# Ethical and Legal Implications of Data Sharing in SaaS Laboratory Management Systems

***Vicrumnaug Vuppalapaty**, Technical Architect, CodeScience Inc. USA*

DOI: 10.55662/AJMRR.2024.5306

## Abstract

Over the years, the use of Software as a Service (SaaS) in a laboratory information management system has transformed sharing and management in the latter system. Such a transformation, however, brings along complex ethical and legal challenges for which scrutiny is supposed to be considered. Implication for adopting SaaS platforms includes fundamental concern about data privacy, security, and the overall integrity of scientific research.

The paper systematically analyses ethical and legal implications associated with data sharing through SaaS platforms in the management of laboratories. This thus revolves around the understanding of how these systems can handle key aspects such as data ownership, respect for privacy, and compliance with international laws, and the resultant effects these would have on respective stakeholders across the scientific community.

We, in this approach, have reviewed a wide range of literature, including fine details of case studies and views by experts, in light of current practices and challenges within SaaS-based laboratory management. We incorporate all these methods within the research to provide an integral view of the multidimensional ethical and legal landscaping, therefore delivering an approach with both depth and context to the analysis.

It was mainly, regarding informed consent, and a very complex legal challenge emphasized in this study for compliance with GDPR, along with data confidentiality, respectively, for compliance with HIPAA. The study focused on the non-existence or lack of uniformity of regulatory frameworks that can provide for the special characteristics of SaaS data

management and cross-border data flows.

## I. Introduction

SaaS-based systems for laboratory management have given a new meaning to the way work is being done in an already established scientific research setup. These platforms are helping in levels of data management and sharing never witnessed before, but they also bring with them sophisticated ethical and legal dilemmas that need to be delved into in detail. That said, this intro builds a base for a detailed investigation of the ethical and legal implications of data sharing within SaaS-based laboratory management systems. In doing so, strong emphasis is made on the significance of sharing data, the dual-edged nature of SaaS systems, the objectives of this study, and the structure of the ensuing discussion.

### A. Significance of Data Sharing

Scientific advancement, therefore, requires that such data be shared, for they form one of the bases upon which researchers can build their work, validate the findings, and create geographies and discipline-based collaborations. This sharing of data underlies concerted and cooperative action by the scientific community in helping to expand the frontiers of knowledge and innovations. It further ensures the effective processes of research without redundancy and that the most effective use of funding or resources is executed. From the perspective of laboratory management, the integration of

SaaS solutions offers the promise that it could change the manner through which data would be stored, accessed, and shared, assuring a step toward the massive collaboration needed for a more dynamic research ecosystem. However, this development does not come without a set of challenges because this increased access to and sharing of data may raise some ethical issues not only regarding privacy, consent, and integrity of the data but also on legal grounds like ownership, copyright, and adherence to regulatory levels.

### B. SaaS Laboratory Management Systems

Contrastingly, SaaS-based laboratory information systems come with a suite of advantages that match the ever-dynamic modern scientific research needs. Some of these cloud-based platforms come with scalable, flexible, and most cost-effective solutions for laboratory data management, and workflows, while also providing room for real-time collaboration among researchers. Allowing access to the data from anywhere at any time would make research teams even more cohesive, allowing them to react fast to new developments. However, the dependence on third-party service providers, which manage and store sensitive research data, gives several challenges in the context of security, privacy, and control of the data. With this development, there arise several questions that now need to be answered, such as the mechanism to ensure the protection of intellectual property rights and access and control of the data and, more importantly, enforcement of the varied international laws on data protection (Singh et al., 2016).

### C. Study Objectives

This scientific paper seeks to dissect the ethical and legal implications of data sharing in SaaS laboratory management systems by highlighting challenges in identification and proposing frameworks for treading such complexities. Precisely, it will do the following:

Describe the ethical SaaS or data-sharing considerations within SaaS platforms, considering in particular privacy, informed consent, and ethical stewardship of the data.

This section undertakes a study of the legal environment that affects data sharing in the management of laboratories, considering, among other things, issues of copyright and intellectual property rights, compliance with laws on data protection, and liabilities of involved parties.

