Balancing Consent and Privacy in AI-Driven Health Sciences Education in the GCC: A Comparative Policy and Practice Analysis

Omar AlJadaan[1], Satheesh Babu[2], Shashi Kant Gupta[3]

[1,2]Lincoln University College - Malaysia; [3] Institute of Engineering and Technology-Chitkara University

Email ID
pdf.OmarTurki@lincoln.edu.my
satheeshbabu@lincoln.edu.my
raj2008enator@gmail.com

Abstract

Objective: The rapid integration of artificial intelligence (AI) in health sciences education across the Gulf Cooperation Council (GCC) raises pressing questions about how informed consent and data privacy are managed in learning systems. While AI promises personalized pathways and immersive simulations, it also creates new risks around ethical boundaries.

Methods: This paper draws on recent literature (2023–2025), institutional policies, and grey reports from GCC universities. A comparative lens is applied, mapping local practices against global frameworks such as GDPR (Europe), FERPA (United States), and Asia-Pacific privacy laws.

Results: The analysis shows that GCC countries have made meaningful strides, especially with data protection laws in the UAE and Saudi Arabia's National Data Management Office frameworks. Yet, gaps remain in operationalizing consent, ensuring transparency in algorithmic decisions, and aligning institutional practices with international norms. Several case studies from regional universities highlight both promising initiatives and overlooked vulnerabilities.

Conclusion: The findings suggest that while GCC institutions are heading in the right direction, there is a need for unified regional policies and stronger alignment with global models. The paper offers practical recommendations for harmonizing consent frameworks, enhancing student trust, and embedding privacy into AI-driven education by design.

Keywords: AI in education; GCC universities; informed consent; data privacy; health sciences

✦ Introduction

Artificial intelligence (AI) is no longer a futuristic buzzword in health sciences education; it's already reshaping classrooms, clinics, and even student study habits. I've seen firsthand how medical students in the Gulf Cooperation Council (GCC) are using AI-driven tutoring platforms and virtual patient simulations to practice diagnoses without the fear of harming a real patient. These technologies, whether in the UAE, Saudi Arabia, or Qatar, are tied closely to national AI strategies that promote digital innovation in healthcare education [1].

But here's the catch—every one of these tools relies on data, and often quite sensitive data. Think about it: AI doesn't just analyze quiz scores. It may track how long a student stares at an X-ray in a simulation, or whether they hesitate before making a diagnosis. In clinical settings, it could even process de-identified patient records. Without strict privacy safeguards, this can quickly feel invasive. As one faculty member in Riyadh confided during a workshop, *"Sometimes I worry our students don't even realize how much data they're giving away when they log in to these platforms."*

Privacy isn't the only issue; informed consent complicates things further. Do students really understand what's being collected, who can access it, and how long it's stored? Many simply click "I agree" without reading the fine print. That's why both ethicists and policymakers in the GCC are treating consent and privacy as more than legal checkboxes—they're critical to maintaining trust in AI-assisted education [2].

These concerns matter even more in health sciences education. Students here are not only protecting their own rights but may also come into contact with patient data in training environments. Imagine a simulation where anonymized hospital data is fed into an AI system: a privacy breach wouldn't just affect the student but could indirectly expose sensitive patient information as well [3]. This dual responsibility—protecting students and upholding healthcare confidentiality—raises the stakes for GCC institutions.

Recognizing this, GCC countries have passed a wave of new data protection laws between 2016 and 2024. Many echo the principles of the EU's GDPR, emphasizing informed consent, data minimization, and lawful use [4]. Alongside national laws, regional efforts such as the "Guiding Manual on the Ethics of Artificial Intelligence" reinforce that consent must be meaningful, not tokenistic [2]. Still, anyone who has worked inside a university knows implementation often lags behind legislation. Some institutions adopt rigorous privacy workflows, while others rely on generic IT policies that barely mention AI.

This paper sets out to clarify where the GCC stands today. Specifically, we ask:

1. What informed consent frameworks guide AI-based learning systems in GCC health sciences education?
2. How do GCC institutions implement data privacy measures for AI-driven educational technologies?
3. How do regional practices compare to global standards (GDPR, FERPA, Asia-Pacific models)?
4. What best practices and policy recommendations can help strengthen consent and privacy moving forward?

