Review Article

The Challenges of Data Privacy and Cybersecurity in Cloud Computing and Artificial Intelligence (AI) Applications for EQA Organizations

Alexander Haliassos[1*], Dimitrios Kasvis[2], Serafeim Karathanos[1]

[1]*ESEAP & GSCC-CB, Athens, Greece*
[2]*HeadWay Consultants, Athens, Greece*

Article Info

[*]***Corresponding Author:***
Alexander Haliassos
ESEAP & GSCC-CB, Athens, Greece
E-mail: haliassos@moleculardiagnostics.gr

Keywords

Cybersecurity, Data Privacy, Cloud Computing, artificial intelligence, AI, EQA, PT

Abstract

Background: The adoption of cloud computing and Artificial Intelligence (AI) technologies offers significant advantages for External Quality Assessment (EQA) providers, including scalability, cost efficiency, and broader accessibility. However, these benefits come with substantial cybersecurity and data privacy challenges.

Methodology: We performed a systematic literature review on cybersecurity risks in healthcare cloud computing, consulted experts in bioinformatics and cybersecurity, and analyzed real-world hacking incidents targeting EQA organizations. A risk-focused framework was developed to outline key challenges and best practice mitigation strategies.

Results: Ten key challenges were identified: 1. data breaches and unauthorized access, 2. compliance with regulations such as HIPAA and GDPR, 3. data sovereignty and jurisdictional issues, 4. shared infrastructure vulnerabilities, 5. insider threats, 6. data loss and availability concerns, 7. inadequate security measures by cloud providers, 8. application vulnerabilities, 9. limited visibility and control, and 10. the complexity of cloud security management.

Conclusion: To fully benefit from cloud computing and AI, EQA providers must implement robust security practices, ensure regulatory compliance, and continuously monitor their environments. Proactive cybersecurity strategies are essential to safeguarding sensitive laboratory data and maintaining operational continuity and accreditation.

Introduction

External Quality Assessment (EQA) schemes have long served as critical tools in maintaining the reliability, accuracy, and comparability of laboratory testing worldwide. Firstly, implemented in limited, often local settings with a small number of participants performing interlaboratory comparison of results on shared samples, EQA schemes have evolved significantly over the past decades [1]. The increasing complexity of laboratory diagnostics, combined with globalization and regulatory demands, has led to a dramatic rise in the number of participating laboratories and the volume of data generated during each EQA cycle. As a result, EQA providers have turned to cloud computing and, more recently, artificial intelligence (AI) technologies to efficiently manage, analyze, and report these large-scale data sets.

Cloud computing offers a scalable, cost-effective, and collaborative environment that supports real-time data access, centralized data storage, automated workflows, and streamlined communication between EQA providers and participant laboratories [2,3]. Similarly, AI technologies, including adaptive machine learning algorithms, natural language processing, and data mining, are increasingly used to automate result evaluations, detect errors, provide personalized feedback, and identify performance trends across laboratories. These innovations enable more dynamic and responsive EQA processes that better support continuous quality improvement in diagnostic testing.

However, as EQA operations become more digitally interconnected, the nature and severity of cybersecurity risks escalate. The sensitive nature of laboratory data that contains patient-related or institution-specific identifiers, combined with the widespread distribution of EQA participants across different countries and regulatory environments, makes EQA platforms attractive targets for cyberattacks. Additionally, the reliance on third-party cloud service providers raises critical questions about data governance, regulatory compliance (e.g., GDPR), and risk ownership in the event of a security breach.

The growing sophistication of cyber threats, ranging from ransomware and phishing campaigns to advanced persistent threats, highlights the urgent need for robust data protection mechanisms and proactive cybersecurity strategies. For EQA providers, ensuring data privacy and system integrity is not merely a technical challenge but a fundamental requirement for maintaining trust, safeguarding accreditation processes, and protecting the broader public health landscape [3].

This paper aims to explore the current and emerging challenges related to data privacy and cybersecurity in the context of cloud computing and AI adoption among EQA providers. Through case examples, risk analysis, and discussion of regulatory frameworks, we aim to provide actionable insights for EQA organizations seeking to navigate the complex digital ecosystem while upholding the highest standards of quality and data protection.

