

Artificial Intelligence Implementation and Governance in Healthcare: A Qualitative Study of Cybersecurity Professionals

T'Oluwani E. Adekunle

toluwani.adekunle@calvin.edu

Calvin University

Joseph Ohaeche²

Corewell Health

Tiwaladeoluwa B. Adekunle³

University of Wisconsin–Madison

Deborah Adekunle⁴

Washington University in St. Louis

Kulwinder Dhaliwal

Rutgers New Jersey Medical School

Michel Kogbe⁶

Calvin University

Research Article

Keywords: Artificial intelligence, Cybersecurity, Health information governance, Sociotechnical systems, Organizational readiness

Posted Date: October 14th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11012612/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Artificial Intelligence Implementation and Governance in Healthcare: A Qualitative Study of Cybersecurity Professionals

T'Oluwani E. Adekunle, PhD, MPH, MBA, MA¹; Joseph Ohaeche²; Tiwaladeoluwa B. Adekunle³; Deborah Adekunle⁴; Kulwinder Dhaliwal, MD, MPH⁵; Michel Kogbe⁶

¹ Social Work, Calvin University, Grand Rapids, Michigan, USA

² Digital Services, Corewell Health, Grand Rapids, Michigan, USA

³ Division of Reproductive and Population Health, Department of Obstetrics and Gynecology, University of Wisconsin School of Medicine and Public Health, Madison, Wisconsin, USA

⁴ Division of Gastroenterology, Washington University in St. Louis, St. Louis, Missouri, USA

⁵ Department of Pediatrics, Division of Population Health, Quality and Implementation Sciences, Rutgers Robert Wood Johnson Medical School, New Jersey, USA

⁶ Undergraduate Division, Calvin University, Grand Rapids, Michigan, USA

Corresponding author: T'Oluwani E. Adekunle, toluwani.adekunle@calvin.edu

Abstract

Background: Artificial intelligence is increasingly integrated into healthcare systems, yet limited evidence describes how organizational conditions support its safe implementation and governance. This study examined cybersecurity professionals' perspectives on organizational processes shaping artificial intelligence implementation and oversight in healthcare settings.

Methods: We conducted semi-structured interviews with 20 cybersecurity professionals working in roles connected to healthcare systems, artificial intelligence, data infrastructure, or digital security. Interviews were conducted by videoconference between May and August 2025, lasted 45 to 60 minutes, and were audio-recorded and transcribed verbatim. Two researchers independently coded transcripts in Dedoose using qualitative content analysis and resolved coding differences through discussion.

Results: Five interconnected domains shaped participants' accounts: organizational readiness for artificial intelligence adoption, training and knowledge translation, continuous monitoring and

governance, resource constraints, and operational safety strategies. Participants described a tension between the pace of technology adoption and the slower development of governance capacity. Resource differences between organizations influenced access to cybersecurity personnel, training, monitoring, and internal control over artificial intelligence systems.

Conclusions: From cybersecurity professionals' perspectives, safe artificial intelligence implementation depends on organizational capacity to integrate governance into routine operations. Early cybersecurity involvement, sustained workforce learning, defined oversight processes, and governance expectations calibrated to organizational resources may support safer and more equitable implementation across healthcare settings.

Keywords: Artificial intelligence; Cybersecurity; Health information governance; Sociotechnical systems; Organizational readiness

Background

Artificial intelligence, ranging from predictive clinical algorithms to generative large language models (LLMs), is increasingly being used in healthcare settings to support how care is delivered and how information is managed [1],[2]. Hospitals and clinics are increasingly adopting artificial intelligence to support clinical decision-making and improve care delivery [3]. These technologies operate within complex digital systems that manage sensitive patient data and clinical workflows [4]. As adoption increases, concerns about system safety and oversight are intensifying [5]. Healthcare organizations must integrate new technologies into existing systems while safeguarding patient information and care quality [6].

The organizational environment shapes how artificial intelligence functions in practice and how it is experienced by users [7]. Implementation occurs within institutional conditions that shape how technologies are introduced and sustained over time [8]. Leadership priorities determine whether AI adoption is a coordinated effort or results in "Shadow AI" - the unsanctioned use of AI tools by clinical staff without formal IT or security oversight [9]. Staff understanding influences how systems are used in everyday work [10]. Organizational capacity determines whether risks

can be identified and addressed as technologies evolve [7]. Governance practices shape expectations for oversight and accountability [11]. These factors position the implementation of artificial intelligence as an organizational process grounded in real-world healthcare operations [12].

Cybersecurity professionals play a central role in this process by protecting health information systems and managing technological risk [6]. Artificial intelligence expands the organizational attack surface, introducing novel vulnerabilities such as adversarial data poisoning and algorithmic bias, which necessitates the integration of cybersecurity expertise [13],[14].

Professionals who safeguard digital environments often play a key role in how systems are introduced and managed [6],[13]. Their perspectives offer insight into how healthcare organizations manage artificial intelligence in routine practice.

