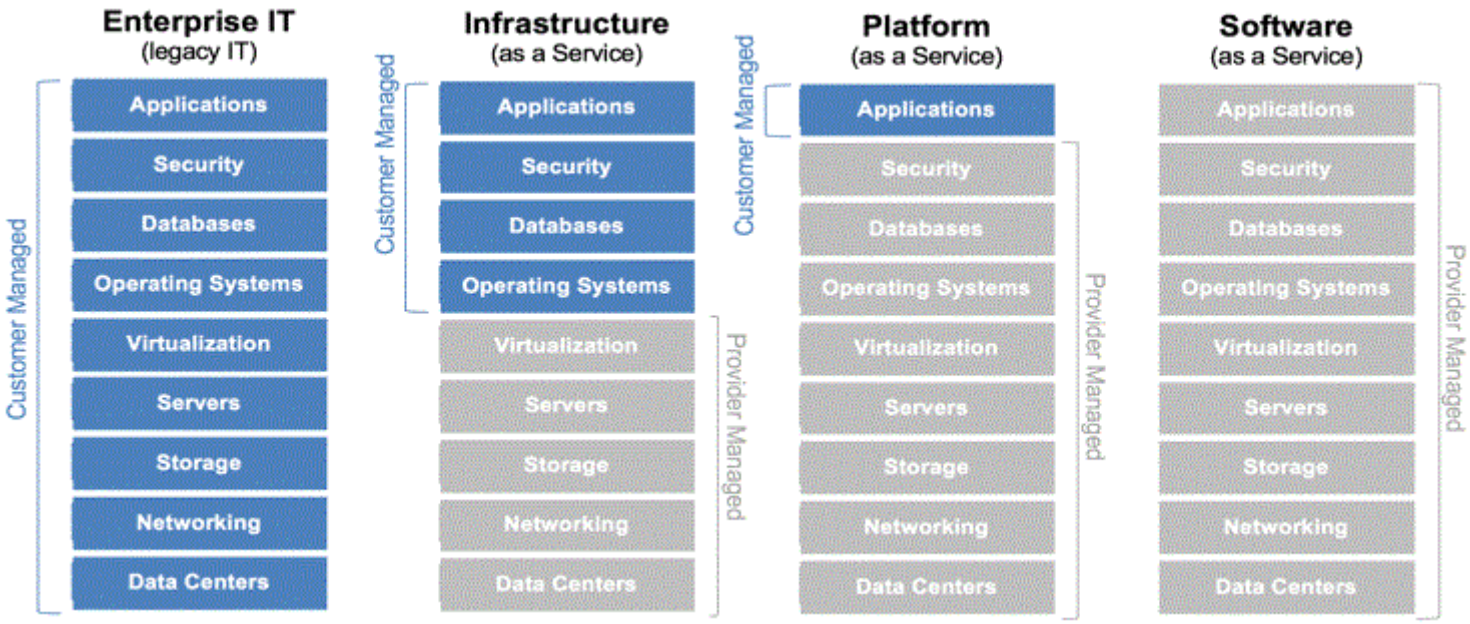

Figure 2: High-level view of the roles for IaaS, PaaS and SaaS.

Enterprise IT: All activities are managed by the customer at its own site. It is considered more expensive as each component requires personnel with different knowledge and expertise and overhead hardware maintenance costs are borne by the customer. With changing market and customer needs, system upgrades are costly and time consuming.

Infrastructure-as-a-Service (IaaS): In this model, the customers are expected to secure their own operating systems, user applications and data/content. The IaaS provider delivers the infrastructure components such as servers, storage, and networking. Also, the IaaS provider is responsible for management services required to manage the applications and platform. Amazon Web Services is one of the bigger players in IaaS based products and services. (IBM, 2018)

Platform-as-a-Service (PaaS): PaaS is a cloud computing service that provides the whole range of IT services and resources that allow customers to build and host their own applications, which are managed and maintained by the customer. All other

needs are taken care by PaaS provider. (IBM, 2018)

Software-as-a-Service (SaaS): SaaS is a cloud-based delivery model in which the provider is responsible for all the IT resources and web application development and management. It is a custom-based IT solution which is accessed by the users through the internet from a diverse range of available devices. This model eliminates the need for companies to manage their applications across their own device network and the burden of managing their data in their own data centres. SaaS offers companies an opportunity to eliminate the high-cost of hardware acquisition, maintenance, software licensing, installation and technical support. (Oracle, 2018)

5.2 Considerations for Delivery Options for Software-as-a-Service (SaaS) Model

A further important aspect to consider is whether the SaaS environment selected is a single tenant or multi-tenant configuration.