Methodology

Our approach included a comprehensive literature review of recent publications indexed in PubMed, Scopus, IEEE Xplore, and ScienceDirect, as well as reports from cybersecurity authorities such as ENISA and the CVE (Common Vulnerabilities and Exposures) database. The references included in this study (1–16) were identified using the following search terms and combinations: “cybersecurity healthcare”, “cloud computing data breach”, “EQA cybersecurity risks”, “AI in EQA”, “cybersecurity”, and “healthcare ransomware attacks”.

We analyzed real-life cases of cyberattacks on healthcare systems and EQA platforms. In addition, we gathered more information through targeted consultations with three experts in the field. These discussions were based on open-ended questions designed to understand emerging threats, common vulnerabilities, and potential mitigation strategies. The findings from the literature review, case studies, and expert input were synthesized to develop a comprehensive framework outlining the main challenges and recommended countermeasures for EQA organizations.

Results

1. Data Breaches and Unauthorized Access

Unauthorized access to sensitive laboratory or participant data is one of the most critical cybersecurity concerns for EQA providers operating within cloud-based environments. EQA workflows, which involve the submission, processing, and evaluation of diagnostic data from multiple laboratories, inevitably generate large volumes of potentially identifiable information. When hosted in the cloud, data becomes vulnerable to exploitation through weak credentials, misconfigured access policies, lack of encryption, or insufficient activity monitoring [4].

To mitigate these risks, EQA providers should implement a multilayered security strategy that begins with robust user authentication. Multi-factor authentication (MFA) must be used at all access points, especially for administrative and evaluator roles, to help prevent unauthorized access. MFA requires users to verify their identity with at least two independent credentials, usually something they know (like a password) and something they have (such as a one-time code, hardware token or an authenticator app on their phones). This approach lowers the chance of unauthorized access, even if passwords are stolen or credentials are compromised [5,6].

Equally important is implementing strict role-based access control (RBAC), which ensures that users only access data and system functions necessary for their defined responsibilities. The principle of least privilege should drive all access permissions, with temporary elevation of rights used only in exceptional cases. Such segmentation significantly limits the potential damage in case of account compromise, minimizing the impact of the attack [7].

Encryption constitutes another fundamental safeguard. All

EQA-related data stored in cloud infrastructure should be encrypted at rest using industry-standard algorithms such as AES-256. Also, data in transit must be protected with a secure communication protocol, preferably TLS version 1.2 or higher, to prevent interception or tampering during upload, retrieval, or analysis [8].

2. Compliance with Regulations

EQA organizations that manage laboratory and healthcare-related data in the cloud must ensure compliance with national and international data protection frameworks. Among the most prominent regulations are the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. These frameworks impose strict requirements on how personal information is stored, accessed, and transmitted, making regulatory compliance not only a legal obligation but also a crucial component of maintaining trust and integrity within the EQA ecosystem [9].

Ensuring compliance in cloud environments presents particular challenges, as control over the underlying infrastructure is often limited. Cloud service providers may not consistently meet all regulatory requirements and consequently EQA providers must take an active role by confirming that their chosen cloud platforms offer the necessary technical and organizational safeguards.

There are cloud providers that offer a range of tools to support compliance management. Platforms such as AWS Artifact, Microsoft Azure Compliance Manager, and Google Cloud's compliance resource center provide documentation, risk assessment templates, and automated controls aligned with regulatory standards.

Beyond the documentation and controls, real-time monitoring of data handling practices is essential. EQA systems should be configured to log all access and activity related to sensitive datasets, including uploads, downloads, modifications, and user authentication events. Audit tools such as AWS CloudTrail, Azure Monitor, and Google Cloud Audit Logs enable continuous surveillance and traceability, which are critical for identifying compliance gaps and responding to incidents [10].

For EQA organizations, failure to comply can lead to significant financial penalties, reputational damage, and loss of credibility among participating laboratories and accreditation bodies.

3. Data Sovereignty and Jurisdictional Issues

Another highly important cloud computing risk for EQA providers is the issue of data sovereignty. As EQA applications increasingly rely on global cloud infrastructures, the potential for laboratory or patient data to be stored or transferred across multiple jurisdictions raises serious compliance and governance concerns as it becomes subject to the laws and political dynamics of the host countries and sometimes outside the control or awareness of the data owner.