Propose recommendations for balancing the derived benefits from open collaboration of SaaS laboratory management systems with the protection of the rights and interests of the stakeholders.

### D. Structure of the Paper

The paper is organized in the following manner to systematically discuss the complexities of sharing data within a SaaS Laboratory Management System: from a literature review that frames the discussion within the current state of research. Methodology: This section outlines the approach undertaken in gathering and analyzing data relevant to our objectives. We move to the heart of our discussion, with sections toward considering the morality of the practice, legal implications, and regulations that would affect data-sharing practices. We synthesize the appropriate information concerning these concepts from case studies and expert interviews in an attempt to provide their real-world applications and end with a set of targeted recommendations intended to guide future practice. The following conclusion arrives from the summarized findings and reflections, pointing out the most important aspect: to be ethically and legally diligent in the SaaS-facilitated scientific collaborative era.

## II. Literature review

### A. Data Sharing Practices

Data sharing in the context of SaaS laboratory management systems has received more significant attention on both potential sides and the current practices and gaps in policies. (Palos-Sánchez et al., 2017) argued that models like SaaS bring an increase in accessibility and efficiency in the management and analysis of scientific data, thus allowing one to build stronger research collaborative networks. However, one clear gap was noticed, especially in the literature that dealt with unique challenges and risks of data privacy and security in such environments.

For example, Berman and Cerf (2013) note that while SaaS permits sharing data, and with it, access to a large number of scientists and researchers in different fields, it raises quite important questions about data sovereignty and its ownership or, on the other hand, control, in the period it moves to the cloud. Adjei (2015) more or less concurs with these ideas when they look at the regulatory and ethical systems that need to be in place for protecting sensitive information in cloud-based systems but point to a lack of well-stipulated regulations on this front concerning sensitive information related to laboratory management. In this perspective, literature so far has pointed toward a strong knowledge base for the benefits of SaaS systems and raised a clarion call for carrying out focused research for mitigating the risks of these digital environments. This gap sets the stage for the present investigation to build an approach toward balancing data sharing that respects the work on one side and keeps innovation and integrity alive on the other side.

### B. Ethical Frameworks

The ethical framework that sets the guidance in sharing the laboratory management SaaS systems data certainly ensures such practice can fulfill moral

3

imperatives and be workable in a pragmatic sense. Literature on this subject often emphasizes a need to invent a new set of ethical guidelines that will discuss the peculiarities of the digital and cloud-based environment. Notably, Dhirani (2023) strongly emphasizes that "ethical frameworks should evolve with the technology and squarely focus on the many new challenges presented by SaaS platforms in data-sharing ecosystems. Therefore, their case is for the frameworks that include considerations of data privacy, user consent, and transparency in data usage (Dhirani, 2023).

Moreover, other scholars like Riso (2017) continue to look at the application of classical bioethical values—especially beneficence, non-maleficence, and justice—to the purview of SaaS-based laboratory management. They argue that guidelines have turned into a base because peculiarities of sharing information within digital data require separate, detailed, and special additional guidance about how to struggle with problems related to data breaches and unauthorized use of sensitive information (Riso, 2017).

Recent debates by Kaikkonen (2019) elaborate further on the ethical part of using SaaS platforms with embedded artificial intelligence and machine learning technologies. There now lies a clear call for "responsive ethical codes" that are flexible enough to stand the rapid test of technological change, while ensuring robust protection for the data of participants to keep the trust (Kaikkonen, 2019).

A recent review of the ethical frameworks undergirding the data flow in cloud-based LMSs highlights a rather unanimous consensus from the literature: the need for dynamic, context-relevant guidelines that can be founded on foundational ethical principles but articulate with the unique circumstances of data sharing within the cloud-based LMS. Based on this understanding, the present insight proceeds in providing the foundation for our inquiry into the elaboration and application of such frameworks that seek to reconcile distances between traditional ethical models and needs imposed by modern technological contexts.