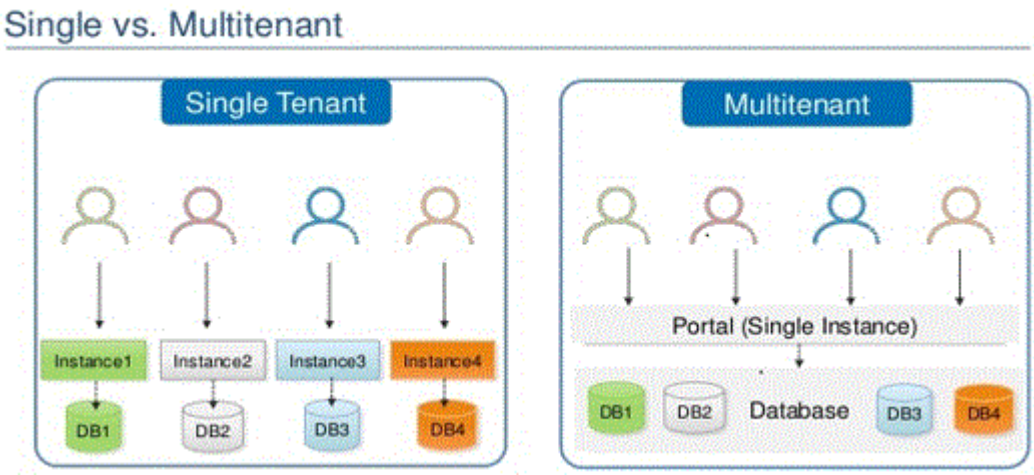

Figure 3: Considerations for Single Tenant or Multi-Tenant SaaS Model

SaaS Single- Tenant architecture: Single-Tenant applications have their own instance of the software application and supporting infrastructure available to them. Each customer, therefore, has their own database and access to data is limited to only each individual companies' users (Mundra, 2015). As a result, single- tenant users will never be affected by the actions of another user using the cloud services (Massicotte, 2017).

SaaS Multi-tenancy architecture: Multi-tenancy architecture SaaS applications are developed to provide support to many synchronized users simultaneously (Amazon, 2018). The concept of 'Multi-Tenants' means that the same software can be used by many users, across diverse enterprises, at the same time. This deployment model not only allows customers to share the software application but also to share access to a shared database. The Multi-tenant application architecture permits system developers to leverage a common infrastructure allowing the expansion of the services as required. As a result, it becomes more economically viable and easier to maintain this architecture as the enterprise grows.

From a data privacy perspective, the decision to deploy and use SaaS applications as either a single tenant or a multi-tenant is key to the initial set up of the contract.

6. User Case Study – GxP Clinical Trial Management SaaS Application

This user case study examines the impact of new GDPR and recent data integrity (DI) guidance on a GxP Clinical Trial environment which utilizes cloud-based applications. It demonstrates the relationship between the regulated company and third parties in a typical clinical trial scenario. The focus of this study is to identify the relevant factors necessary to assure data integrity and data privacy using an electronic data collection (EDC) system as a SaaS-based application in a clinical trials environment. A representative Clinical Trials Architecture (see Figure. 4) has been developed to help understand the relationships when using SaaS as an open system application.

In this case study, the pharma company (Trial Sponsor) outsources its research and development (R&D) to a clinical research organization (CRO) which operates on multiple sites. However, the CRO in turn outsources the data collection duties to a hospital where the trial subject/patient data is collected. The CRO also contracts a third-party IT Company (SaaS Provider) which is responsible for the data management processes associated with the clinical trial. The EU clinical trial regulation

(European Commission, 2014) is clear that the Trial Sponsor retains overall responsibility for the compliance, integrity and data security of all data associated with the trial and with any submissions made in support of a new drug application (NDA) or abbreviated new drug application (ANDA).

