PriMera Scientific
Medicine and Public Health
Volume 8 Issue 2 February 2026
ISSN: 2833-5627

Aligning Privacy and Device Oversight for Healthcare AI: A Governance Cross-Walk and Reform Options

Type: Review Article
Received: December 19, 2025
Published: January 29, 2026

Citation:
Valentina Palama. "Aligning Privacy and Device Oversight for Healthcare AI: A Governance Cross-Walk and Reform Options". PriMera Scientific Medicine and Public Health 8.2 (2026): 30-40.

Valentina Palama*

Department of Computer and Information System, Prairie View A &M University, USA

***Corresponding Author:** Valentina Palama, Department of Computer and Information System, Prairie View A &M University, USA.

Abstract

Background: The rapid use of software-based clinical tools in U.S. care settings has outpaced governance designed for static devices and siloed data. In practice, privacy obligations under HIPAA/HITECH and safety/effectiveness oversight by the FDA proceed in parallel rather than in sync, creating lifecycle gaps once tools are deployed and updated.

Methods: We conducted a structured, desk-based review of publicly available federal materials FDA device decisions, ONC certification resources, CMS coverage determinations and state statutes on medical devices and health data, supplemented by a targeted scoping review of peer-reviewed policy literature (2019-2025). No human-subjects data were collected.

Results: A cross-walk of these sources shows overlapping mandates with material gaps in post-deployment monitoring, data provenance, and change control. State privacy laws diverge on de-identification and secondary use, and payer policies vary in recognizing real-world performance evidence. These disconnects concentrate compliance burden on providers and vendors while offering limited clarity on ongoing risk management. We provide a governance cross-walk that maps HIPAA/HITECH requirements to FDA lifecycle stages and specifies practical artifacts (e.g., risk analysis, de-identification memorandum, audit-log procedures) to streamline reviews.

Conclusion: Fragmented privacy and device oversight creates operational, legal, and economic friction for health systems. Harmonized, risk-based oversight that pairs privacy and safety at each lifecycle stage supported by standardized impact assessments and minimum post-deployment monitoring can reduce duplication and support more equitable adoption without weakening patient protections.

Keywords: Health information privacy; medical device oversight; HIPAA; FDA; policy analysis; implementation barriers

Introduction

In 2019, health professionals predicted that AI would greatly change healthcare. This prediction was correct. Today, AI tools are transforming healthcare quickly. These tools analyze medical images, predict patient outcomes, and assist doctors in decision-making. Since 2018, more AI devices have been approved annually (Benjamens et al., 2020). These software tools are used in US healthcare faster than traditional rules for devices and records. In the US, privacy rules under HIPAA and device reviews by the FDA mostly operate separately. This separation causes issues when software is updated after use.

AI tools are now common in US hospitals and clinics. They help detect diseases early using X-rays, CT scans, and MRIs. They also forecast patient health risks and support planning for beds, staff, and medicine. These tools can save lives and reduce costs. However, the current laws do not keep pace with AI technology. This creates confusion and risks for patients and staff. Multiple government agencies oversee healthcare AI. However, their efforts often lack coordination. The main rules, HIPAA and FDA, mostly function separately and do not address AI-specific issues (Price & Gerke, 2020). HIPAA was created in 1996 to protect health information. It sets rules for data use and sharing. It also protects patient privacy when data is shared (Moore et al., 2019). AI needs large amounts of data to learn. It often updates and improves using new patient information after deployment (Zaidan & Ibrahim, 2024). This causes problems with HIPAA rules:

1. ***Data anonymization issues***. HIPAA allows some data sharing without identifying individuals. But AI needs detailed data for proper function. Removing too much information can hinder AI performance. Also, studies show that individuals can sometimes be re-identified in large data sets (Rocher et al., 2019).
2. ***Consent issues***. Many old consent forms do not mention AI training or testing. This makes it unclear whether using data for these purposes is allowed (Hurley et al., 2024).
3. ***Data use after deployment***. Unlike fixed devices, AI is regularly updated. HIPAA does not specify rules for ongoing data use for learning purposes (Hurley et al., 2024).