### C. Legal and Regulatory Analysis

The study of legal and regulatory frameworks in such a context, given the rapidly changing technology landscapes and their corresponding legal challenges, no doubt forms an important area of scholarship for SaaS-based LIMS. This scientific paper focuses on the application of some of the comprehensive data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Guided by principles, they have strict guidelines in handling data, which for a SaaS company operating internationally, these standards hold huge implications (European Commission, 2016; U.S. Department of Health & Human Services, 1996).

On the other side of the spectrum, Pearson (2010) takes an extensive view of the need for "the legal framework to adapt to the decentralized nature of the data flow" and for SaaS platforms to have very solid compliance measures for them to effectively handle the cross-jurisdictional data (Pearson, 2010). On the other hand, Bartolini (2018) dealt with the issue of intellectual property rights within the SaaS environment, where data ownership interests between stakeholders are still intricate in the matter of access to shared datasets and usages of the same.

The available regulatory frameworks indeed fall short of giving the desired effective protection from peculiar vulnerabilities that are emerging in a cloud-based data management system, as might be testified and most certainly exploited in laboratory settings. These improve measures of the betterment to secure data suitably and to protect susceptible information, lineament with promoting customized updates to regulations (Savolainen, 2023).

### D. Case Studies

In the following case studies, practical ethical and legal dilemmas of data sharing brought forth by SaaS Laboratory Management Systems are brought to light. These real-life examples were highly important concrete instances of how applicable the nuances in applying the theoretical framework to actual situations are: bringing out the complexities that arise when theory meets practice.

One very remarkable instance where a multinational pharmaceutical company used the SaaS-based laboratory management system to make data sharing better among its global research sites. In the example, as Sousa (2023) states, this example is characteristic of the gains in efficiencies and challenges to privacy that the system has brought. Researchers noted that, on one hand, the platform quickened the research process significantly, as it gave real-time access to data. On the other hand, it posed a risk concerning data sovereignty and breach risk, more so, if it crossed from one legal jurisdiction to another (Sousa, 2023).

The other critical case highlighted by Hamilton and Yadegaridehkordi (2020) relates to the collaborative research partnership between academic institutions for the use of a common SaaS platform. The paper underlines the emerging intellectual disputes on the ownership of the data and the attendant challenges that may arise in drafting the agreement that will indeed reflect the contributions of the respective parties in such data collection. This again brings to the forefront the importance of clear, crisp legal frameworks and cooperation agreements within cooperative environments so that both parties can maintain a harmonious working relationship and avoid conflicts that will impede smooth operations (Yadegaridehkordi, 2020).

These case studies are of huge importance in painting the actual ethical and legal complexities that may come up during the deployment and use of SaaS-based laboratory management systems. These results make the clear point that governments can learn much from the US example and point to critical lessons for the robust ethical guidelines and legal agreements that will be needed to help them guide the possible minefields of high-tech data sharing. The real-world applications and challenges documented in these cases suggest areas for future research and policy development that could enhance the governance of data-sharing practices.

## III. Methodology

This methodology helped to derive the ethics and laws behind the consequential effect of sharing data for SaaS Laboratory Management Systems. We synthesized the development conclusions as data from the literature compiled in this article, including case studies and expert opinions.

### A. Methods for Data Collection

The key approach to literature sources data collection was applied through systematic reviews of peer-reviewed journals, industry reports, and authoritative articles among others. In addition, vast literature was also used in the search for laboratory SaaS application documents, data-sharing ethics documents, and legal framework documents from PubMed, IEEE Xplore, and Google Scholar among others. For example, they have used these keywords in combinations: "laboratory management Saas," "ethics data sharing," "implications, legal," and "cloud computing use in research".

It includes public sources of case studies and corporate white papers describing laboratory SaaS implementations, including triumphs and failures, with an accent on their ethical and legal issues.

### B. Sample Choice

The literature and case studies are identified from high-quality and influential sources, and they have been published within the last 15 years. The sources selected were the legal documentation relevant to the jurisdiction in question, relating to the data protection regulations in the EU, US, and Asia. The authors were selected from their published work, professional roles, and experts of the world-famous technology and ethics conversation in leading conferences and seminars.