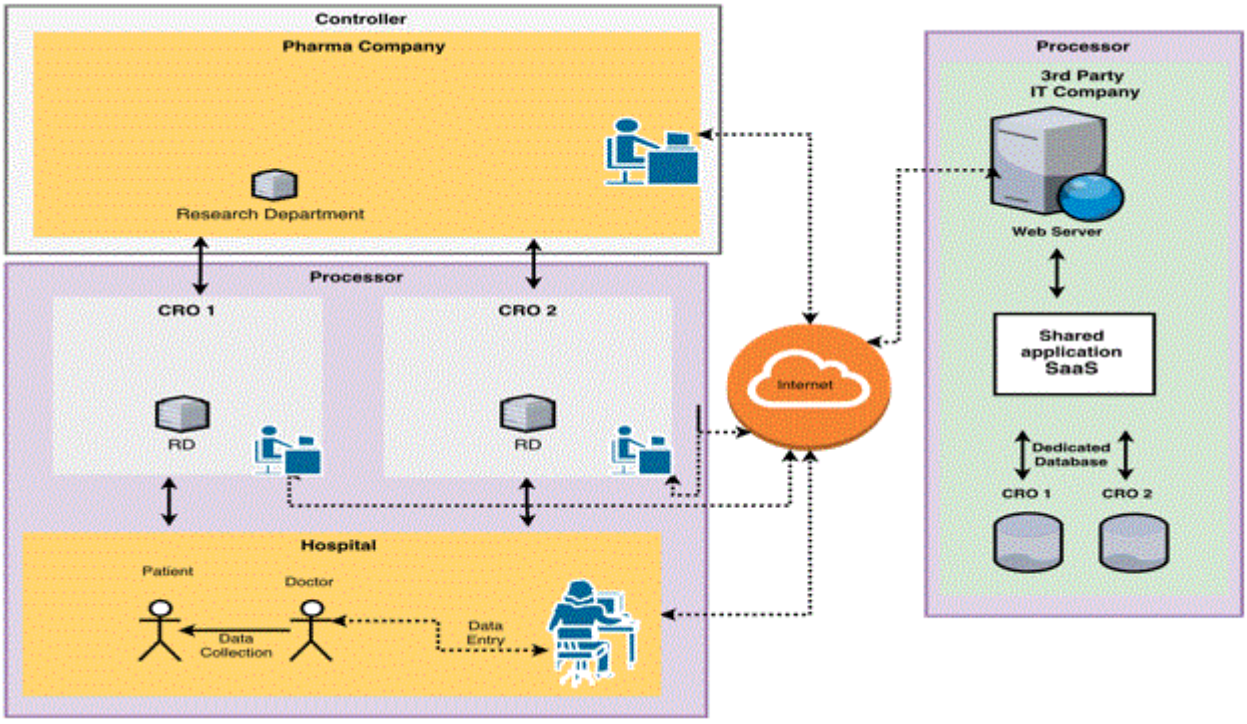

Figure 4: Clinical Trials Architecture using SaaS

6.1 The Clinical Research Organization (CRO) and Data Integrity

At the CRO site, subjects are interviewed, personal details and health history are collected in a manual, paper-based case report form (CRF) and this record is then transcribed into a SaaS-based electronic data collection (EDC) system, where the data is reviewed and made available to the regulated company. Figure 5 shows a CRO carrying out a clinical trial study on behalf of the sponsor company.

According to PIC/s *Good Practices For Computerized Systems in Regulated "GxP" Environments, 'Data should be reviewed and, where appropriate, evaluated statistically after completion of the process to determine whether outcomes are consistent and compliant with established standards. The evaluation should take into consideration all data, including atypical, suspect or rejected data, together with the reported data. This includes a review of the original paper and electronic records'* (PIC/S, 2007).