The FDA reviews whether AI tools used for diagnosis or treatment are safe and effective. Its rules were developed when medical devices were less adaptable (Hurley et al., 2024). Common approval paths include:

1. ***510(k) clearance***: for devices similar to existing ones.
2. ***De Novo classification***: for new devices with moderate or low risk without a specific comparison.
3. ***Premarket approval (PMA):*** for high-risk devices, the strictest review process.

AI and machine learning software can fit into these pathways in inconsistent ways. Using different approval routes for similar tools can cause confusion. Post-market monitoring of AI devices is also inconsistent. In practice, HIPAA and FDA rules overlap but are not well integrated. This leads to conflicting requirements, such as how to anonymize data while demonstrating safety. It also creates unclear authority over privacy and safety, as both HHS OCR and FDA have roles. This ambiguity can delay or discourage companies from releasing new AI tools.

Current research gaps remain. Many discussions focus on ideas rather than practical issues. Questions include: What problems do providers face when applying current rules? How do developers and clinicians see the rules fitting their work? Where do privacy, safety, and data sharing interfere in daily operations? How do costs and AI use differ for small clinics? Most studies examine individual rules without considering how they work together in real life (Gerke et al., 2020). Grounded evidence from practice is important. It helps create better rules that consider real clinical settings. We need to know what causes delays, who is responsible, and how to ensure safety while adopting new technology. This article summarizes existing information about common problems and possible solutions. It does not present new data but reviews public sources.

Our primary goal is to identify where US regulations on privacy, safety, and system integration do not match and hinder AI adoption. We then aim to develop clear policy recommendations to address these gaps.

Our secondary goal is to compare US policies with international, risk-based, step-by-step approaches. We look for similarities to find practices that could benefit US policies. Our method involves a desk review. Sections 2-4 describe what we did, what we found, and our policy suggestions. We analyzed public information from FDA, ONC, CMS, and state agencies, focusing on data from 2019-2025. We did not conduct interviews or involve external participants. Our goal was to examine the entire environment through publicly available sources to identify policy gaps that need fixing.

Materials and Methods

Study Design

This is a desk-based policy analysis. It doesn't include people or patient records. We looked at some public records from the FDA about medical devices. These include decisions and summaries for software-based devices like 510(k), De Novo, and PMA. We also checked guidance from the ONC about health IT standards for data exchange, transparency, and safety. Plus, we reviewed Medicare and Medicaid policies that affect services supported by software. Lastly, we looked at state laws about medical devices, data privacy, and how automated systems are held accountable.

Search and Selection

We looked at FDA and ONC websites. We searched by device type and simple keywords like "software used for diagnosis," "clinical decision support," and "software as a medical device." We also checked CMS NCDs and manuals. Plus, we looked at state legal rules about automated decision tools in healthcare. For background info, we did a search from 2019 to 2025 in PubMed, Scopus, and SSRN. We used words that combined health software with rules about safety, privacy, fairness, and post-market checks.

Synthesis Approach

We looked at different stages of the product before it hits the market, when it's being used, and after it's out there. We found issues, conflicts, and gaps. We put all this info into a table. This table shows where things are broken up and where following the rules is hard. We didn't do interviews, surveys, or talk to people for this.

Policy and Legal Framework Analysis

We reviewed U.S. rules about healthcare software. We looked at HIPAA privacy and security rules, FDA device rules, and big policy ideas. We used government guides, research articles, and policy reports. We checked where HIPAA data rules might clash or line up with FDA safety rules.

Data Analysis

Quantitative. We looked at basic stats to summarize FDA pathways and timelines like 510(k), De Novo, and PMA, plus any post-market checks.

Qualitative. We read reports, case summaries, and policy papers to find common issues, tips, and advice from stakeholders.

Integration. We put the summaries and themes together in charts to check our findings and make them clearer.

Ethical Considerations

This study only used publicly available documents. We didn't work with any human data or do any experiments. So, no need for review board approval.

Results

Findings from Public Sources

Public FDA records, ONC/CMS stuff, and state laws all show there are two main ways things are looked at. One is the federal privacy rules that deal with protected health info. The other is device review, which checks if devices are safe, work well, have proper labels, are secure from hacking, and if companies have to do follow-up work after they sell the device. Experts and government reports say these two systems don't really match up closely. This means there are delays and missing info during testing, rolling out, updates, and taking devices off the market. People also mention common problems like how to handle data minimization and anonymization, how to use data again or work with vendors, and how clear rules are around checking devices after they are used. Smaller groups with fewer staff also struggle more with these rules. Around the world, new risk-based systems are coming up. These combine privacy and safety rules into one schedule, which could be a good model for the U.S. to follow.