### C. Methods of analysis

The method of data analysis used was a qualitative synthesis. This method allowed me to identify common themes and divergent opinions on law and ethics based on SaaS data sharing. This allowed the addition of several views on the topic and also gave a more in-depth analysis of the same. Legal issues were that of data ownership, compliance, and intellectual property rights, while the ethical part lay on the line of privacy, informed consent, and data integrity.

Thus, the triangulation of the findings of the literature review with findings of the case study and expert interviews gives the full understanding of the environment in place and, hence, the emerging issues. Triangulation of this nature serves to make the findings of the study strong by supporting or reinforcing evidence through various sources and perspectives (Farquhar, 2020).

## IV. Ethical Considerations

### A. Privacy and Confidentiality

In the SaaS laboratory management systems environment, the issues of privacy and confidentiality are paramount. The research data usually have very sensitive patient information, scientific knowledge in some special jurisdiction, and personal data that would be needed for protection with rigor to sustain trust and adherence to ethical standards.

As described by Abdulsalam (2021), the complexity of ensuring privacy in cloud-based systems is such that the data being handled is stored not only remotely but possibly across different jurisdictions as well. This is to make sure that they strongly embed encryption protocols and access management controls against data compromising with the involvement of any third party that would correspond to their data security framework (Abdulsalam, 2021). It is also pertinent to ensure compliance with laws such as GDPR and HIPAA, which provide a legal framework concerning personal information and health information, respectively, for cloud-based environments (European Commission, 2016; U.S. Department of Health & Human Services, 1996).

For example, privacy by all means is a principal concept that has to be considered at each layer of the development and deployment of the SaaS system, therefore, Liu et al. (2022) place "privacy by design" among the abstract. This ensures that privacy is not an afterthought but is built into the system from its beginning (Liu et al., 2022).

To do this, the lab should develop and implement privacy policies that clearly outline every user of the SaaS Laboratory Management Systems. This is because, on one hand, we have the legislation of necessity that requires occasional audits and updates, and on the other hand, staff continually needs training about what practices of data protection will be the ones to ensure the confidentiality and trust vested in these systems.

### B. Informed Consent

Informed consent is part of the foundational essentials of ethical research, to show that the participants are fully informed about what the research is, the use of their data, and the rights of the participants when participating in the research. A further point of difficulty in obtaining informed consent, particularly in the case of SaaS laboratory management systems, refers to the electronic means by which data collection and management are performed.

The literature identifies that the informed consent process needs to be adapted to the complexities introduced by SaaS platforms, which often imply several layers of data use not immediately transparent to participants. It is, therefore, necessary that the consent forms explicitly dwell on, including, how the data is stored, accessed, and disseminated across the platforms so that the participants are making fully informed decisions based on the comprehensive information (Reichenberger, 2022).

Lastly, Muller (2023) highlights how their findings may be signalling the development of a dynamic consent model that would allow for the modulation of degrees of consent by participants across varied scopes of the research or policies for sharing data at any time. This becomes all the more critical within a SaaS environment, where this flexibility of data management may encroach on the original agreed-upon terms of consent (Muller, 2023).

Best practices stipulate that the consent processes should be ongoing, and not just one-off formalities. This is achievable through maintaining continuous contact with research subjects, therefore actualizing transparency and trust, most especially with the emergence of new uses of data or new advancements in technologies (Goode, 2015). This involvement can be enhanced through regular updating and easy access to the platforms so that the subjects can review, if not modify, their consent at any time.

### C. Balancing Benefits and Risks

In the light of these SaaS laboratory management systems, the ethical principle of balancing benefits and risks acquires special importance, meaning that their potential to bring about great scientific advancement must be weighed equitably against the risks of data misuse, breach, and ethical violations. This balance is critical to maintaining trust and integrity within the scientific community and with the public.

Some authors, such as Bezuidenhout (2013), have discussed the moral dilemmas that emerge with the dual-use potential of shared data. To some authors, data sharing can enable easier and faster scientific discovery, even fostering collaboration, but at the same time allows more risks to privacy and unauthorized use. The authors propose building up strong risk assessment protocols that will evaluate the potential harms and benefits within various stages of the data-sharing processes (Bezuidenhout, 2013).