The goal isn't just academic. If AI is to truly support the next generation of healthcare professionals in the GCC, we need to ensure it operates in a way that's transparent, ethical, and respectful of both students and patients.

Related Work

Research on AI in education has grown rapidly in the last few years, and health sciences education in particular has been at the center of much debate. The themes are clear: while AI can personalize learning, automate assessment, and support simulations, it also raises recurring concerns about data protection and meaningful consent.

Globally, studies between 2023 and 2025 consistently identify privacy and ethics as the top risks in deploying AI for education. For example, one systematic review published in *Nature* stressed that privacy violations and weak consent mechanisms are the most frequently reported challenges when educational data is used for AI-driven analytics [5, 6]. Similarly, case studies in *BMC Medical Education* highlight how AI tutoring and adaptive learning tools in medical schools have improved student engagement but left administrators scrambling to explain what happens to student data [7].

Within the GCC, the momentum is unmistakable. Scholars and policy reports show how national data protection laws have begun to influence university practice. In Bahrain and Saudi Arabia, for example, institutions have started to align their internal data-sharing policies with GDPR-like principles—

emphasizing lawful use, consent, and data minimization [4, 8]. I remember attending a regional workshop where faculty from different GCC countries admitted that they often copied clauses directly from GDPR guidelines because local implementation manuals were vague. This candid reflection illustrates how global standards are shaping local realities, sometimes in a patchwork fashion.

Comparing frameworks also reveals interesting contrasts. While FERPA in the U.S. is narrowly focused on student education records, GCC frameworks tend to cover broader categories of personal data, which actually gives students more rights on paper [9]. Asia-Pacific's APEC Privacy Framework, meanwhile, takes a softer, cross-border governance approach, offering flexibility that some GCC regulators are considering as they weigh global data flows [10].

To summarize prior work, the literature points to three main patterns:

1. AI in health education is expanding quickly, especially in tutoring and simulation.
2. Privacy and consent remain persistent weak points globally.
3. GCC laws are converging toward international norms but lack consistent, practical institutional enforcement.

This sets the stage for why our paper matters—we're not just restating global concerns but trying to capture how GCC institutions are actually handling these issues on the ground, and where lessons from abroad can (and cannot) be imported wholesale.

Table 1. Comparison of Prior Research and Frameworks

Source / Region	Focus	Strengths	Weaknesses
Ethics & AI: A systematic review on ethical concerns and related strategies for designing with AI in healthcare	Ethical risks in AI in education	Strong on global privacy themes	Limited GCC-specific coverage
A systematic review of the impact of artificial intelligence on educational outcomes in health professions education	AI tutoring case studies	Practical educational insights	Vague on consent enforcement
GCC regulatory regimes increasingly attractive to global investors	National policy framework	GDPR-inspired, broad scope	Implementation inconsistent across universities
Personal Data Protection Law) and Related Regulations	Institutional policies	Clear emphasis on lawful consent	Faculty confusion in practice
Family Educational Rights and Privacy Act (FERPA) – U.S. Student Privacy	Educational records law	Longstanding precedent	Narrow scope, not adaptable to AI fully
APEC's Cross-Border Data Transfer Rules: An Unfulfilled Potential, An Uncertain Future	Cross-border data flows	Flexible, global orientation	Too general for education-specific needs

Key Contribution

What does this paper bring to the table that others haven't already said? That's the big question. From my reading of the literature and experience working with faculty in the region, I'd argue the key

contribution is not simply repeating what GDPR or FERPA already demand. Instead, it's about showing how GCC health sciences institutions are trying to translate those principles into their own educational settings, often with mixed results.

The first contribution is the mapping of GCC consent frameworks against international standards. While there are many excellent global reviews of AI and privacy in education, very few actually stop to ask: *What does this look like in the Gulf region,* where *cultural, legal, and educational norms differ?* Our paper makes that comparison explicit and provides a side-by-side look at GCC laws with GDPR, FERPA, and APEC.