FDA regulatory pathways

Public FDA summaries from 2019-2024 show that most software tools for clinics get cleared through the 510(k) process. Fewer go through De Novo, and even fewer go through PMA. It takes less time for 510(k) and more for De Novo. PMA usually takes the longest. After they are on the market, companies have to keep an eye on how well they work. But this is not the same for all, so it varies.

HIPAA compliance challenges

Looking at public reports and policy reviews, we see common issues with privacy and data use. These include: (i) trying to remove identifiers without losing usefulness, (ii) questions about getting permission to use old data for new purposes, (iii) unclear rules from vendors about sharing data, and (iv) expectations about how open companies should be about their data and models. Of these, being transparent takes the most time because it needs teams from legal, compliance, and tech to work together.

How Compliance Affects Costs

Getting ready for rules and trade rules costs money. Smaller hospitals and clinics feel this more. They spend more on lawyers, changing contracts with vendors, fixing technical stuff, and training staff. Bigger hospitals, like universities, handle these costs more easily. Smaller places have less money for technology, so they spend more of it on staying compliant (Rebecca and Julie 1996)

Suggestions from Stakeholders

People involved in policy and research agree on some key points. First, they want a single system that connects privacy rules with device safety checks. Second, they want clear rules for tools that get updates after being used. Third, they want standard forms for privacy checks and contracts. Fourth, they need easy advice for big projects that involve many different hospitals working together(Scott et al., 2019).

Changes Over Time in Rules

Stories from 2019 to 2024 say that making rules got harder. There are more rules from different states and the federal government. They also expect updates to be ongoing, and the paperwork is more detailed. Hospitals say they have to deal with more points of compliance now than before(Markus et al., 2023).

International benchmarking

Brief comparisons with the European Union and Singapore suggest movement toward unified, risk-stratified governance abroad, while U.S. oversight remains split between privacy (HIPAA) and safety/effectiveness (FDA). This contrast highlights opportunities for U.S. policymakers to reduce fragmentation without sacrificing protections.

Lifecycle stage	*FDA focus*	*HIPAA/HITECH touch-points*	*Common friction points*	*Practical artifacts*
1) Planning & data strategy (pre-submission)	Intended use; risk category; user/population; human-factors plan	Lawful basis; minimum necessary; de-identification (Safe Harbor vs Expert Determination); BAAs; Security Rule risk analysis (45 CFR 164.308)	Re-use of historical records; multi-site data pooling; unclear vendor hosting	Data governance plan; de-identification memo; BAA template; risk analysis; role-based access matrix
2) Pre-market testing & validation	Verification/validation; clinical evaluation; software lifecycle docs; cybersecurity plan	Use of identifiable info; disclosures log; access controls; audit logs; separate operations vs research	Mixing QI with research; weak data provenance	Data provenance log; disclosures log; audit-log setup; privacy impact assessment (PIA)
3) Submission / clearance	Traceable evidence; labeling/IFU; known risks/mitigations; change control	Avoid identifiers in submissions; secure transfer to FDA; sub-processor BAAs	Third-party reports with traceable records; unclear vendor chain	De-identified evidence pack; secure transfer SOP; vendor inventory & BAAs
4) Deployment in a covered entity	Usability; implementation instructions; hardening; site readiness	Security Rule controls; BAAs; minimum necessary config; right of access & transparency	Vendor remote access; logs capturing identifiers; role creep	Access-control matrix; audit-log config SOP; DUA/BAA package; user training checklist; site privacy notice
5) Post-market monitoring & updates	Complaints; field corrections; safety reporting; change management	Ongoing uses/disclosures; breach notification; reassess de-identification; update BAAs if telemetry changes	Telemetry considered PHI; off-site monitoring storage; performance changes over time	Post-deployment monitoring plan; change-control SOP; breach playbook; retention schedule; transparency addendum
6) End-of-life / decommissioning	Retirement plan; device removed from service	Secure disposal (45 CFR 164.310(d)(2)); vendor delete certifications; revoke access	Stranded backups; lingering accounts; unclear ownership	Decommission checklist; certificate of destruction; account revocation log

Table 1: Privacy–Safety Governance Cross-Walk Across the Device Lifecycle.