Additionally, Slade (2013) emphasizes the need for transparency and accountability in managing these risks. This means that data ethics should be part of the protocols developed for data sharing by ethical oversight committees to ensure that any data-sharing activity between institutions includes an ethical outlook, with a focus on the minimal harm and maximal benefit to society (Slade, 2013).

In addition, the use of technological solutions, including data de-identification and secure data-sharing platforms, could aid in risk minimization. In the same breath, these technologies should provide mechanisms through which the data they protect can be used to do research productively and at the same time maintain very basic privacy levels and fend off potential misuse of the data. It is, therefore, imperative that such measures are carried through so that due balance between risk and benefit can be maintained—proof of shoring up the edifice of ethical research practice.

### D. Ethical Standards Maintenance

In this respect, the data-sharing practices with the laboratory management systems of SaaS are specifically taken into regard with the maintenance of the ethical standard, so that they effectively meet both the ethical guideline and regulatory requirements. This includes developing clear protocols for managing the data, regularly looking over it, and most importantly, developing a culture of alertness toward ethics in each of the parties involved.

As emphasized in the literature, the essentials stipulate the development of very broad ethics guidelines that essentially target the fine management of digital data in the SaaS environment. These should be data integrity points, including consent and privacy protection for subjects, for the two parties to be made aware of ethical responsibility (Reamer, 2017).

These standards further need follow-up with continuous training and education at different levels to make the researchers and the technical staff aware of the ethical issues. This enhances the argument of Bos-Brouwers (2010) that another good strategy that the management can employ to ensure the staff has been updated on the most recent ethical practices and technology is the organization holding periodic workshops and seminars. This will enhance the focus on the practice of ethics in operations.

Besides, ethical audits are important in maintaining the standards and must be done at appropriate intervals to judge whether the company is in line with its inner guidelines and outside regulations, thus pointing at areas that could be

improved. This kind of audit may bring forth results that will guide the revision of the protocols and practices such that the SaaS systems are not only efficient but ethically sound.

The implementation of these measures will require leadership committed to ethical considerations as the core aspects of organizational strategy, with an eye on ensuring that organizational strategic imperatives do not override the need to uphold high standards of social, environmental, and economic practices.

## V. Legal Implications of Data Sharing in SaaS Laboratory Management Systems

### A. Data Ownership and Intellectual Property

Within this SaaS realm, data ownership questions on laboratory management systems and, by extension, usage rights continue to represent some of the most difficult legal battles, along with intellectual property (IP) rights. Scientific research environments are data-rich areas, so generally moving to cloud-based systems raises the question of who owns this data and what is due to the holders of intellectual property, i.e., the creators and users or SaaS providers.

The complexity of ownership involves three main parties in the SaaS environment. Data contributors, like researchers generating the data, or their institutions, on whose behalf the research is being carried out, are many at times considered to have stakes in the ownership of the data, besides other third-party SaaS providers that manage the data storage and processing aspects. This becomes a veritable labyrinth when international projects are concerned, since about the ownership right, one might have laws of different countries entering into contradiction with others. As Bartolini (2018) further advises, it is highly important to define this ownership well within user agreements, noticing it as a very good prevention method for avoiding any possible disputes that might consequently slow down research and innovation.

In the same way, intellectual property rights can be very complex. The following uses SaaS and therefore would arise in a case where the line between IP control and the terms upon which the SaaS platform is uploaded becomes indistinguishable: Opara-Martins (2017) stresses the fact of strong IP clauses in the contracts with SaaS providers; on the one side, it will allow the creator to maintain control of his contributions, while on the other, data usage and contributions made should comply with the agreed terms.

### B. Data Protection Laws

Basically, use of the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States can never be overemphasized as far as regulation of SaaS-based data sharing is concerned. These are going to give frameworks within which data will be ethically handled from misuse; the data might be personal and sensitive.

It imposes very strict requirements for processing the data, such as minimizing the data, limiting the purposes, and accuracy of the data, and giving rights to individuals to access, rectify, and erase the data. The GDPR is very explicit on compliance with any SaaS system that either operates or has data from EU citizens (European Commission, 2016).