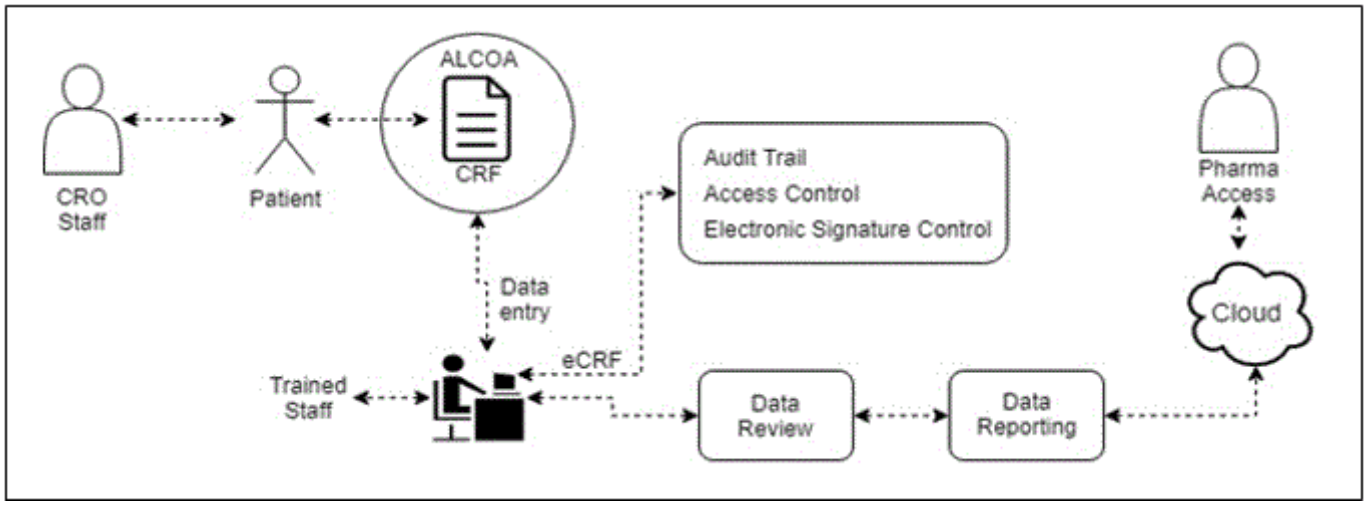

Figure 5: A schematic diagram with CRF for personal data collection at the CRO

6.2 Dataflow at the Hospital

The data flow in a clinical data collection scenario at the hospital is shown in Figure 6. The clinical trial investigator (e.g. a doctor) is considered to assume the role of a data processor as per the GDPR, (Intersoft Consulting , 2018). In the data flow schematic (see Figure. 6), the trial sponsor (regulated company) has oversight responsibility to assure data quality and compliance by the clinical trial investigator to Good Clinical Practice (GCP). At the hospital, each patient /trial subject's data, such as blood pressure, electrocardiograms are recorded on the CRF (i.e. the paper-based source document) contemporaneously as the tests/ observations are conducted and then subsequently transcribed into a validated EDC system by an authorized staff member. Note, the source document must also be retained by the investigator (doctor) in the format that the document was initially generated (MHRA, 2016).

When utilizing an EDC for clinical data, it is important that the system meets the sponsor's requirements for completeness, accuracy, reliability, and consistent intended performance, therefore, the validation of the computerized EDC system is vital. Logical controls, such as an audit trail, and other security measures such as encryption and pseudonymization must be applied to the system to assure data privacy and integrity of the electronic data. (Pseudonymization enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms)

As per data protection requirements, data is reviewed for accuracy by a trained staff member and made available for the sponsor (controller-regulated company) for review and reporting. Full traceability and transparency of all actions taken related to the data, meta-data and associated audit trail must be retained.