Caption: Alignment of FDA reviewers' expectations with HIPAA/HITECH privacy and security checkpoints from planning through decommissioning. The table flags common friction points and lists practical artifacts (e.g., de-identification memo, access-control matrix, audit-log SOP) to streamline paired safety-privacy review.

Notes: This is a planning aid, not legal advice. Institutions should follow the HIPAA Security Rule for risk analysis and media disposal (e.g., 45 CFR 164.308; 45 CFR 164.310(d)(2)).

Abbreviations: BAA = Business Associate Agreement; DUA = Data Use Agreement; FDA = Food and Drug Administration; HIPAA = Health Insurance Portability and Accountability Act; HITECH = Health Information Technology for Economic and Clinical Health Act; IFU = Instructions for Use; PHI = Protected Health Information; PIA = Privacy Impact Assessment; SOP = Standard Operating Procedure.

Domain	*United States*	*European Union*
Primary privacy law	HIPAA (1996) – protects PHI; limited scope for modern software	GDPR (2018) – broad data rights; strong cross-border rules
Primary device oversight	FDA (510(k), De Novo, PMA pathways)	MDR (Medical Devices Regulation, 2021)
AI-specific regulation	No dedicated federal AI law; agency guidance applies	AI Act (risk-based approach)
Post-market surveillance	Defined for devices; variable for software	Mandatory for high-risk systems
Risk classification	Device-based; not AI-specific	Explicit tiers (minimal, limited, high, unacceptable)

Table 2: U.S.–EU Regulatory Landscape for Software-Enabled Clinical Tools.

Caption: Side-by-side comparison of core elements that shape governance: primary privacy law, device oversight regime, presence of AI-specific statutes or guidance, post-market monitoring expectations, and approach to risk classification.

Notes: Status of the EU AI Act should be reported as of the manuscript's submission date.

Abbreviations: GDPR = General Data Protection Regulation; MDR = Medical Devices Regulation; FDA = Food and Drug Administration; HIPAA = Health Insurance Portability and Accountability Act.

Category	*Artifact*	*Purpose / where used*
Planning	Data governance plan	Defines data sources, roles, retention; planning & pre-submission
Planning	De-identification memo	Safe Harbor vs Expert Determination; planning & submissions
Planning	Risk analysis (45 CFR 164.308)	Security Rule compliance; planning & deployment
Vendor	BAA / DUA package	Contractual privacy duties; deployment & operations
Monitoring	Audit-log SOP	Access monitoring; deployment & post-market
Monitoring	Post-deployment monitoring plan	Pair safety & privacy checks; post-market
Change	Change-control SOP	Versioning & update reviews; post-market
Incident	Breach response playbook	Incident governance; post-market
EoL	Decommission checklist	Secure disposal & account revocation; end-of-life

Table 3: Artifact Checklist to Support Coordinated Safety and Privacy Review.

Caption: Recommended documentation set, mapped to purpose, ownership, timing, and retention, to operationalize a single-cadence governance process (e.g., risk analysis, de-identification memorandum, vendor inventory, audit-log configuration SOP, change-control SOP, decommission checklist).

Abbreviations: As above.