This study is guided by a sociotechnical organizational framework that conceptualizes artificial intelligence implementation as shaped by three interacting domains: organizational context, cybersecurity expertise, and governance processes [7],[15],[16]. Organizational context refers to the institutional conditions within healthcare systems that influence how technologies are introduced and sustained [10],[16]. Cybersecurity expertise represents professional knowledge that informs how risks are interpreted and managed during implementation [6],[14]. Governance processes reflect the organizational mechanisms through which artificial intelligence is monitored and maintained over time [16]. The framework posits a bidirectional relationship where organizational context shapes the engagement of cybersecurity expertise. Cybersecurity expertise then influences governance processes that determine how artificial intelligence functions in routine healthcare operations. This conceptualization frames health AI implementation as an organizational process. It supports examination of factors that influence their safe and sustainable adoption. This is consistent with sociotechnical research showing that organizational conditions shape expertise engagement and governance [8],[15]. Figure 1 provides a visual representation of the conceptual framework for this study.

This study examines cybersecurity professionals' perspectives on organizational processes shaping artificial intelligence implementation and governance in healthcare. The research explores how participants understand the institutional conditions that shape integration and oversight. By focusing on organizational experience, the study provides empirical insight to support safe and sustainable artificial intelligence implementation.

Figure 1. Sociotechnical framework for health artificial intelligence implementation in healthcare organizations

Methods

Study design

This qualitative descriptive study used semi-structured in-depth interviews to examine how cybersecurity professionals describe organizational processes shaping artificial intelligence implementation and governance in healthcare systems. The sociotechnical organizational framework informed the study aim and interview topics while inductive coding allowed categories to be developed from participants' accounts [7, 15-17].

Research team and reflexivity

Interviews were conducted by the principal investigator (TEA), a female public health researcher trained in qualitative health research and experienced in studying health systems and organizational processes. The analytic team included a cybersecurity professional with experience in healthcare technology environments. No researcher had a prior relationship with participants. The interviewer maintained reflexive memos throughout data collection and analysis to examine how disciplinary assumptions and professional perspectives shaped questioning and interpretation.

Participants and recruitment

Eligible participants were cybersecurity professionals working in roles connected to healthcare systems, artificial intelligence, data infrastructure, or digital security. Participants were recruited through professional networks, LinkedIn outreach, and snowball sampling to reach specialized

professionals who may not be accessible through healthcare-based recruitment channels.

Recruitment was purposive and non-random. The sample was intended to capture cybersecurity perspectives relevant to healthcare technology; direct participation in a healthcare artificial intelligence deployment or governance committee was not required. Recruitment and preliminary analysis proceeded concurrently. Interviews continued until 20 participants had been interviewed and further interviews were no longer adding substantively new categories relevant to the focused study aim. This stopping decision reflected thematic sufficiency and information power, not a claim of universal saturation [23, 24].

Ethics approval and consent to participate

The study was conducted in accordance with the ethical principles of the Declaration of Helsinki. The study was approved by the Calvin University Institutional Review Board (IRB #25-002). All participants provided written informed consent before participation.

Data collection

Data were collected between May and August 2025 using secure videoconferencing. Interviews lasted approximately 45 to 60 minutes and were audio-recorded with permission, transcribed verbatim, and de-identified. The semi-structured guide elicited participants' current cybersecurity roles, years and areas of experience, healthcare work or consulting experience, perceptions of artificial intelligence in healthcare, data protection and trust, ethical and equity concerns, moral or faith-informed perspectives, and recommendations for secure implementation. The interviewer used follow-up probes to elicit examples and clarify how these processes operated in healthcare environments. Field notes were completed after each interview. The interview guide is provided as Additional file 1.

Participants also completed a brief demographic questionnaire. Variables included age, race or ethnicity, education, geographic location, household income, and cybersecurity domain.

Demographic data were used descriptively and were not linked to quotations.

Data analysis

Data were analyzed using inductive qualitative content analysis [18, 19]. Both coders first read transcripts in full to become familiar with the dataset. They independently applied descriptive codes to relevant excerpts and used constant comparison to examine similarities and differences across interviews [20]. Dedoose version 10.0.35 was used to store de-identified transcripts, apply and retrieve codes, compare coding, and organize analytic memos [21]. Coding differences were discussed until agreement was reached. Related codes were grouped into higher-order categories and then refined into domains that explained recurring organizational processes [22]. The sociotechnical framework was used during interpretation to examine relationships among organizational context, cybersecurity expertise, and governance; it did not supply a predetermined coding tree. Reflexive and analytic memos and an audit trail documented coding decisions, category revisions, and the development of the final domains.

Rigor

Credibility was supported through independent coding, interdisciplinary analytic discussion, constant comparison, reflexive memoing, and maintenance of an audit trail. The team examined variation within categories, including accounts of organizations with established monitoring processes and those in which governance followed technology adoption. Quotations were selected to demonstrate the range and basis of each interpretation. Transferability was supported through reporting participant characteristics and recruitment context.

Results

Twenty participants completed interviews. Most were 25 to 34 years old (65%), and 80% identified as Black or African American. Seventy-five percent held a master's or professional degree, 55% lived in urban settings, and 45% reported household incomes of at least \$100,000. Participants represented network and infrastructure security, offensive and defensive security, health informatics, data science and analytics, cloud and application security, artificial intelligence and machine learning, data-center engineering, and generalist cybersecurity roles. Table 1 presents participant characteristics. Years of cybersecurity experience, institution type,

and direct involvement in healthcare artificial intelligence implementation were not collected systematically.