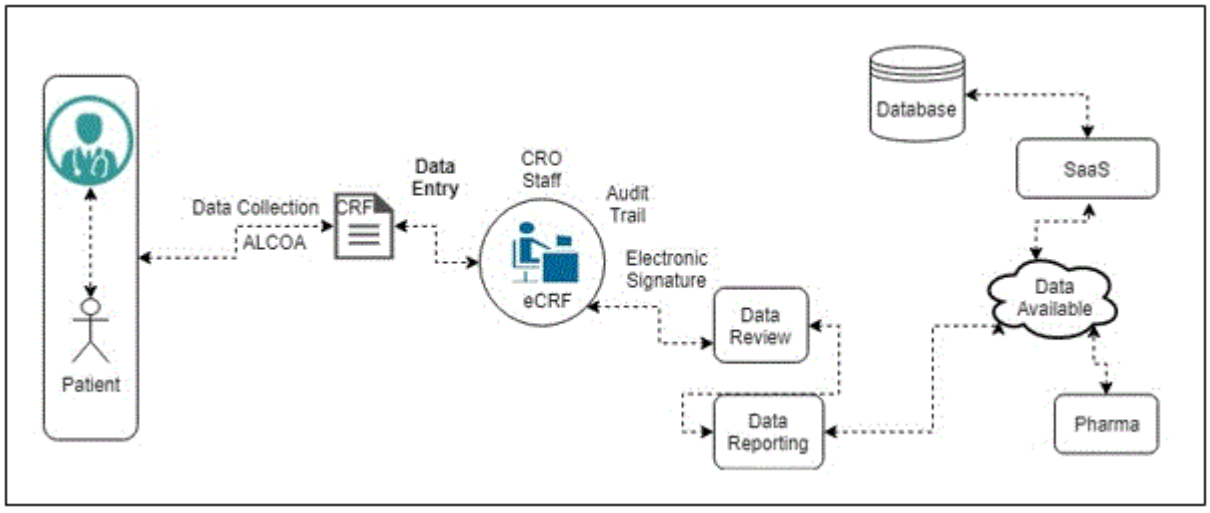

Figure 6: A dataflow schematic for collection of clinical data at the hospital

6.3 Compliant SaaS Provider Responsibilities

The SaaS provider role in this study is to provide a validated, shared EDC application with a dedicated database hosted on their own qualified infrastructure. In this scenario, the clinical data is being managed by a SaaS provider through a validated EDC application supported by a fully qualified infrastructure, capable of demonstrating compliance with all DI, DP and GCP regulations.

The validation of the SaaS EDC system is vital to assure that appropriate controls are in place to monitor and secure each user's access to the network and the EDC application. Since the EDC both stores electronic records and uses some format of electronic signatures, the SaaS provider should be aware of the applicable underlying regulations such as FDA 21 CFR Part 11 and / or EU GMPs Annex 11 in order to implement the necessary validation procedures and policies. Qualified IT infrastructure is a fundamental requirement stated in EU Annex 11, however, many cloud-based solution providers unfamiliar with the life science sector are struggling to implement these qualification requirements.

Platform, personnel, and processes are considered the three major elements of the IT infrastructure that can have an impact on data integrity and data privacy (See Figure 7). The quality management system in place should ensure that the necessary processes are implemented to control the IT infrastructure platform(s), and that capable staff are able to accomplish given activities (ISPE, 2005). Over recent years, global regulatory bodies have been increasingly concerned regarding IT networks

and other aspects of infrastructure management, triggering the issuance of numerous warning letters (Unger, 2018). Even though the guidance is clear that the accountability for the overall system validation remains with the regulated company (trial sponsor), the qualification and validation of the SaaS environment should be executed by the SaaS provider under the approval of the sponsor. It is not feasible for the regulated sponsor company to attempt to perform the qualification and validation activities for an environment that they do not control.