Lifecycle stage (FDA lens)	*FDA focus (what reviewers expect)*	*HIPAA/HITECH touchpoints (what privacy officers check)*	*Common friction points*	*Practical artifacts to prepare*
1) Planning & data strategy (pre-submission)	Define intended use; risk category; user/population; human-factors plan	Lawful basis for using patient info; "minimum necessary"; de-identification approach (Safe Harbor vs. Expert Determination); Business Associate Agreements (BAAs); Security Rule risk analysis (45 CFR 164.308)	Re-use of historical records without clear consent; combining datasets from multiple sites; vendor hosting	Data governance plan; de-identification memo; BAA template; security risk analysis; role-based access matrix
2) Pre-market testing & validation	Verification/validation; clinical evaluation; software lifecycle documentation; cybersecurity plan	Whether testing used identifiable info; accounting of disclosures; access controls and audit logs; separation of operations vs. research uses	Mixing "quality improvement" with research without clear documentation; weak provenance for sample data	Data provenance log; disclosure log; audit-log setup; privacy impact assessment (PIA)
3) Submission/clearance	Traceable evidence package; labeling/IFU; known risks/mitigations; change control	Avoid inclusion of identifiable data in submissions; secure transfer to FDA; vendor/sub-processor BAAs	Third-party test reports that contain traceable records; unclear vendor chain	De-identified evidence pack; secure transfer SOP; vendor/sub-processor inventory & BAAs
4) Deployment in a covered entity	Usability; implementation instructions; cybersecurity hardening; site readiness	Security Rule controls (access, encryption, audit trails); BAAs executed; "minimum necessary" configuration; patient right of access & transparency	Vendor remote access; cloud logs that capture identifiers; role creep beyond "minimum necessary"	Access-control matrix; audit-log configuration SOP; DUA/BAA package; user training checklist; site privacy notice text
5) Post-market monitoring & updates	Complaint handling; field corrections/removals; safety reporting; change management for updates	Ongoing uses/disclosures; breach notification; reassess de-identification if new data are collected; update BAAs if telemetry scope changes	Telemetry sent back to vendor considered PHI; monitoring data stored outside the covered entity; performance changes over time requiring updates	Post-deployment monitoring plan; change-control SOP; breach response playbook; data retention schedule; patient-facing transparency addendum
6) End-of-life / decommissioning	Retirement plan; device removal from service	Secure disposal (45 CFR 164.310(d)(2)); vendor return/delete certifications; revoke access	Stranded backups; lingering vendor accounts; unclear ownership of stored info	Decommission checklist; certificate of destruction; account revocation log

Table 4: Governance Cross-Walk: Privacy Obligations Mapped to FDA Lifecycle Stages.

Discussion

Principal Findings

Looking at public sources, we see that privacy work and device checks often happen separately. This causes problems at different points in the process. Common issues include: (1) not knowing the legal reasons or methods for anonymizing data when preparing datasets for testing; (2) confusion about what vendors and subcontractors need to do when deploying; and (3) unclear expectations for monitoring and updating after deployment. Smaller organizations seem to feel these problems more, according to reports. A simple fix is to put privacy tasks together with device milestones so you plan once and reuse that information in both areas.

How This Looks Compared to Other Research

Our quick review matches what other studies say about U.S. health data rules and device oversight. Public sources often mention that HIPAA's de-identification rules can make models worse and still leave a risk of re-identification in big or linked datasets (Rocher et al., 2019). Also, reviews of FDA decisions show that many rely on the 510(k) process for software tools. They often have different ideas about monitoring after the product is approved (Benjamens et al., 2020). Instead of making new rules, we organize these issues into a simple chart. This chart shows where privacy and safety processes clash, especially for tools that get updated after they are used. The strain on smaller hospitals seen here is similar to long-standing concerns about fairness in digital health adoption, which other studies also mention (Adler-Milstein & Jha, 2017).

Policy Implications

The findings from this study point to several key actions that policymakers should consider to improve coordination and fairness in healthcare technology regulation.

A Single, Coherent Set of Rules

At present, oversight is divided among several agencies such as the FDA and the Office for Civil Rights under HIPAA, each applying different standards. This fragmented approach often causes confusion and delays. A unified framework that combines both safety and privacy requirements would simplify compliance and create a clearer path for developers and healthcare organizations, while still ensuring strong patient protection (Pham, 2025).

Scaled Rules for Smaller Healthcare Facilities.

Smaller hospitals and clinics face significant costs and administrative challenges in meeting complex regulatory standards. Creating simpler, risk-based rules for technologies that pose lower risks would reduce their burden. Streamlined procedures, clear templates, and shared technical resources could help these institutions remain compliant without overextending their limited budgets and staff.

Oversight for Changing Technologies

Many of today's digital tools, especially those that rely on data-driven updates, evolve after they are first approved. Most existing regulations, however, were designed for fixed systems that do not change. Policymakers need to clarify how ongoing monitoring should occur, who is responsible for tracking updates, and what steps should be taken when technology is modified after deployment. Clearer rules on post-deployment review, periodic reassessment, and data management would make oversight more effective and predictable. Other regions such as the European Union and Singapore have already introduced risk-based regulatory models that adjust oversight according to the potential impact and complexity of the technology (Aboy, Liddell, & Sreenivasan, 2024). Adapting similar models in the United States could promote innovation while maintaining a consistent focus on safety, privacy, and accountability in healthcare.