Table 1. Participant demographic and professional characteristics

Characteristic	Category	n (%)
Age	25-34	13 (65.0)
	35-44	5 (25.0)
	45-54	2 (10.0)
Race or ethnicity	Black or African American	16 (80.0)
	Asian	2 (10.0)
	White	1 (5.0)
	Other	1 (5.0)
Education	Master's or professional degree	15 (75.0)
	Four-year degree	4 (20.0)
	Doctorate	1 (5.0)
Geographic residence	Urban	11 (55.0)
	Suburban	9 (45.0)
Household income	\$100,000 or more	9 (45.0)
	\$75,000-\$99,999	1 (5.0)
	\$50,000-\$74,999	5 (25.0)

Characteristic	Category	n (%)
	\$25,000-\$49,999	3 (15.0)
	Less than \$25,000	1 (5.0)
	Prefer not to say	1 (5.0)
Cybersecurity domain	Network and infrastructure security	4 (20.0)
	Offensive and defensive security	4 (20.0)
	Health informatics	4 (20.0)
	Data science and analytics	3 (15.0)
	Cloud and application security	2 (10.0)
	Generalist	1 (5.0)
	Artificial intelligence and machine learning	1 (5.0)
	Data-center engineering	1 (5.0)

160 Analysis identified five interconnected organizational domains: readiness for artificial intelligence
161 adoption, training and knowledge translation, continuous monitoring and governance, resource
162 constraints, and operational safety strategies. Across these domains, participants described a
163 recurring tension between rapid technology adoption and the slower development of
164 organizational capacity to govern it.

165 Organizational readiness emerged as a key factor shaping how artificial intelligence is adopted
166 in healthcare settings

167 Participants consistently described healthcare organizations as variably prepared for AI
168 integration, with readiness shaped by existing infrastructure, leadership engagement, and data
169 management practices. One participant reflected on baseline preparedness:
170 “I think some organizations are ready in terms of having the systems in place, but a lot of them
171 are still trying to figure it out. They might have the tools, but they don’t necessarily have the
172 structure for how everything connects together.” (Participant #006)
173 Others emphasized that AI adoption often outpaces organizational planning. They noted that
174 security and governance considerations are frequently addressed only after systems are
175 already in use, creating avoidable vulnerabilities.
176 “A lot of times they bring in the technology first, and then later they start asking questions about
177 security and governance. It’s backwards. You’re supposed to build that foundation before you
178 start using these systems.” (Participant #014)
179 Several participants highlighted gaps in data infrastructure. They emphasized that fragmented
180 systems and dispersed data environments complicate governance and increase vulnerability
181 when AI is layered onto existing platforms. As one participant explained:
182 “Most hospitals have data everywhere. Different departments, different platforms, different
183 vendors. So, when AI comes in, it’s just added on top of all that. There isn’t always a centralized
184 way of managing it.” (Participant #009)
185 Preparedness was also linked to leadership priorities. Participants emphasized that decisions
186 about data integration, governance, and security reflect whether institutional leadership treats AI
187 as a strategic responsibility or a technical add on. According to one participant: “If leadership
188 doesn’t see cybersecurity as part of operations, then AI just becomes another project instead of
189 something that needs long term planning.” (Participant #018)
190 Participants noted that readiness extends beyond technology to organizational culture. They
191 emphasized that staff understanding, engagement, and shared expectations shape whether AI-
192 related processes are followed in practice.

193 “Some places are open to change and some are not. That really affects how AI gets
194 implemented, because if people don’t understand why it matters, they don’t follow the
195 processes.” (Participant #010)

196 Together, these accounts show readiness as an alignment problem. Technical infrastructure,
197 leadership priorities, and staff expectations had to develop together. When adoption preceded
198 that alignment, cybersecurity and governance became corrective activities after deployment.
199 Training and knowledge translation infrastructures were essential to safe AI use in healthcare
200 Participants consistently emphasized that implementing AI safely requires sustained efforts to
201 translate cybersecurity expertise into everyday organizational practice. Training was described
202 as continuous, relational, and adaptive rather than episodic. One participant explained:
203 “Oh, that, yeah, that’ll be sharing their experience, expertise and knowledge. You know, the
204 professionals are to share their experts and knowledge to people around... the more you share
205 their knowledge around, the more knowledge understanding about the structure that we have in
206 our environment. You could have seminars and outreaches also to help people. If the idea is
207 just to disseminate this idea as much as we can. This can also include community involvement,
208 volunteering, the likes. I think that’s it.” (Participant #015)

209 Another emphasized the need for repetition and reinforcement. They noted that one-time
210 training is insufficient for sustaining understanding and adherence as AI systems and
211 associated risks continue to evolve. As a participant mentioned,
212 “Yeah, that would be training and retraining. You cannot just do it once and expect people to
213 remember everything. Things change, systems change, and threats change, so you have to
214 keep coming back to it.” (Participant #015)

215 Several described their role as actively translating technical concepts for clinicians and
216 administrators. They emphasized that effective AI use depends on shared understanding rather
217 than technical expertise alone.