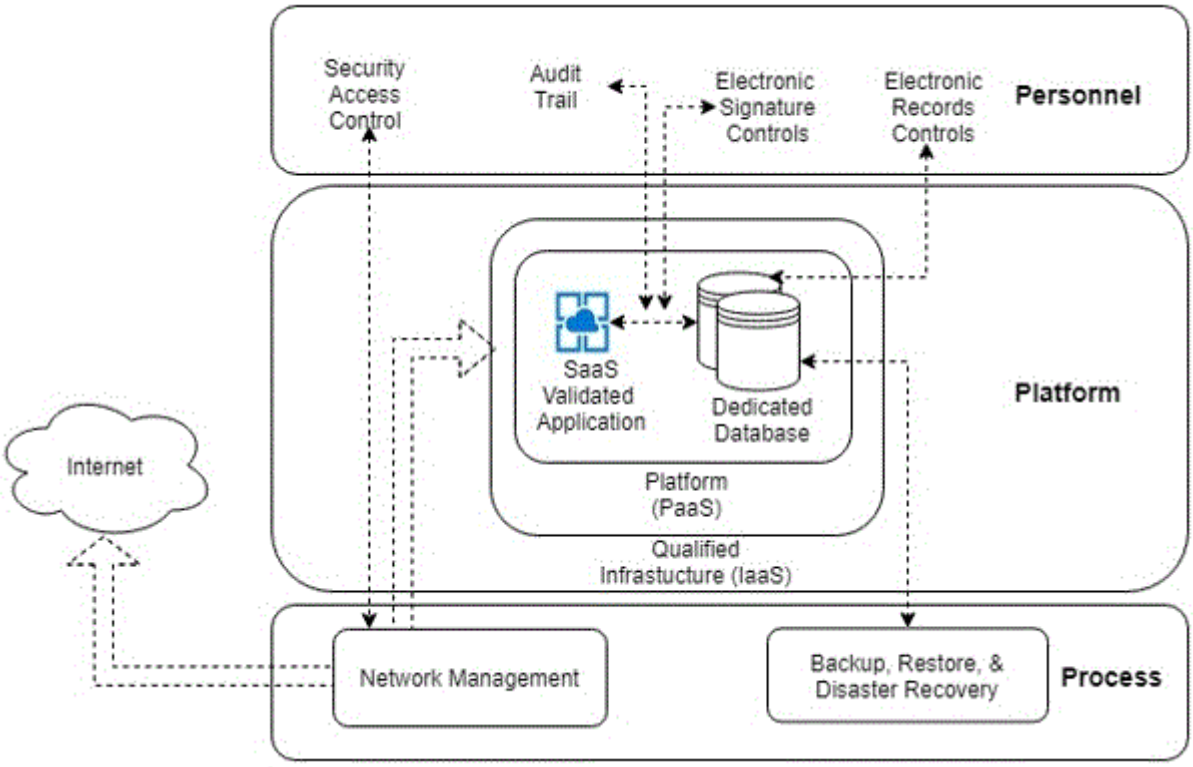

Figure 7: Schematic for a Typical GxP Cloud Based Infrastructure

7. Recommendations

Specifically with respect to a GxP clinical trials environment, the research finds that the following critical aspects should be considered by the data controller (trial sponsor) and data processors (CRO, Hospital, SaaS Provider) to assure both the data integrity (DI) and data privacy (DP) regulatory requirements.

7.1 Supplier Assessment

Data Integrity Considerations: When auditing a SaaS provider it is crucial to understand their experience regarding GxP data lifecycle processes as required by the international DI regulatory guidance. Many non-GxP software suppliers use different software development lifecycle approaches, for example the ‘agile’ model and are not familiar with the GxP DI requirements. The SaaS provider should have, at a minimum, a documented Quality Management System (QMS) describing how they operate and manage their business. The SaaS provider’s QMS should provide an established quality approach comprising a collection of controls and procedures that they utilize to carry out their activities (ISPE, 2017). The SaaS provider should be able to demonstrate that they are capable of delivering a validated GxP system and the regulated company must have a robust Supplier Level Agreement (SLA) in place to control the delivery, operation and on-going maintenance of the validated SaaS environment.

Data Protection Considerations: Under the new European General Data Protection Regulation, both the data controller (the regulated company) and the processor (SaaS provider), are accountable for the protection of the data. Prior to commencing data processing activities, cloud service providers (processors) must demonstrate that the necessary organizational and technical measures are in place to demonstrate that their data processing activities are fully compliant with the GDPR requirements. A Data Protection Impact Assessments (DPIA) is a tool designed to enable organizations to work out the risks that are inherent in proposed data processing activities before those activities commence. This, in turn, enables organizations to address and mitigate those risks before any processing begin, (Data Protection Commissioner, 2018). This impact assessment should be carried out by the data controller in conjunction with all/any data processors involved.

Cross-border data transfers must be taken into consideration in any supplier assessment process. If the data processor is processing data across multiple EU member states, one state must be nominated as the “lead” and the data protection authority in that state shall act as the lead authority. Controllers and processors that are located outside the European Economic Area (EEA) that are not subject to the GDPR, may adhere to a code of conduct in order to create a framework for providing adequate protection to personal data in third countries. The GDPR specifically allows adherence of non-EEA controllers and processors to an approved code of conduct to provide the basis for cross-border data transfers, (White & Case, 2017).

7.2 Supplier Contracts and Service Level Agreements (SLA)

Data Integrity Considerations: When using SaaS, regulated companies have limited control over their own data from the moment their data is collected. However, the regulated company still has full responsibility for the integrity of that data. Therefore, the supplier contract and Service Level Agreement (SLA) is the primary way that life science companies can assure that their data is managed as per the regulatory requirements. The contract and SLA should be written to clarify and ensure that the required controls are implemented. Additionally, the level and frequency of reporting should be established, and the need for supplier support during regulatory inspections agreed (ISPE, 2017). The contract should establish the responsibilities of the service provider regarding continued availability and readability of the data over the record retention period. Disaster recovery arrangements should be established to ensure the restoration of the system as per its validated state, if required. The MHRA 2018 GxP DI guidance recommends ‘*business continuity arrangements should be included in the contract, and tested. The need for an audit of the service provider should be based upon risk.’,* (MHRA, 2018).

Data Protection Considerations:

Many processors will need to understand their obligations under the GDPR and adapt and amend their services, contracts and background processes accordingly (Webber, 2016).

The GDPR is prescriptive about the contents of the contract between a data controller and a data processor. It should specify essential requirements including:

- The subject-matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subjects;
- The obligations and rights of the controller.