A critical risk arises when cloud infrastructure is managed or controlled by entities based in a single country. In the case of geopolitical tensions, sanctions, or policy shifts, that country could stop or restrict service provision to other regions.

To mitigate such risks, EQA organizations must implement strict data residency controls. Many platforms offer options to select specific geographic regions for data storage. These tools allow organizations to restrict data within legally permitted areas. Additionally, geofencing mechanisms can be configured to restrict data flows and processing to pre-approved areas, reducing the risk of non-compliant cross-border transfers [9,10].

Regular consultation with legal and compliance specialists ensures that storage and processing strategies are aligned with applicable local regulations, especially when operating in multiple countries or handling data from multinational laboratory networks.

4. Shared Infrastructure Vulnerabilities

Cloud environments typically operate on shared infrastructure, where multiple tenants utilize the same underlying hardware through virtualization technologies. While this model enables scalability and cost efficiency, it also introduces risks. A failure in isolation mechanisms through hypervisor exploits, container escape vulnerabilities, or misconfigured virtual machines could result in unauthorized access to sensitive data hosted by other tenants.

To address these concerns, EQA organizations should enforce strict workload isolation by deploying services within dedicated virtual private clouds (VPCs) or segmented virtual networks. Network segmentation using firewalls, subnets, and security groups adds further restriction. Ensuring hypervisors and container runtimes are regularly patched is essential, along with leveraging hardware-level virtualization protections such as Intel VT-x or AMD-V [11,12].

5. Insider Threats

In addition to external cyberattacks, internal threats raise a significant risk to data confidentiality. Cloud service provider employees could theoretically have access to underlying systems, and without strong internal safeguards, this access could be used to retrieve or manipulate sensitive EQA or healthcare data.

To mitigate this risk, EQA organizations should implement strict access control frameworks, including just-in-time (JIT) provisioning and immediate revocation of access when no longer required. In addition, monitoring all administrative activities using cloud-based tools, such as AWS CloudWatch, Azure Security Center, or Google Cloud Security Command Center, can identify mishandling and enforce accountability.

Most importantly, by using customer-managed encryption keys (CMKs), organizations retain exclusive control over the encryption and decryption of their data, thereby minimizing the risk of unauthorized access even at the provider level [13].

6. Data Loss and Availability Concerns
Service outages, accidental deletions, or even data corruption can also occur in cloud-based systems and seriously impact the continuity of EQA operations and the availability of critical laboratory information. Without robust backup and recovery strategies, such events can lead to irreversible data loss or extended downtime that put at risk the reporting schedules and stakeholder trust.
In order to avoid these risks, EQA organizations should adopt automated backup procedures, ensuring that backups are encrypted and distributed across multiple regions to protect against localized failures. Disaster recovery plans must be routinely tested to validate their effectiveness in real-world scenarios. Additionally, designing infrastructure with built-in redundancy, such as deploying applications across multiple availability zones or regions, enhances resilience. High-availability database services like AWS RDS Multi-AZ, Azure SQL Database with geo-replication, or Google Cloud Spanner can further support business continuity during unexpected outages [14].

7. Inadequate Security Measures by Cloud Providers
Not all cloud providers implement the same security practices, and some may not implement basic protections such as strong encryption, intrusion detection systems, or application-level firewalls. For EQA organizations handling sensitive laboratory data, blindly relying on a provider's default controls can leave critical assets exposed to cyberthreats.
For this reason, organizations should perform rigorous and detailed search before selecting a provider by evaluating security certifications (e.g., ISO 27001, SOC 2), independent audit reports, and compliance documentation. Once committed, they should leverage the provider's advanced platform security services, such as AWS GuardDuty, Azure Defender, or Google Cloud Security Scanner. Importantly, cloud-based security should be reinforced with third-party tools such as endpoint protection platforms, intrusion detection/prevention systems (IDS/IPS), and web application firewalls (WAFs), offering an additional layer of defense beyond the provider's basic level [15].