The SaaS systems are subject to HIPAA rules, which regulate the confidentiality and security of U.S. medical information that is shared through electronic health records. The rule calls for safeguards: administrative, physical, and technical means that shall be applied in the protection of patient data—for example, assessment of risks and the encryption of data in transmission (U.S. Department of Health & Human Services, 1996).

### C. Legal Responsibilities

Therefore, the legal obligation for the parties concerned with SaaS-based data sharing is data accuracy. On the other hand, the creators of the data—mostly either researchers themselves or institutions—have a moral obligation to ensure that the data they make available are accurate and reliable and that it must have been collected ethically. They must navigate the aegis of consent processes required for data collection from individuals so that participants are properly informed of the nature in which their data shall be used.

SaaS providers, therefore, should not only protect the data in their platforms with strong security but most importantly should be able to ensure observance of pertinent laws regarding data protection from their side. They should be open in their operations, helping users to understand how their data is taken care of, stored, and possibly shared with other parties.

Any further use of the data, such as that used by researchers who have been granted access to shared datasets for analysis, must be done under the terms outlined in the access agreement. This should include the commitment to the confidentiality and privacy of the data subjects and compliance with the limitation and restriction of data use.

This, therefore, means that legal implications and regulations about data sharing through

SaaS laboratory management systems are still to be well-defined with a good knowledge of the data owner, respective rights of the parties related to intellectual property, and laws of data protection and obligations from the parties involved. More so, if the context of this article has clearly laid down legal agreements and assured conformity to the law for a secured and productive environment in scientific collaboration, this can further be lessened.

## VI. Regulatory Frameworks Governing Data Sharing in SaaS Laboratory Management Systems

### A. Regulatory frameworks

Regulatory frameworks One of the leading tasks relating to the deployment and use of these technologies in compliance with legal standards and ethical norms in SaaS-based Laboratory Management Systems is to regulate data sharing between the system's users, as well as general control.

These frameworks contain very many international laws on data protection and standards specific to industries that seek to protect the integrity of the data being exchanged across the platforms, besides ensuring confidentiality. If you consider the European Union's General Data Protection Regulation (GDPR) as one of the most prominent frameworks, it raises significantly high levels for ensuring the protection of personal data, obliging those responsible and, respectively, processing it to ensure privacy and the security of data. This includes enforcing data subject rights and implementing data protection measures (European Commission, 2016).

The United States follows the Privacy and Security of Health Information by the Health Insurance Portability and Accountability Act (HIPAA), which in general, sets standards for securing the handling, transmission, and disclosure of protected health information (U.S. Department of Health & Human Services, 1996). There are several widely specific standards on the subject within the industry. For example, the International Organization for Standardization (ISO) provides ISO/IEC 27001 as requirements for information security management systems (ISMS) at the organizational level with sensitive information from the company and clientele using SaaS platforms (ISO/IEC, 2021). The foregoing thus forms very essential standards for SaaS Providers in Laboratory Management to ensure that their clients are served with the highest security criterion possible.

**B. Regulatory Gaps and Challenges**

Adequate guidance in this respect is the existing framework but still suffers from important gaps, most notably about the rapid pace at which new technology advancements are occurring within SaaS technologies. The challenge becomes more onerous due to the difficulty of jurisdictions created when the data crosses different boundaries, thus, at times, having the effect of a compliance nightmare as a result of different legal requirements.

Besides, regulations that apply to SaaS platforms may lack specificity and applicability. This is caused by uncertainty in the responsibilities of location-related and access control obligations concerning the data, given the fact that traditional laws on data protection do not cover those required by the cloud for dynamic resource allocation and data handling (Greenleaf, 2017).

The granularity of consent and individual control over data is another area where existing frameworks often fall short. Most of the SaaS applications are not very clear and direct to the users on how their data is managed and shared between platforms, hence making it even harder to enforce consent under individualized data rights-focused laws, such as GDPR (Bygrave, 2014).