The contract must also stipulate that the processor shall:

- Process the personal data only on documented instructions from the controller (including with regard to transfers of personal data to a third country or an international organization);
- Ensure confidentiality and make appropriate measures to ensure security. (Webber, 2016).

The processor should be aware that in the case of engaging another processor for managing specific processing activities on behalf of the controller, the controller must be notified and have the right to agree or not with the introduction of the new data processor. Furthermore, the new processor must be able to provide the same level of compliance. This means transitioning to a regime of sub-contracting may only commence with the controller`s authorization (Intersoft Consulting , 2018).

7.3 Security Access Control

Data Integrity Considerations: Logical and physical controls are two key security measures to limit the access to a computerized system.

Examples of both logical and physical controls include:

- Logical: An audit trail is a logical control required for GxP Systems that helps to protect the the integrity of electronic records and is one of the main electronic data control requirements established in FDA 21 CFR part 11. This mechanism should provide a transparent chronology of the “who, what, when, and why” of an electronic record, recording the date and time of operator entries and actions that create, modify, or delete electronic records (FDA, 2016).

- Physical: The physical control reduces the possibility of unauthorized access, intended or accidental damage by personnel or loss of data and should be defined prior to the system being ready for operation (PIC/S, 2007).

The technical and organizational mechanisms by which logical and physical controls are implemented and deployed within a SaaS environment – right across the data lifecycle - should be clearly understood to assure data integrity. These features should be purposefully designed into the environment at the outset and means for routine/ periodic review provided for.

Data Protection Considerations:

Mention is given throughout the GDPR regulation that controllers and processors shall apply suitable technical and organizational methods to assure a level of security. Pseudonymisation and encryption are some of the technical measures suggested in the EU GDPR to prevent a data breach and maintain data in a secured state (Redstor, 2017).

7.4 Data Backup, Restore & Business Continuity

Data Integrity Considerations: Data backup and restore activities are clearly designated as part of the data lifecycle. Business continuity planning (BCP) is implemented as part of the initial application system planning as it plays a very important role when any potential threat is faced by an organization. BCP is a process of creating a regular backup of live systems that are recoverable when the system is down due to potential threats such as weather related events, earthquakes or power outages. BCP is an important part of risk management planning (Elliott, D., Swartz, E., & Herbane, B., 1999). Business continuity provisions should be incorporated in the contract and tested properly for all the possible treat scenarios before the system goes live. (MHRA, 2018)

Data Protection Considerations: The GDPR does not impose specific requirements regarding disaster recovery and business continuity. It does bring strict conditions for any data transfers either to another country or another organization and at the end of contracts. More recently, organizations must carefully consider and manage the data protection threats and impacts posed by a potential hacking attempt. These scenarios should be addressed in the supplier contract or SLA.

8. Conclusion

The research has shown that to build an effective data integrity and data privacy plan within a SaaS environment, the terms of the contract and SLA are of paramount importance to establish accountability and to promote compliance with the requirements of the various regulatory bodies. Furthermore, SaaS providers must operate an effective QMS which enables them to meet their contractual requirements. The regulated company then has the responsibility to ensure adequate oversight of the contract, periodically re-assess or audit the supplier (based on risk) and demonstrate by example good data and record management practices and behaviours.

Market evidence indicates that some SaaS providers are still struggling to meet the life science standards as they seek new opportunities within the regulated sector. The regulated entities should expect their SaaS vendors to demonstrate the same levels of experience, expertise, and commitment to compliance as they have themselves.

The main point of resonance between data integrity and data privacy regulations identified in this research relates to measures deemed necessary to avoid a data breach. While, from the GxP perspective, the compliance burden still sits squarely with the regulated entities, data protection requirements share the responsibilities between the controller and the processors. With the increased adoption of cloud-based solutions across the life science sector, it is likely that the most capable partners will be those who have prepared well for the impacts of the new GDPR on their business and that of their clients.

References

Amazon. (2018). *What is Cloud Computing?* Retrieved 04 20, 2018, from https://aws.amazon.com/what-is-cloud-computing/

Data Protection Commissioner . (2018). *What is Personal Data?* Retrieved April 29, 2018, from https://www.dataprotection.ie/docs/What-is-Personal-Data-/210.htm

Data Protection Commissioner. (2018). *The GDPR and you*. Data Protection Commissioner.