8. Application Vulnerabilities
EQA applications hosted in the cloud may be vulnerable due to insecure code, misconfigured Application Programming Interfaces (APIs), or outdated components. Such weaknesses can be exploited by hackers to gain unauthorized access, manipulate data, or disrupt services.
To address this risk, organizations must integrate secure development practices throughout the software lifecycle. This includes applying static and dynamic security testing (SAST/DAST), conducting regular code reviews, and performing security audits before deployment. Particular attention should be paid to API security, as exposed interfaces are common attack vectors. APIs should be protected with protocols like OAuth 2.0, governed by rate-limiting policies, and managed through API gateways. Additionally, strict input validation and sanitization must be enforced to prevent injection attacks [11,16].

9. Limited Visibility and Control
A common challenge in cloud-based environments is the limited visibility that organizations have over their own data, infrastructure, and security configurations. For EQA providers, this lack of transparency can hinder timely detection of threats, delay incident response, and complicate compliance monitoring.
To overcome these limitations, organizations should implement centralized logging and monitoring using platforms like AWS CloudWatch, Azure Monitor Logs, or third-party tools such as Splunk or the ELK Stack. These solutions enable real-time visibility across distributed systems. Additionally, deploying Cloud Security Posture Management (CSPM) tools such as AWS Config, Azure Policy, or Prisma Cloud, helps maintain continuous oversight of configuration drift and policy violations. When integrated with Security Information and Event Management (SIEM) systems, these tools provide a comprehensive view of security events and support rapid threat detection and remediation across the cloud environment [16].

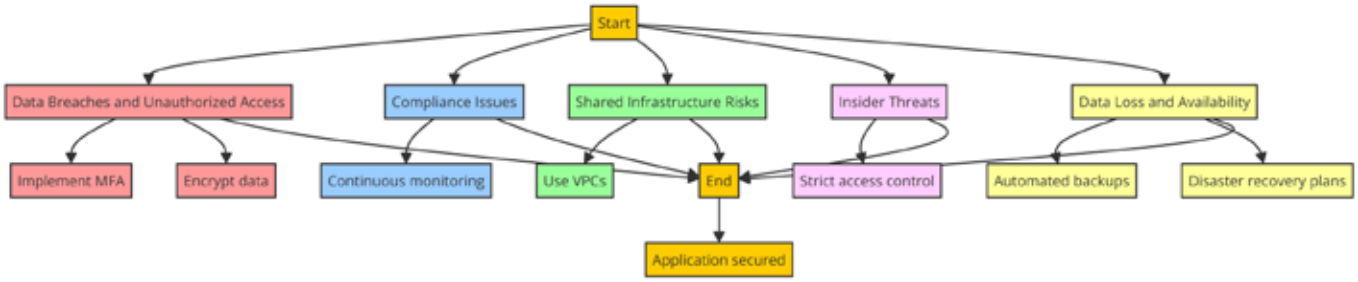
10. Complexity of Cloud Security
In contrast to traditional systems, cloud infrastructures are highly dynamic, involve numerous interdependent services, and require specialized expertise. Without proper controls and up-to-date knowledge, misconfigurations or overlooked vulnerabilities can create critical security gaps.
To manage this complexity, EQA organizations should adopt Infrastructure as Code (IaC) tools - such as Terraform, AWS CloudFormation, or Azure Resource Manager - that enable consistent and automated implementation of secure configurations. Regular security audits and vulnerability assessments, using tools like Nessus, Qualys, or native cloud scanners, are essential to proactively identify risks. Equally important is investing in ongoing training for technical staff, ensuring that both development and operations teams are trained and familiar with current best practices and awareness of evolving cloud threats.

Discussion
Examples from real-world incidents reinforce the criticality of addressing these challenges. The 2019 AMCA breach, affecting nearly 20 million patients, was caused by insufficient encryption practices. Cloud outages like AWS S3's 2017 downtime highlighted the need for resilient disaster recovery plans [17].
Countermeasures must combine technical, procedural, and legal elements. Technologies such as MFA, CMKs, SIEM, VPC segmentation, and automated configuration management significantly reduce risk. At the organizational level, training,

strict access policies, and legal compliance frameworks must be maintained.