Why It Matters for Patients and Money

Making everyone follow the same rules for AI tools is hard. Smaller hospitals and rural clinics spend more time and money on compliance. Larger hospitals move faster and get new tech sooner. Also, most FDA-approved devices are not tracked after they are used,

so patients might be at risk if algorithms change. From a money point of view, smaller hospitals spend about a third of their AI budget just on following rules. That's a lot of wasted resources that could go toward actually helping patients or trying new things (Say and Thomson, 2003).

Combining Privacy and Safety Reviews

Table 4 provides a clear guide that links the privacy and security requirements of HIPAA and HITECH with the safety review steps of the FDA. The goal is to help healthcare technology teams plan once and meet both sets of rules without repeating work. The first column outlines what the FDA looks for during each stage of device approval. The second column lists the privacy and security checks needed at those same points. Areas marked as "friction points" show where teams often face challenges (Filkins et al., 2016). The final column gives examples of useful documents such as records of how data were made anonymous, access-control lists, and log files showing who used the system. This table can be used as a practical checklist to guide reviews, clarify what vendors must do (including subcontractors), and ensure that both safety and privacy are reviewed regularly, even after updates are made to a device (Filkins et al., 2016).

This combined review is useful in two main stages: before deployment and after deployment. Before a product is released, the checklist helps teams prepare a clear report showing how they followed privacy and safety rules. This supports both regulatory approval and compliance with local privacy standards. After deployment, it serves as a routine checkup to confirm that the system remains safe and secure. These follow-up checks include reviewing access logs, tracking how and when data are shared, confirming which data are collected, and verifying how long they are stored. If data have been made anonymous, teams should record which method was used such as Safe Harbor or Expert Determination and explain why it was chosen. Any future changes, such as adding new data fields, should prompt a review of the earlier decision. When a device is retired or replaced, it must be properly wiped, and related user accounts should be closed to prevent leftover access to private information (Hadi, et al.,2019).

This crosswalk is meant as a planning and management tool, not as legal advice. Local, state, or insurance rules may include extra requirements. Teams should follow the HIPAA Security Rule when performing risk reviews or disposing of digital media (see 45 CFR §164.308 and §164.310(d)(2)). Vendor agreements should also be updated whenever services, software, or equipment change (Hadi, et al.,2019). From a broader policy viewpoint, combining privacy and safety checks in this way promotes regular, coordinated oversight. National agencies could make this process easier by providing standard templates such as risk review forms, de-identification records, and audit log examples to help ensure consistency and accountability across different healthcare organizations.

Limitations

This analysis is based on publicly available information. It does not include non-public guidance, internal compliance interpretations, or recent payer policy changes. We did not evaluate how organizations implement practices. Our conclusions are based on the information available at the time of review.

Future Research Priorities

More studies over time are needed. These studies should examine how new regulations affect AI use and clinical results. Comparing different countries can show which practices best balance innovation and patient safety. Using implementation science methods can identify what organizational and environmental factors support navigating regulations effectively.

Conclusion

Guidance and analysis show that fragmented privacy rules and device oversight create barriers to using software tools in healthcare. The main issues are repeated reviews, unclear handoffs during updates, and inconsistent monitoring after deployment. A simple, risk-based governance model can improve this. It should combine privacy and safety evidence at each stage. Using standard documents and clear vendor responsibilities can lower uncertainty and protect patient safety. Federal guidance that supports this review process and

provides templates can help organizations adopt new tools safely and fairly.

Data Availability Statement

No new data were generated. This article synthesizes publicly available materials (FDA device decisions and guidance, ONC/CMS documents, and state statutes).

Competing Interests

The authors declare no competing financial interests.