Data Protection Commissioner. (2018). *What Should be Contained in a contract between a Data Controller and Data Processor*. Retrieved April 20, 2018, from https://www.dataprotection.ie/docs/710-What-should-be-contained-in-a-con...

European Commission, Clinical Trial Regulation EU No 536/2014, 27 May 2014, accessed at https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_...

Elliott, D., Swartz, E., & Herbane, B. (1999). Just waiting for the next big bang: business continuity planning in the UK finance sector. *Journal of Applied Management Studies*, 8, 43-60.

FDA. (2016). *Use of Eletronic Health Record in Clinical Investigations - Guidance for Industry*. FDA.

IBM. (2018). *IaaS, PaaS and SaaS – IBM Cloud service models*. Retrieved 04 25, 2018, from https://www.ibm.com/cloud/learn/iaas-paas-saas

ICH. (1996). *INTERNATIONAL CONFERENCE ON HARMONISATION OF TECHNICAL REQUIREMENTS FOR REGISTRATION OF PHARMACEUTICALS FOR HUMAN USE- GUIDELINE FOR GOOD CLINICAL PRACTICE.* ICH.

Intersoft Consulting. (2018). *General Data Protection Regulation*. Retrieved April 25, 2018, from https://www.intersoft-consulting.de/en/gdpr/

ISPE. (2005). *GAMP Good Practice Guide: IT Infrastructure Control and Compliance*. ISPE.

ISPE. (2008). *GAMP 5: A risk-Based Approach to Compliant GxP Computerized Systems.* ISPE.

ISPE. (2013). *The Application of Gamp®5 to the Implementation and Operation of GxP Compliant Clinical System.* ISPE.

ISPE. (2017). *Good Practice Guide: Global Information Systems Control & Compliance*. ISPE.

ISPE. (2017). *Records and Data Integrity Guide*. ISPE.

Massicotte, R. (2017). *Prophix Blog - Single-Tenant vs. Multi-Tenant for Cloud Software Explained.* Retrieved 04 20, 2018, from https://blog.prophix.com/single-tenant-vs-multi-tenant-explained/

MHRA. (2016). *MHRA GxP Data Integrity Definitions and Guidance for Industry.* MHRA.

MHRA. (2018). *"GxP" Data Integrity Guidance and Definitions*. Revision 1, MHRA.

Mundra, M. (2015). *SAP Blog - Multi-tenant Vs. Single-tenant Architecture (SaaS)*. Retrieved 04 20, 2018, from https://blogs.sap.com/2015/07/12/multi-tenant-vs-single-tenant-architect...

Oracle. (2018). *What Is a Software-as-a-Service Cloud Suite?* Retrieved 02 26, 2018, from https://www.oracle.com/cloud/applications.html

Palm, M. (2005). *Pharma Tech.com - Is your IT infrastructure Qualified?* Retrieved March 15, 2018, from http://www.pharmtech.com/your-it-infrastructure-qualified.

PIC/S. (2007). *Good Practices For Computerized Systems in Regulated "GxP" Environments - PIC/S Guidance*. PIC/S.

PIC/S. (2016). *Good Practices For Data Management And Integrity In Regulated GMP/GDP Environment*. PIC/S.

Redstor. (2017). *GDPR and Ciber-Security `Technical and Organizational Measures'.* Retrieved April 28, 2018, from https://www.redstor.com/news/gdpr-and-cyber-security-technical-and-organ...

Rouse, M. (2018). *TechTarget - Software as a Service (SaaS)*. Retrieved 04 20, 2018, from https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Ser...

Singleton, D. (2018). *What is SaaS? 10 FAQs About Software as a Service*. Retrieved 04 20, 2018, from https://www.softwareadvice.com/resources/saas-10-faqs-software-service/

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (2016). GDPR Regulations. *Official Journal of the European Union*, 1-88.

Unger, B. (2108). *An Analysis Of FDA FY2017 Drug GMP Warning Letters*, Pharmaceutical Online, accessed at https://www.pharmaceuticalonline.com/doc/an-analysis-of-fda-fy-drug-gmp-...

Webber, M. (2016). The GDPR's impact on the cloud service provider as a processor. *Privacy & Data Protection*, 16(4).

White & Case (2017). *GDPR Handbook: Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law.* Accessed at https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-e...

World Health Organization (2016). WHO Expert Committee on Specfications for Pharmaceutical Preparations (Fiftieth report), *Annex 5 - Guidance on Good Data And Record Managemnt Practices*, accessed at http://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf

---