218 “A big part of my job is explaining to staff what’s happening behind the scenes. They don’t need
219 all the technical details, but they need to understand how their actions affect security. If they
220 don’t understand that, then the systems don’t work the way they’re supposed to.” (Participant
221 #004)

222 Others highlighted the importance of accessibility in communication. They emphasized that
223 security and AI guidance must be conveyed in ways that align with clinical workflows and time
224 constraints. As one participant explained:

225 “You have to break it down in simple terms. Doctors and nurses are busy. If you make it
226 complicated, they tune out. So we try to explain things in a way that makes sense to their day-
227 to-day work.” (Participant #012)

228 Training was also described as occurring through informal channels. Participants emphasized
229 peer-to-peer learning and everyday conversations as important sources of knowledge transfer:

230 “We do workshops, emails, short sessions, whatever works. Sometimes it’s just having
231 conversations in the hallway. It’s not always formal, but it still matters.” (Participant #019)

232 Participants framed education as foundational to safe AI use. They emphasized its role in
233 supporting consistent and informed practice: “If people don’t understand how the systems work,
234 they won’t use them properly. And that creates risk. So training is really part of the
235 infrastructure.” (Participant #008)

236 These narratives position education as a translation mechanism between cybersecurity
237 requirements and clinical work. Formal instruction provided a common baseline, while repeated
238 and informal communication helped staff adapt guidance to changing systems and daily
239 workflows.

240 Continuous monitoring and governance workflows were described as essential to sustaining AI
241 safety over time

242 Participants consistently described AI implementation as requiring ongoing oversight through
243 structured monitoring and governance processes. Security was framed as iterative work
244 embedded within organizational routines. One participant stated:
245 “Security isn’t something you set up and walk away from. You have to keep checking, testing,
246 updating. AI just makes that more important because the systems are always changing.”
247 (Participant #012)

248 Another described formal evaluation practices as a routine part of organizational operations:
249 “We do regular assessments, penetration testing, vulnerability scans. It’s scheduled. It’s part of
250 operations. That’s how we catch problems early.” (Participant #007)

251 Participants emphasized learning from incidents. They described documentation and review as
252 essential for refining systems and preventing repeated failures. According to one participant:
253 “When something goes wrong, we document it, review it, and adjust the system. That’s how you
254 improve over time. You don’t just fix it and forget it.” (Participant #016)

255 Several highlighted the importance of clear escalation pathways. They emphasized that defined
256 roles and response timelines support timely and coordinated action when AI-related issues
257 arise. As one participant explained: “There has to be a process for escalation. Who gets
258 notified, who makes decisions, how fast you respond. That has to be clear before anything
259 happens.” (Participant #12)

260 Monitoring was directly linked to clinical continuity. Participants emphasized that early detection
261 of system issues helps prevent disruptions that could affect patient care:
262 “If a system goes down, patient care is affected. So we’re constantly watching for issues before
263 they become major problems. That’s just part of the job.” (Participant #003)

264 Participants also described governance as collaborative. They emphasized that shared
265 responsibility across security, compliance, IT, and clinical leadership supports coordinated
266 responses to AI-related issues. As one participant explained:

267 “It’s not just security watching things. Compliance is involved, IT is involved, sometimes clinical
268 leadership too. Everyone has a role when something comes up.” (Participant #018)

269 These accounts show that monitoring depended on routinized organizational relationships, not
270 surveillance tools alone. Scheduled testing, incident learning, escalation pathways, and cross-
271 departmental authority enabled organizations to detect problems and act on them before clinical
272 disruption intensified.

273 Resource constraints and institutional inequities shaped how AI safety was enacted across
274 healthcare settings

275 Participants described resource availability as a central factor shaping how AI governance is
276 implemented across healthcare settings, noting stark disparities between organizations. One
277 participant explained how institutional size and financial stability shape cybersecurity capacity.
278 They noted that this results in uneven levels of protection across healthcare settings. “Big
279 hospitals can afford security teams. Smaller clinics can’t. They’re just trying to keep the doors
280 open. So the level of protection ends up being very different.” (Participant #006)

281 Staffing limitations were frequently raised. Participants noted that insufficient personnel weaken
282 organizations’ ability to manage AI safely: “Sometimes there’s one IT person doing everything.
283 There’s no way they can manage AI security on top of everything else they already have to do.”
284 (Participant #011)

285 Budget constraints further restricted implementation. Participants emphasized that financial
286 limitations shape which security measures and training efforts organizations can realistically
287 sustain. As one participant explained: “Security tools cost money. Training costs money. Not
288 every organization has that kind of budget, even if they want to do things the right way.”
289 (Participant #017)

290 Participants also noted uneven access to technical expertise across healthcare settings. They
291 emphasized that reliance on external managed security service vendors can limit organizational
292 control over AI systems and constrain internal governance capacity. As one participant

293 explained: "Some places have specialists. Others rely completely on vendors. That changes
294 how much control they really have over their own systems." (Participant #020)

295 These disparities were described as translating directly into unequal levels of patient protection.
296 Participants emphasized that differences in expertise and oversight shape the degree of
297 security patients experience across care settings. "You end up with very different levels of
298 security depending on where people receive care. That's just the reality." (Participant #005)

299 Participants emphasized that such inequities shape organizational capacity to sustain AI
300 governance over time.

301 Practical strategies for operationalizing AI Safety

302 Participants described concrete practices used to reduce risk and support sustainable AI
303 integration. They emphasized anticipatory design and layered protections as foundational to AI
304 safety. One participant described foundational safeguards: "You start with data protection.
305 Encryption, access controls, separating identifiers. That's the base. If you don't get that right,
306 everything else becomes harder." (Participant #015)

307 Early involvement of cybersecurity teams was described as critical for shaping safer
308 implementation pathways. Participants emphasized that security considerations must inform
309 system design rather than be retrofitted after deployment. Another participant noted: "We try to
310 be part of the conversation from the beginning, not after the system is already live. That makes
311 a big difference." (Participant #014)