In Figure 1, a flowchart summarizing the recommended security measures provides a systematic approach to securing cloud-based EQA infrastructures, beginning from basic access control to advanced threat detection and automated audits.

Figure 1: Security measures for cloud-based EQA infrastructures.



In Figure 2, we present interwoven the solutions to all possible security issues that lead to our ultimate goal, the security of healthcare and EQA applications on the net.

Figure 2: Solutions to all possible security issues.

References

1. Buchta C, Marrington R, De la Salle B, Albarède S, Badrick T, Bietenbeck A, et al. Behind the scenes of EQA – characteristics, capabilities, benefits and assets of external quality assessment (EQA) Part I – EQA in general and EQA programs in particular. Clin Chem Lab Med. 2025;63(5):844–858. doi:10.1515/cclm-2024-1289.
2. Sobeslav V, Maresova P, Krejcar O, Franca TCC, Kuca K. Use of cloud computing in biomedicine. Journal of Biomolecular Structure and Dynamics. 2016;34(12):2688–2697. doi:10.1080/07391102.2015.1127182
3. Al-Issa Y, Ottom MA, Tamrawi A. EHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering. 2019;2019:7516035. doi:10.1155/2019/7516035.
4. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare data breaches: Insights and implications. Healthcare (Switzerland). 2020;8:100. doi:10.3390/healthcare8010100.
5. De Carvalho Junior MA, Bandiera-Paiva P. Health Information System Role-Based Access Control

Current Security Trends and Challenges. Journal of Healthcare Engineering. 2018;2018:6510249. doi:10.1155/2018/6510249.
6. Williamson J, Curran K. The Role of Multi-factor Authentication for Modern Day Security. Semiconductor Science and Information Devices. 2021;3(1):16–23. doi:10.30564/ssid.v3i1.3152.
7. Saffarian M, Sadighi B. Owner-based role-based access control OB-RBAC. In: ARES 2010 - 5th International Conference on Availability, Reliability, and Security. (ARES). 2010;236-241. doi:10.1109/ARES.2010.94.
8. Mohamed NN, Othman H, Isa MAM, Noor NAM, Hashim H. A secure communication in location based services using AES256 encryption scheme. In: ISCAIE 2017 - 2017 IEEE Symposium on Computer Applications and Industrial Electronics. Institute of Electrical and Electronics Engineers (ISCAIE). 2017;163-167. doi:10.1109/ISCAIE.2017.8074970.
9. Rose RV, Kass JS. Mitigating Cybersecurity Risks. Continuum. 2017;23(2):553–556. doi:10.1212/CON.0000000000000442.
10. Ng MY, Helzer J, Pfeffer MA, Seto T, Hernandez-Boussard T. Development of secure infrastructure for advancing generative artificial intelligence research in healthcare at an academic medical center. J Am Med Inform Assoc. 2025;32(3):586–588. doi:10.1093/jamia/ocaf005.
11. Schabacker DS, Levy LA, Evans NJ, Fowler JM, Dickey EA. Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. Front Bioeng Biotechnol. 2019;7. doi:10.3389/fbioe.2019.00061.
12. Regola N, Chawla NV. Storing and using health data in a virtual private cloud. J Med Internet Res. 2013;15(3). doi:10.2196/jmir.2548.
13. Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. PeerJ Comput Sci. 2022;8:e964. doi:10.7717/peerj-cs.964.
14. Miller AR, Tucker CE. Encryption and the loss of patient data. J Policy Anal Manage. 2011;30(3):534–556. doi:10.1002/pam.20590.
15. Whaiduzzaman M, Gani A. Measuring security for cloud service provider: A third-party approach. In: 2013 International Conference on Electrical Information and Communication Technology (EICT). IEEE; 2014. doi:10.1109/EICT.2014.6777855.
16. González-Granadillo G, González-Zarzosa S, Diaz R. Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors. 2021;21(14):Article/status. doi:10.3390/s21144875.
17. Alder S. Multistate settlement resolves 2019 American Medical Collection Agency data breach investigation. HIPAA Journal [Internet]. 2021 Mar 12 [cited 2025 Aug 20]. Available from: https://www.hipaajournal.com/multistate-settlement-resolves-2019-american-medical-collection-agency-data-breach