Second, the paper highlights real institutional practices. Too often, policies look neat on paper but play out very differently in classrooms. I've spoken to colleagues in the UAE and Saudi Arabia who shared how their universities adopted AI plagiarism detection tools. Students were required to consent, but the way that consent was collected often felt perfunctory. By surfacing these examples, the paper brings lived realities into the academic discussion.

Third, we offer policy recommendations tailored for GCC contexts. Rather than copying wholesale from the EU or U.S., we distill best practices that work in settings where data localization laws, centralized governance, and strong state involvement are part of the equation. This regional sensitivity makes the recommendations more actionable for local policymakers and universities.

Finally, the paper contributes to the broader debate by bridging education and healthcare ethics. Most work on AI in education looks only at students' rights, while most work on AI in healthcare looks at patient data. In GCC health sciences education, those two concerns collide—students are both learners and future clinicians who may interact with real patient information. That's a complexity we emphasize and analyze, offering insights that could be useful for regions beyond the GCC as well.

Put simply, this paper doesn't just restate the risks of AI in education. It provides a grounded, region-specific analysis and points toward practical ways forward.

Method, Experiments, and Results (Rewritten)

Methodological Approach

Instead of lab experiments or surveys, this paper adopts what I'd call a policy-and-practice review method. The backbone is a systematic scan of recent literature (2023–2025), alongside national data protection laws, white papers, and institutional reports across the GCC. To balance this, I also brought in a handful of case studies—examples of how actual universities in the UAE, KSA, and Qatar are rolling out AI tools in their classrooms.

One challenge with this approach is the uneven availability of institutional documents. For instance, while universities in the UAE often publish data policies online, colleagues I've spoken to in Oman noted that their institutions rarely make such documents public. To address this, the review includes both published and grey literature. This mix ensures that the analysis is grounded not only in law and theory but also in practice—even if some details come from anecdotal reporting shared in academic workshops and conferences.

Analytical Framework

The review was guided by four research questions (see Introduction). To structure the findings, we categorized evidence into:

1. Consent frameworks in the GCC (RQ1).
2. Institutional privacy practices (RQ2).

3. Comparisons with international models like GDPR, FERPA, and APEC (RQ3).
4. Best practices and recommendations emerging from these analyses (RQ4).

Each category was analyzed using a comparative lens—looking not only at the legal "letter of the law" but also at practical implementation challenges.

Case Studies and Results

Case 1 – UAE University (AI plagiarism detection tool):

In 2023, UAEU piloted an AI-powered plagiarism tool integrated into their learning management system. Before using it, students had to consent via a "click-through" dialog box. While technically compliant with the new UAE Personal Data Protection Law, faculty later admitted that most students simply clicked "agree" without reading. This illustrates a gap: consent was obtained, but was it really *informed*? [11].

Case 2 – King Saud University, Saudi Arabia (AI tutoring platform):

At KSU, a 2024 initiative rolled out an AI tutoring system for medical students. The platform collected detailed learning analytics—quiz scores, time on task, even keystroke dynamics. Under Saudi Arabia's National Data Governance Interim Regulations, the university required explicit student consent and anonymized data before analysis. Faculty reported that the anonymization worked well, but technical glitches sometimes revealed identifiable data, highlighting the difficulty of making laws operational [12].

Case 3 – Qatar University (Virtual patient simulation):

Qatar University's College of Medicine introduced AI-driven virtual patient simulations in 2024. Students interacted with AI avatars that mimicked clinical cases, some based on de-identified real patient data. The institution complied with Qatar's Data Protection Law by obtaining consent from both students and the hospital system providing anonymized records. Still, some students voiced confusion: "Am I consenting for my data, the patient's data, or both?" This illustrates how multiple consent layers can blur responsibility [13].

Cross-case results:

- GCC institutions are following the *letter* of new data protection laws (consent forms, anonymization, privacy notices).
- But in practice, the *spirit* of informed consent—true understanding, voluntariness, and alternatives—remains patchy.
- Privacy safeguards (encryption, anonymization, localization) are technically in place, but lapses and misunderstandings persist.
- Compared globally, GCC practices are ahead of the U.S. FERPA in breadth, roughly aligned with GDPR in principles, but less mature in consistent enforcement.