312 Participants also described designing systems with failure in mind. They framed resilience as a
313 planning principle rather than an exceptional response. As one participant put it: "You assume
314 something will eventually fail, so you design systems to limit the impact. That's just how you
315 have to think." (Participant #009)

316 Collaboration across organizational roles was viewed as essential for operationalizing AI safety.
317 Participants emphasized shared responsibility across departments. One participant described

this collaborative approach: “It’s not just IT. You need compliance, clinical leadership, administration. Everyone has a role in making sure things work.” (Participant #018)

Preparedness for disruption was described as a normal condition of healthcare technology environments. Participants framed planning for failure as an expected component of responsible AI governance. Another participant reflected: “You plan for downtime. You plan for breaches. That’s just reality in healthcare technology.” (Participant #003)

These accounts illustrate a pragmatic safety orientation centered on anticipation, containment, and recovery. Early cybersecurity involvement connected governance to system design, while layered protections and downtime planning treated failure as an operational possibility requiring advance preparation. These five interconnected organizational domains and their relationships are summarized in Figure 2.

Figure 2. Organizational processes shaping health artificial intelligence implementation and governance

Discussion

This study examined cybersecurity professionals’ perspectives on organizational processes shaping artificial intelligence implementation and governance in healthcare. Five interconnected domains described how readiness, workforce learning, monitoring, resources, and operational safeguards function together. The central contribution is an organizational capacity gradient: participants described how the same governance expectations can produce different levels of protection when healthcare organizations differ in staffing, expertise, infrastructure, and control over vendors. This finding extends sociotechnical accounts of implementation by showing how cybersecurity work connects organizational conditions to the routine enactment of governance [7-10, 15-17].

Organizational readiness emerged as a central condition shaping implementation. Participants described readiness as coordination among infrastructure, leadership, data management, and organizational culture. This finding is consistent with evidence that context and leadership

influence digital health adoption [9, 26, 44]. It also adds an important temporal tension: participants reported that artificial intelligence was sometimes introduced before security and governance structures were established. In these circumstances, cybersecurity work became reactive, limiting the organization's ability to shape system selection and design before deployment.

Training and knowledge translation were identified as mechanisms through which governance reached routine practice. Participants described cybersecurity professionals as translating technical requirements into language compatible with clinical workflows. This boundary-spanning function helps explain why written policies or one-time instruction may be insufficient. Safe use depended on repeated formal and informal communication that connected evolving threats with staff actions [30, 32, 33].

Continuous monitoring and governance were described as organizational learning processes. Testing, incident documentation, escalation, and cross-departmental review enabled institutions to revise practices as technologies and threats changed. This interpretation is consistent with health information governance and patient-safety research emphasizing continuous oversight and clear accountability [34-36]. The findings further indicate that monitoring has limited value when organizations lack authority, personnel, or workflows for responding to what monitoring reveals.

Resource constraints shaped whether governance expectations could be enacted. Participants contrasted organizations with specialized security teams and smaller settings in which one staff member managed multiple technology functions. Existing research documents uneven cybersecurity capacity across healthcare systems [13, 37-39]. The present findings connect this variation to equity in digital safety: patients may encounter different levels of protection depending on the resources and expertise available where they receive care.

Participants emphasized early cybersecurity involvement, layered safeguards, and planning for disruption. These practices align with responsible artificial intelligence and resilience

frameworks [40-43, 47, 48]. Their accounts suggest that multidisciplinary collaboration is most useful when cybersecurity professionals have influence before procurement and deployment, not only responsibility for responding after a problem occurs.

Implications

Healthcare organizations should assess cybersecurity staffing, data architecture, workforce learning, escalation authority, and vendor oversight before artificial intelligence deployment. Governance requirements should specify who can pause or modify a system when risks emerge and how lessons from incidents will alter practice. Policymakers and health-system leaders should also account for differences in institutional capacity. Uniform expectations without implementation support may widen differences between well-resourced organizations and smaller settings.

Cybersecurity professionals can contribute to institutional trust by connecting data protection commitments with observable organizational practices. Their early involvement may strengthen accountability for system selection, monitoring, and incident response. Trustworthy implementation therefore depends on sustained investment in the organizational conditions through which governance is carried out [43, 46, 47, 49].

Limitations

Several limitations warrant consideration. The study captured cybersecurity professionals' perspectives and did not include patients, clinicians, executives, vendors, or regulators. Recruitment through professional networks, LinkedIn, and snowball sampling was non-random, and the sample was demographically concentrated, with 80% identifying as Black or African American and 65% aged 25 to 34 years. Years of experience, institution type, country of employment, healthcare-specific responsibilities, and direct involvement in artificial intelligence implementation were not collected systematically. We therefore could not compare findings by professional experience or organizational setting, and participants' eligibility should not be interpreted as evidence that every participant had deployed an artificial intelligence system in a

healthcare organization. Demographic data were not linked to quotations, which also precluded subgroup analysis. The findings represent professional perspectives and may not transfer to all healthcare systems. The focused sample and interview depth supported thematic sufficiency for the study aim, but the study does not claim saturation across cybersecurity or healthcare contexts. Future research should compare governance processes across organizational types and include stakeholders directly involved in specific artificial intelligence implementations.