**C. Recommendations for Regulatory Enhancements**

The following proposals for enhancement to the regulatory frameworks could be considered to tackle these challenges:

**International Standard Setting:** An international standard in the area of cloud data management may contribute to the harmonization between jurisdictions and help SaaS providers be applied to the same set of rules, independently of hosting or processing the data.

**Data Protection Laws Amended:** Specific provisions of data protection laws applying to cloud computing and the SaaS platform will lead to a clearer understanding in respect to responsibilities and duties of all parties involved for data handling.

That would include data on data localization requirements, clearer guidelines on issues of data ownership, and, of course, heightened rights of data subject individuals from within the SaaS systems.

**Regulatory Sandboxes**: Setting up regulatory sandboxes, where regulators and SaaS providers together, with users, will be able to experiment with new and innovative techniques of data sharing and privacy in a controlled environment, would encourage the adoption of new technology and put in place both strong and flexible regulatory frameworks (Kuner, 2010).

## VII. Conclusion

This critical review of ethical and legal implications concerning data sharing in SaaS-based laboratory management systems uncovers a complex web of challenges and considerations. The main ethical issues that should be included in data sharing include data privacy, security, and the problem of informed consent. From a legal perspective, the focus will be on the protection of ownership and intellectual property rights, whereby adherence to the various data protection laws has been stipulated under the GDPR and HIPAA. The findings underscore the necessity for adaptive frameworks with changes in technology and globalization of research.

The main question of ethics concerns the consideration of privacy, when in this case, the data is always prone to leakage or unauthorized access, therefore requiring permanent vigilance and possible tightening up of security measures. The legal environment is even more complex with the international dimensions of SaaS platforms—bunches of laws to reconcile worldwide.

Concerning the use of SaaS platforms in data sharing, researchers should put in place ethical and legal dimensions. They should observe relevant laws and ethics, more so in consent and informed protection of data.

There is, therefore, the need for institutions to come up with clear policies on how data management, security protocols, and training programs will help guide staff to know the ethical and legal issues regarding sharing over a SaaS platform.

SaaS providers need to focus on security above everything, conforming even more to international standards of data protection. In addition to this, it should provide clear documentation of its data handling and privacy policies that would guide users in understanding and being assured about the approaches to data security and compliance.

Policymakers are to always update and fine-tune data protection laws in step with technological progress. They, therefore, should be in a position to come up with more specific regulations that take care of the specific challenges in cloud computing and the SaaS environment so that judicious and ethical use may be ensured.

## VIII. Future Research Directions

This, therefore, is a call for future research that will focus on these critical areas that would otherwise be helpful in the understanding and mitigation of ethical and legal risks in the practice of data sharing under SaaS. This includes next-generation security technologies that enhance data privacy without losing efficiency in scientific collaboration. In this age of data sharing and exchange of information as enforcement across research settings, one has to delve into new principles focusing on the techniques of encryption, access controls, and anomaly detection systems.

Moreover, further study of the impacts of new technologies, including artificial intelligence (AI) and machine learning, on data-sharing practices is important. Such technologies open a new set of legal and ethical questions, in particular for bias, transparency of decision-making, and the use of data produced by artificial intelligence.

Similarly, more work needs to be done, with technologists and legal scholars working together to look at how international law may develop to fit better with the transnationality problems presented by SaaS platforms. The same shall, therefore, include the scrutiny of, inter alia, the feasibility of a universally applicable legal regime that can take care of such data protection-related complications in diverse legal systems successfully.

Last but not least, these ethical frameworks need some periodic reviews because the technologies and practices of sharing data have changed. This simply means revisiting or updating the ethical guidelines through input from empirical research and feedback from stakeholders, which would update such knowledge or more likely, change societal values reflected in them as and when required.

Although SaaS comes with a huge plethora of benefits for laboratory management and scientific research, it likewise brings a series of ethical and legal challenges that have to be carefully managed. Preempting these issues and constantly adjusting to the developments would put the scientific community in a position where they can turn these powerful tools into an even more responsible and effective weapon.

**IX. References**

Singh, A., Sharma, S., Kumar, S. R., & Yadav, S. A. (2016, February). Overview of PaaS and SaaS and its application in cloud computing. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 172-176). IEEE.