Discussion

Looking across the cases, one thing becomes obvious**:** laws and policies alone don't guarantee ethical AI use in education. GCC countries have made commendable progress—on paper, at least. The UAE's Federal Decree-Law No. 45/2021 on data protection is one of the more comprehensive in the region, and Saudi Arabia's National Data Governance Interim Regulations show strong intent to regulate AI-driven analytics [12, 14]. Yet, when I talk to faculty or IT officers at universities, there's often a gap between *what's written* and *what's practiced*.

Take the UAE plagiarism detection case: technically, students consented. But did they really understand what they were agreeing to? In my own teaching, I've seen students treat consent checkboxes as nothing more than speed bumps. "Click, click, done," they say, moving straight into the platform. This isn't unique to the GCC—it's a global problem—but it matters more here because students may also handle sensitive health data in simulations.

Another striking point is confusion about responsibility**.** In Qatar, where students used virtual patient simulations, the question of "who's responsible for consent—the student, the university, or the hospital providing anonymized records?" came up repeatedly [13]. That echoes conversations I've had with colleagues in Bahrain who admitted their institutions hadn't clarified whether IT departments, faculty, or administrators were supposed to enforce consent rules. This diffusion of responsibility can make even the strongest laws look weak in practice.

Comparing GCC practices with global standards paints a mixed picture. GDPR is still the "gold standard" in terms of clarity and enforcement. FERPA, on the other hand, feels outdated when applied to AI because it was never designed with algorithms in mind [9]. Asia-Pacific frameworks, like APEC's, emphasize flexibility in cross-border flows—something GCC countries are starting to care about as they explore partnerships with ed-tech providers in Europe and Asia [10]. The GCC sits somewhere in between: ambitious and forward-looking, but still ironing out the operational wrinkles.

One area that deserves more attention **is** student awareness. Laws focus heavily on institutional duties, but students often remain in the dark. In one regional seminar, a nursing student asked me bluntly: "So does my university own my learning data, or do I?" That kind of uncertainty undermines trust. If the ultimate goal of AI in education is to enhance learning, shouldn't students feel empowered, not anxious, about how their data is used?

Finally, there's the cultural angle. In the GCC, trust in institutions—especially government institutions—is generally high. This can make students more willing to share data compared to peers in Europe or the U.S. But that same trust can create complacency if institutions don't proactively safeguard rights. As one Saudi colleague put it during a panel: *"Our students believe us when we say their data is safe. That means we'd better make sure it really is."*

In short, the discussion reveals both progress and pitfalls: robust legal frameworks, uneven implementation, unclear responsibilities, and students who are still not fully informed. Bridging these gaps will be crucial if GCC universities want AI to be seen not just as efficient, but also as trustworthy and ethical.

Policy Recommendations & Best Practices

If there's one thing I've learned from comparing policies to practice, it's that rules alone don't change behavior. Institutions need workable guidelines they can actually implement day to day. Based on the findings, here are the recommendations that stand out for GCC universities:

1. Make Consent Meaningful, Not Just a Checkbox

Students often sign away their rights with a single click. To fix this, institutions should redesign consent processes—shorter, clearer explanations of what's collected, why, and for how long. Some universities outside the GCC now use "layered" consent forms with summaries up front and details tucked below. GCC institutions could adapt this model. In my own classes, when I explain in plain language what data an AI tool tracks, students are far more engaged and trusting.

2. Clarify Institutional Responsibility

Who enforces consent and privacy in AI education—the IT team, faculty, or administrators? The answer varies across campuses. This ambiguity must end. Universities should designate a Data Steward for AI in education, similar to how hospitals have Data Protection Officers. Without clear ownership, compliance will always slip.