Conclusions

Cybersecurity professionals described safe artificial intelligence implementation as an organizational capacity issue. Governance became actionable when leadership, workforce learning, monitoring, resources, and operational safeguards were coordinated. Differences in staffing and expertise may create unequal capacity to protect patients across healthcare settings. Healthcare organizations should involve cybersecurity professionals early and build governance processes that can detect, interpret, and respond to risks throughout the technology lifecycle.

List of abbreviations

AI: Artificial intelligence

IRB: Institutional Review Board

LLM: Large language model

Declarations

Ethics approval and consent to participate

The study was conducted in accordance with the ethical principles of the Declaration of Helsinki. The Calvin University Institutional Review Board approved the study (IRB #25-002). All participants provided written informed consent before participation.

Consent for publication

Not applicable.

Availability of data and materials

422 The de-identified qualitative data generated and analyzed during the current study are not
423 publicly available because interview transcripts may contain contextual information that could
424 compromise participant confidentiality. Data may be available from the corresponding author on
425 reasonable request and subject to institutional approval and applicable ethical restrictions.

426 Competing interests

427 The authors declare that they have no competing interests.

428 Funding

429 This work was supported by the Blue Cross Blue Shield of Michigan Foundation (grant number
430 2025-09). The funder had no role in the study design, data collection, analysis, interpretation,
431 decision to submit, or preparation of the manuscript.

432 Authors' contributions

433 TEA conceptualized the study, developed the methodology, conducted the interviews,
434 contributed to analysis, acquired funding, and drafted the manuscript. MK contributed to
435 qualitative analysis. JO contributed cybersecurity subject-matter expertise and interpretation.
436 TBA, DA, and KD contributed to interpretation and critical revision of the manuscript. All authors
437 read and approved the final manuscript.

438 Acknowledgements

439 Not applicable.

440 Additional file

441 Additional file 1 (.docx): Semi-structured interview guide. Questions used to explore
442 cybersecurity professionals' roles and experience, perceptions of artificial intelligence in
443 healthcare, data security and trust, ethics and equity, moral or faith-informed perspectives, and
444 recommendations for secure implementation.

445 References

446 1. Wang F, Beecy A. Implementing AI models in clinical workflows: a roadmap. BMJ Evid Based
447 Med 2024:bmjebm-2023-112727. <https://doi.org/10.1136/bmjebm-2023-112727>.

448 2. Schwamm LH, Pletcher S, Erskine A. AI and Technology Enabled Clinical Workflow
449 Redesign. *Telemed Rep* 2024;5:415–20. <https://doi.org/10.1089/tmr.2024.0079>.

450 3. Maleki Varnosfaderani S, Forouzanfar M. The Role of AI in Hospitals and Clinics:
451 Transforming Healthcare in the 21st Century. *Bioengineering* 2024;11:337.
452 <https://doi.org/10.3390/bioengineering11040337>.

453 4. Fernandes Prabhu D, Gurupur V, Stone A, Trader E. Integrating Artificial Intelligence,
454 Electronic Health Records, and Wearables for Predictive, Patient-Centered Decision Support in
455 Healthcare. *Healthcare* 2025;13:2753. <https://doi.org/10.3390/healthcare13212753>.

456 5. Freeman S, Wang A, Saraf S, Potts E, McKimm A, Coiera E, et al. Developing an AI
457 Governance Framework for Safe and Responsible AI in Health Care Organizations: Protocol for
458 a Multimethod Study. *JMIR Res Protoc* 2025;14:e75702. <https://doi.org/10.2196/75702>.

459 6. Bodnari A, Travis J. Scaling enterprise AI in healthcare: the role of governance in risk
460 mitigation frameworks. *NPJ Digit Med* 2025;8:272. <https://doi.org/10.1038/s41746-025-01700-4>.

461 7. Singh H, Sittig DF. A Sociotechnical Framework for Safety-Related Electronic Health Record
462 Research Reporting: The SAFER Reporting Framework. *Ann Intern Med* 2020;172:S92–100.
463 <https://doi.org/10.7326/M19-0879>.

464 8. Greenhalgh T, Wherton J, Papoutsis C, Lynch J, Hughes G, A’Court C, et al. Beyond
465 Adoption: A New Framework for Theorizing and Evaluating Nonadoption, Abandonment, and
466 Challenges to the Scale-Up, Spread, and Sustainability of Health and Care Technologies. *J Med*
467 *Internet Res* 2017;19:e367. <https://doi.org/10.2196/jmir.8775>.

468 9. Nilsen P, Bernhardsson S. Context matters in implementation science: a scoping review of
469 determinant frameworks that describe contextual determinants for implementation outcomes.
470 *BMC Health Serv Res* 2019;19:189. <https://doi.org/10.1186/s12913-019-4015-3>.

471 10. Li J. A Sociotechnical Approach to Evaluating the Impact of ICT on Clinical Care
472 Environments. *Open Med Inform J* 2010;4:202–5.
473 <https://doi.org/10.2174/1874431101004010202>.

474 11. Saenz AD, McCoy T, Mantha AB, Martin R, Damiano R, Adair D, et al. Establishing
475 responsible use of AI guidelines: a comprehensive case study for healthcare institutions. NPJ
476 Digit Med 2024;7:348. <https://doi.org/10.1038/s41746-024-01300-8>.