Berman, F., & Cerf, V. (2013). Who will pay for public access to research data? Science, 341(6146), 616-617.

Palos-Sánchez, P. R., Arenas-Márquez, F. J., & Aguayo-Camacho, M. (2017, January 1). Cloud Computing (SaaS) Adoption as a Strategic Technology: Results of an Empirical Study. Journal of Mobile Information Systems. https://doi.org/10.1155/2017/2536040

Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. Info, 17(1), 54-67.

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: a review. Sensors, 23(3), 1151.

Riso, B., Tupasela, A., Vears, D. F., Felzmann, H., Cockbain, J., Loi, M., & Rakic, V. (2017). Ethical sharing of health data in online platforms–which values should be considered? Life sciences, society, and policy, 13, 1-27.

Kaikkonen, T. (2019). SaaS Application Integration Challenges.

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and making technological advances benefit all parties concerned without compromising ethical and legal standards. of the Council. Regulation (EU), 679, 2016.

Act, A. (1996). Health insurance portability and accountability act of 1996. Public law, 104, 191.

Pearson, S., & Benameur, A. (2010, November). Privacy, security, and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE.

Bartolini, C., Santos, C., & Ullrich, C. (2018). Property and the cloud. Computer Law & Security Review, 34(2), 358-390.

Savolainen, S. (2023). Evaluating security and privacy of SaaS service.

Sousa, R., Peixoto, H., Abelha, A., & Machado, J. (2023, July). Implementing a Software-as-a-Service Strategy in Healthcare Workflows. In International Symposium on Distributed Computing and Artificial Intelligence (pp. 347-356). Cham: Springer Nature Switzerland.

Yadegaridehkordi, E., Nilashi, M., Shuib, L., & Samad, S. (2020). A behavioral intention model for SaaS-based collaboration services in higher education. Education and information technologies, 25, 791-816.

Farquhar, J., Michels, N., & Robson, J. (2020). Triangulation in industrial qualitative case study research: Widening the scope. Industrial Marketing Management, 87, 160-170.

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.

Liu, H., Wang, Y., Fan, W., Liu, X., Li, Y., Jain, S., & Tang, J. (2022). Trustworthy ai: A computational perspective. ACM Transactions on Intelligent Systems and Technology, 14(1), 1-59.

Reichenberger, J., Radix, A. K., Blechert, J., & Legenbauer, T. (2022). Further support for the validity of the social appearance anxiety scale (SAAS) in a variety of German-speaking samples. Eating and Weight Disorders-Studies on Anorexia, Bulimia, and Obesity, 27(3), 929-943.

Muller, S. H., van Thiel, G. J., Mostert, M., & van Delden, J. J. (2023). Dynamic consent, communication and return of results in large-scale health data reuse: Survey of public preferences. Digital Health, 9, 20552076231190997.

Goode, S., Lin, C., Tsai, J. C., & Jiang, J. J. (2015). Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. Decision Support Systems, 70, 73-85.

Bezuidenhout, L. (2013). Data sharing and dual-use issues. Science and engineering ethics, 19, 83-92.

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. American Behavioral Scientist, 57(10), 1510-1529.

Reamer, F. G. (2017). Evolving ethical standards in the digital age. Australian Social Work, 70(2), 148-159.

Bos-Brouwers, H. E. J. (2010). Corporate sustainability and innovation in SMEs: Evidence of themes and activities in practice. Business strategy and the environment, 19(7), 417-435.

Bartolini, C., Santos, C., & Ullrich, C. (2018). Property and the cloud. Computer Law & Security Review, 34(2), 358-390.

Opara-Martins, J. (2017). A decision framework to mitigate vendor lock-in risks in cloud (SaaS category) migration (Doctoral dissertation, Bournemouth University).

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 33(7), 76-105.

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Including Indonesia and Turkey (January 30, 2017), 145, 10-13.

Bygrave, L. A. (2014). Data privacy law: an international perspective.

Kushner, C. (2010). Regulation of transborder data flows under data protection and privacy law: past, present, and future. TILT Law & Technology Working Paper, (016)