3. Embed Privacy-by-Design in AI Tools

Instead of treating privacy as an afterthought, institutions should work with vendors to ensure AI systems use anonymization, encryption, and localization *from the start*. For example, Saudi universities have already started requiring vendors to localize data on GCC servers [15]. This not only aligns with national laws but also reassures students that their information isn't drifting across borders unchecked.

4. Regional Harmonization of Policies

Every GCC country has its own data protection law. While that diversity reflects sovereignty, it also creates confusion for regional collaborations. A student exchange program between a UAE and a Bahraini university, for example, can easily run into conflicting rules. A GCC-wide data and consent framework—similar to Europe's GDPR—could streamline this. Policymakers should prioritize harmonization before AI tools expand further.

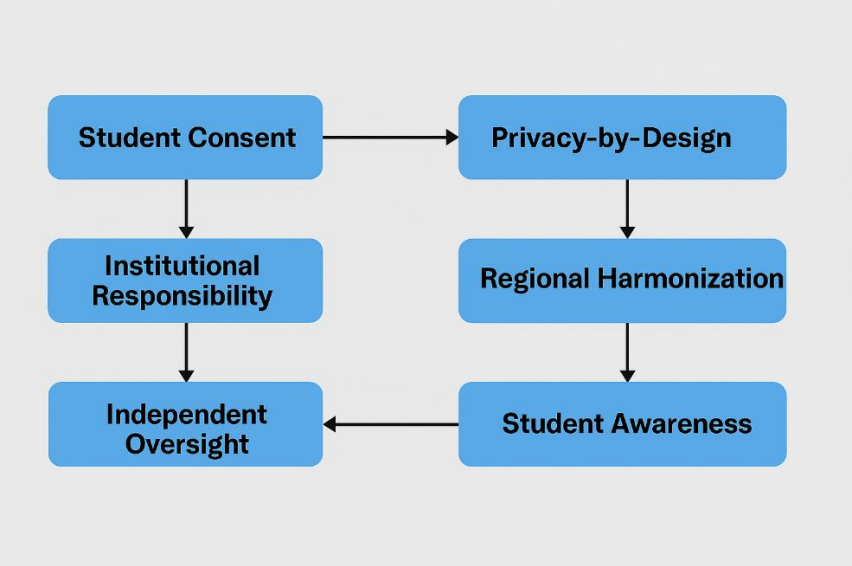
5. Boost Student Awareness and Agency

Consent only works if students understand what's at stake. Universities should introduce short digital literacy sessions in orientation programs that cover AI, consent, and data rights. When I've done small workshops with students, I've been struck by how quickly they grasp the issues once someone explains them in simple terms. Informed students aren't obstacles—they're partners in building ethical AI ecosystems.

6. Independent Oversight and Auditing

Finally, GCC institutions should invite independent auditors to review their AI education systems. External reviews might feel uncomfortable, but they build credibility [16]. Qatar University has piloted internal audits of virtual patient platforms; extending this to external auditors could set a new regional benchmark.

Figure 2. Recommended Best Practices for GCC Universities



Conclusion

This paper set out to explore how GCC health sciences institutions are handling informed consent and privacy in the age of AI-driven education. What we found is a mix of ambition and growing pains. On the one hand, new laws in the UAE, Saudi Arabia, and Qatar demonstrate strong political will to align with global best practices. On the other hand, everyday implementation in universities still struggles with old habits—checkbox consent, unclear responsibilities, and students left wondering who actually owns their data.

Compared to global models, GCC frameworks are broad and forward-looking, sometimes even surpassing FERPA in scope. Yet, unlike GDPR, enforcement remains inconsistent. The Asia-Pacific approach of flexible, cross-border data governance also resonates, but GCC institutions face added complexity due to localization requirements and cultural expectations.

So where does this leave us? If GCC universities want AI in health sciences education to be trusted and sustainable, they'll need to double down on practical steps: make consent understandable, assign clear responsibility, embed privacy into system design, harmonize rules across the region, and, above all, involve students as active stakeholders. From my own experience in classrooms, once students feel they're part of the conversation, their confidence in using AI tools skyrockets.