477 12. Wenderott K, Krups J, Weigl M, Wooldridge AR. Facilitators and Barriers to Implementing AI
478 in Routine Medical Imaging: Systematic Review and Qualitative Analysis. J Med Internet Res
479 2025;27:e63649. <https://doi.org/10.2196/63649>.

480 13. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective.
481 J Med Internet Res 2018;20:e10059. <https://doi.org/10.2196/10059>.

482 14. Di Palma G, Scendoni R, Ferorelli D, De Benedictis A, Tambone V, De Micco F. AI-Induced
483 Cybersecurity Risks in Healthcare: A Narrative Review of Blockchain-Based Solutions Within a
484 Clinical Risk Management Framework. Risk Manag Healthc Policy 2025;Volume 18:3479–97.
485 <https://doi.org/10.2147/RMHP.S544523>.

486 15. Salwei ME, Carayon P. A Sociotechnical Systems Framework for the Application of Artificial
487 Intelligence in Health Care Delivery. J Cogn Eng Decis Mak 2022;16:194–206.
488 <https://doi.org/10.1177/15553434221097357>.

489 16. Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in
490 health care. Journal of the American Medical Informatics Association 2020;27:491–7.
491 <https://doi.org/10.1093/jamia/ocz192>.

492 17. Carayon P, Salwei ME. Moving toward a sociotechnical systems approach to continuous
493 health information technology design: the path forward for improving electronic health record
494 usability and reducing clinician burnout. Journal of the American Medical Informatics
495 Association 2021;28:1026–8. <https://doi.org/10.1093/jamia/ocab002>.

496 18. Hsieh H-F, Shannon SE. Three Approaches to Qualitative Content Analysis. Qual Health
497 Res 2005;15:1277–88. <https://doi.org/10.1177/1049732305276687>.

498 19. Elo S, Kääriäinen M, Kanste O, Pölkki T, Utriainen K, Kyngäs H. Qualitative Content
499 Analysis. Sage Open 2014;4. <https://doi.org/10.1177/2158244014522633>.

500 20. Glaser BG, Strauss AL. Discovery of grounded theory: Strategies for qualitative research.
501 2017. <https://doi.org/10.4324/9780203793206>.

502 21. Dedoose Version 10.0.35. Cloud application for managing, analyzing, and presenting
503 qualitative and mixed method research data 2023.

504 22. Saldana J. The Coding Manual for Qualitative Researchers. 2025.
505 <https://doi.org/10.4135/9781036235611>.

506 23. Saunders B, Sim J, Kingstone T, Baker S, Waterfield J, Bartlam B, et al. Saturation in
507 qualitative research: exploring its conceptualization and operationalization. Qual Quant
508 2018;52:1893–907. <https://doi.org/10.1007/s11135-017-0574-8>.

509 24. LaDonna KA, Artino AR, Balmer DF. Beyond the Guise of Saturation: Rigor and Qualitative
510 Interview Data. J Grad Med Educ 2021;13:607–11. <https://doi.org/10.4300/JGME-D-21-00752.1>.

511 25. Lo B, Durocher K, Charow R, Kimball S, Pham Q, Sockalingam S, et al. Application of a
512 Sociotechnical Framework to Uncover Factors That Influence Effective User Engagement With
513 Digital Mental Health Tools in Clinical Care Contexts: Scoping Review. J Med Internet Res
514 2025;27:e67820. <https://doi.org/10.2196/67820>.

515 26. Li Q, Li P, Hao H, Padman R, Gao H, Travis Gossey J, et al. The impact of leadership on AI
516 deployment study outcomes in healthcare: an integrative analysis. NPJ Digit Med 2025;8:799.
517 <https://doi.org/10.1038/s41746-025-02177-x>.

518 27. Sendak M, Gao M, Nichols M, Lin A, Balu S. Machine Learning in Health Care: A Critical
519 Appraisal of Challenges and Opportunities. EGEMs (Generating Evidence & Methods to
520 Improve Patient Outcomes) 2019;7:1. <https://doi.org/10.5334/egems.287>.

521 28. Torab-Miandoab A, Samad-Soltani T, Jodati A, Rezaei-Hachesu P. Interoperability of
522 heterogeneous health information systems: a systematic literature review. BMC Med Inform
523 Decis Mak 2023;23:18. <https://doi.org/10.1186/s12911-023-02115-5>.

524 29. Anian S, Mahmud A, Abd Rahman A, Kharie MF, Omar M. A multi-country review of the
525 governance of hospital information systems interoperability. *Eastern Mediterranean Health*
526 *Journal* 2025;31:581–9. <https://doi.org/10.26719/2025.31.10.581>.

527 30. Birkeli G, Lindahl AK, Hammersbøen ÅM, Deilkås ECT, Ballangrud R. Strategies and tools
528 to learn from work that goes well within healthcare patient safety practices: a mixed methods
529 systematic review. *BMC Health Serv Res* 2025;25:538. [https://doi.org/10.1186/s12913-025-](https://doi.org/10.1186/s12913-025-12680-2)
530 12680-2.

531 31. Carayon P, Wooldridge A, Hoonakker P, Hundt AS, Kelly MM. SEIPS 3.0: Human-centered
532 design of the patient journey for patient safety. *Appl Ergon* 2020;84:103033.
533 <https://doi.org/10.1016/j.apergo.2019.103033>.