References

1. Aboy M, Minssen T and Vayena E. "Navigating the EU AI Act: implications for regulated digital medical products". NPJ Digit Med 7.1 (2024): 237.
2. Adler-Milstein J and Jha AK. "HITECH Act Drove Large Gains in Hospital Electronic Health Record Adoption". Health Aff (Millwood) 36.8 (2017): 1416-1422.
3. Benjamens S, Dhunnoo P and Meskó B. "The state of artificial intelligence-based FDA-approved medical devices and algorithms: An online database". NPJ Digital Medicine 3.1 (2020): 118.
4. Braun V and Clarke V. "Using Thematic Analysis in Psychology". Qualitative Research in Psychology 3 (2006): 77-101.
5. Cohen IG., et al. "The legal and ethical concerns that arise from using complex predictive analytics in health care". Health Affairs (Millwood) 33.7 (2014): 1139-1147.
6. Cohen IG., et al. "The legal and ethical concerns that arise from using complex predictive analytics in health care". Health Affairs 33.7 (2021): 1139-1147.
7. Creswell. J.W. and Creswell JD. "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches". 4th Edition, Sage, Newbury Park (2017).
8. Gerke, S., Minssen, T., and Cohen IG. "Ethical and legal challenges of artificial intelligence-driven healthcare". Cambridge Quarterly of Healthcare Ethics 29.2 (2020): 264-273.
9. Goktas P and Grzybowski A. "Shaping the Future of Healthcare: Ethical Clinical Challenges and Pathways to Trustworthy AI". J Clin Med 14.5 (2025): 1605.
10. Jiang F., et al. "Artificial intelligence in healthcare: Past, present and future". Stroke and Vascular Neurology 2.4 (2017): 230-243.
11. Jiang F., et al. "Artificial intelligence in healthcare: Past, present and future". Stroke and Vascular Neurology 2.4 (2017): 230-243.
12. McHugh ML. "Interrater reliability: the kappa statistic". Biochem Med (Zagreb) 22.3 (2012): 276-82.
13. Moore W and Frye S. "Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules". J Nucl Med Technol 47.4 (2019): 269-272.
14. Price WN 2nd and Cohen IG. "Privacy in the age of medical big data". Nat Med 25.1 (2019): 37-43.
15. Rocher L, Hendrickx JM and de Montjoye YA. "Estimating the success of re-identifications in incomplete datasets using generative models". Nat Commun 10 (2019): 3069.
16. Stevens I., et al. "Bring a 'Patient's Medical AI Journey' to the Hill". The American Journal of Bioethics 25.3 (2025): 132-135.
17. Guest G, Bunce A and Johnson L. "How Many Interviews Are Enough? An Experiment with Data Saturation and Variability". Field Methods 18.1 (2006): 59-82.
18. HIMSS. "2023 Healthcare AI Adoption Survey". Healthcare Information and Management Systems Society (2023).
19. Malterud K, Siersma VD and Guassora AD. "Sample size in qualitative interview studies: Guided by information power". Qualitative Health Research 26.13 (2016): 1753-1760.
20. McHugh ML. "Interrater reliability: the kappa statistic". Biochem Med (Zagreb) 22.3 (2012): 276-82.
21. Markus Hinterleitner, Christoph Knill and Yves Steinebach. "The growth of policies, rules, and regulations: A review of the literature and research agenda" (2023).

22. Rebecca Boden and Julie Froud. "Obeying the rules: Accounting for regulatory compliance costs in the United Kingdom". Accounting, Organizations and Society 21.6 (1996): 529-547.
23. Scott JT., et al. "Bridging the research-policy divide: Pathways to engagement and skill development". Am J Orthopsychiatry 89.4 (2019): 434-441.
24. Say RE and Thomson R. "The importance of patient preferences in treatment decisions--challenges for doctors". BMJ 327.7414 (2003): 542-5.
25. Pham T. "Ethical and legal considerations in healthcare AI: innovation and policy for safe and fair use". R Soc Open Sci 12.5 (2025): 241873.
26. Filkins BL., et al. "Privacy and security in the era of digital health: what should translational researchers know and do about it?". Am J Transl Res 8.3 (2016): 1560-80.
27. Hadi Ghayoomi., et al. "Assessing resilience of hospitals to cyberattack". Digital Health (2021).
28. Genevieve P Kanter, Jack Kufahl and I Glenn Cohen. "Beyond Security Patches-Fundamental Incentive Problems in Health Care Cybersecurity". JAMA Health Forum 2.10 (2021): e212969.
29. "An Insight into the Current Security Posture of Healthcare IT: A National Security Concern". The Institute for Critical Infrastructure Technology (2019).