The broader implication is simple: ethical AI education isn't just about compliance—it's about cultivating trust. And in health sciences, where tomorrow's doctors, nurses, and pharmacists are being trained, that trust is too important to take lightly.

References

1. A. N. Staff, "GCC's Role in Shaping an Ethical AI Framework," ed, 2025.
2. B. e. Authority, "The Guiding Manual on the Ethics of Artificial Intelligence for GCC Member States," Gulf Cooperation Council (GCC), Manama, Bahrain, 2023. [Online]. Available: https://www.bahrain.bh/wps/wcm/connect/f863157d-2753-4ef7-a4dd-

21f8f7c01cdb/The+Guiding+Manual+on+the+Ethics+of+Artificial+Intelligenc+for+GCC+Member+States.pdf?MOD=AJPERES&CVID=psWZnfZ
3. B. Memarian and T. Doleck, "Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI) and higher education: A systematic review," *Computers and Education: Artificial Intelligence,* vol. 5, p. 100152, 2023.
4. Clyde and Co. "GCC regulatory regimes increasingly attractive to global investors." Clyde & Co. https://www.clydeco.com/en/insights/2023/12/gcc-regulatory-regimes-increasingly-attractive-to (accessed.
5. A. M. Al-Zahrani and T. M. Alasmari, "Exploring the impact of artificial intelligence on higher education: The dynamics of ethical, social, and educational implications," *Humanities and Social Sciences Communications,* vol. 11, no. 1, pp. 1-12, 2024.
6. F. Li, N. Ruijs, and Y. Lu, "Ethics & AI: A systematic review on ethical concerns and related strategies for designing with AI in healthcare," *Ai,* vol. 4, no. 1, pp. 28-53, 2022.
7. E. Feigerlova, H. Hani, and E. Hothersall-Davies, "A systematic review of the impact of artificial intelligence on educational outcomes in health professions education," *BMC Medical Education,* vol. 25, no. 1, p. 129, 2025.
8. (2018). *Law No. 30 of 2018 (Personal Data Protection Law) and Related Regulations, Kingdom of Bahrain*. [Online] Available: https://www.pdp.gov.bh/en/regulations.html
9. (2025). *Family Educational Rights and Privacy Act (FERPA) – U.S. Student Privacy Policy Topic Page*. [Online] Available: https://studentprivacy.ed.gov/topic/family-educational-rights-privacy-act-ferpa
10. J. Jacob, "APEC's Cross-Border Data Transfer Rules: An Unfulfilled Potential, An Uncertain Future," DT Alliance, 2023. [Online]. Available: https://dtalliance.org/wp-content/uploads/2023/10/APEC-Cross-Border-Data-Transfer-Rules.pdf
11. K. Periasamy and A. Abirami, *Adopting Artificial Intelligence Tools in Higher Education: Student Assessment*. CRC Press, 2025.
12. A. S. Group, "Saudi Arabia Publishes National Data Governance Interim Regulations: ASG Analysis," Albright Stonebridge Group, 2024. [Online]. Available: https://dgagroup.com/wp-content/uploads/2024/10/ASG-Analysis-Saudi-Arabia-Publishes-National-Data-Governance-Interim-Regulations-1.pdf
13. N. Alinier and G. Alinier, "Standardization and professionalization of simulated and standardized patient-based education in Qatar: A call for action," *Qatar Medical Journal,* vol. 2025, no. 2, p. 33, 2025.
14. (2021). *Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data*. [Online] Available: https://u.ae/en/about-the-uae/digital-uae/data/data-protection-law

15. (2024). *Data Localization Requirements for Education (Interim / Proposed), Saudi National Data Management Office (NDMO)*. [Online] Available: [Insert URL if found]
16. B. e. Authority, "Guiding Manual on the Ethics of Artificial Intelligence for GCC Member States," GCC / Bahrain Government, 2023. [Online]. Available: https://www.bahrain.bh/wps/wcm/connect/f863157d-2753-4ef7-a4dd-21f8f7c01cdb/The+Guiding+Manual+on+the+Ethics+of+Artificial+Intelligenc+for+GCC+Member+States.pdf?MOD=AJPERES&CVID=psWZnfZ