534 32. Birken S, Clary A, Tabriz AA, Turner K, Meza R, Zizzi A, et al. Middle managers' role in
535 implementing evidence-based practices in healthcare: a systematic review. *Implementation*
536 *Science* 2018;13:149. <https://doi.org/10.1186/s13012-018-0843-5>.

537 33. Montgomery A, Lainidi O, Georganta K. Why Talking Is Not Cheap: Adverse Events and
538 Informal Communication. *Healthcare* 2024;12:635. <https://doi.org/10.3390/healthcare12060635>.

539 34. Ghaffari Heshajin S, Sedghi S, Panahi S, Takian A. A framework for health information
540 governance: a scoping review. *Health Res Policy Syst* 2024;22:109.
541 <https://doi.org/10.1186/s12961-024-01193-9>.

542 35. Alizadeh-Dizaj G, Damanabi S, Hejazi ME, Raoofi S, Kalankesh LR. Implementation of
543 patient safety monitoring systems in hospitals: a systematic review. *BMJ Health Care Inform*
544 2025;32:e101392. <https://doi.org/10.1136/bmjhci-2024-101392>.

545 36. Labkoff S, Oladimeji B, Kannry J, Solomonides A, Leftwich R, Koski E, et al. Toward a
546 responsible future: recommendations for AI-enabled clinical decision support. *Journal of the*
547 *American Medical Informatics Association* 2024;31:2730–9.
548 <https://doi.org/10.1093/jamia/ocae209>.

37. Hasegawa K, O'Brien N, Prendergast M, Ajah CA, Neves AL, Ghafur S. Cybersecurity Interventions in Health Care Organizations in Low- and Middle-Income Countries: Scoping Review. *J Med Internet Res* 2024;26:e47311. <https://doi.org/10.2196/47311>.
38. Ikegwu AC, Alo UR, Nweke HF. Cyber threats in mobile healthcare applications: systematic review of enabling technologies, threat models, detection approaches, and future directions. *Discover Computing* 2025;28:152. <https://doi.org/10.1007/s10791-025-09686-z>.
39. Gellert GA, Borgasano D, Palermo R, Gellert GL, Kelly SP. Third-Party Access Cybersecurity Threats and Precautions: A Survey of Healthcare Delivery Organizations. *Appl Clin Inform* 2025;16:1518–30. <https://doi.org/10.1055/a-2713-5725>.
40. Papagiannidis E, Mikalef P, Conboy K. Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems* 2025;34:101885. <https://doi.org/10.1016/j.jsis.2024.101885>.
41. Lindgren H, Lindvall K, Richter-Sundberg L. Responsible design of an AI system for health behavior change—an ethics perspective on the participatory design process of the STAR-C digital coach. *Front Digit Health* 2025;7. <https://doi.org/10.3389/fdgth.2025.1436347>.
42. Zhu H, Huang F, Wang J, Huang L, Deng Q, Chen T, et al. A resilience assessment framework for healthcare systems considering water electricity and transportation system failures. *Journal of Safety Science and Resilience* 2026:100288. <https://doi.org/10.1016/j.jnlssr.2026.100288>.
43. Matheny ME, Goldsack JC, Saria S, Shah NH, Gerhart J, Cohen IG, et al. Artificial Intelligence In Health And Health Care: Priorities For Action. *Health Aff* 2025;44:163–70. <https://doi.org/10.1377/hlthaff.2024.01003>.
44. Boyacı H, Söyük S. Healthcare workers' readiness for artificial intelligence and organizational change: a quantitative study in a university hospital. *BMC Health Serv Res* 2025;25:813. <https://doi.org/10.1186/s12913-025-12846-y>.

- 574 45. Mistri IU, Badge A, Shahu S. Enhancing Patient Safety Culture in Hospitals. *Cureus* 2023.
575 <https://doi.org/10.7759/cureus.51159>.
- 576 46. Dankwa-Mullan I. Health Equity and Ethical Considerations in Using Artificial Intelligence in
577 Public Health and Medicine. *Prev Chronic Dis* 2024;21:240245.
578 <https://doi.org/10.5888/pcd21.240245>.
- 579 47. Wells BJ, Nguyen HM, McWilliams A, Pallini M, Bovi A, Kuzma A, et al. A practical
580 framework for appropriate implementation and review of artificial intelligence (FAIR-AI) in
581 healthcare. *NPJ Digit Med* 2025;8:514. <https://doi.org/10.1038/s41746-025-01900-y>.
- 582 48. Alharbi A, Alkhalifah A. Cybersecurity governance in the healthcare sector during digital
583 transformation: an integrated model and hybrid analytical approach. *Front Public Health*
584 2025;13. <https://doi.org/10.3389/fpubh.2025.1703689>.
- 585 49. Steerling E, Siira E, Nilsen P, Svedberg P, Nygren J. Implementing AI in healthcare—the
586 relevance of trust: a scoping review. *Frontiers in Health Services* 2023;3.
587 <https://doi.org/10.3389/frhs.2023.1211150>.

Organizational Context

Infrastructure Capacity, Leadership Priorities, Workflow Integration



Cybersecurity Expertise

Risk Interpretation, Safeguards, Decision Influence



Governance Processes

Monitoring, Accountability, Incident Response, Oversight Structures



AI Implementation Outcomes

System Reliability, Safe Use, Organizational Trust



Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [SemiStructuredInterviewGuide.docx](#)