HEALTH ORGANIZATION AND ETHICS
J. Heal Ethics Admin
Volume 11 | Number 4 (Fall 2025)
www.jheaonline.org
ISSN 2474-2309 | doi:10.22461/jhea.6.7165
https://doi.org/10.22461/jhea.6.7165
Published Nov 04, 2025

ETHICAL ALIGNMENT OF BLOCKCHAIN DESIGN FRAMEWORKS WITH SOCIAL WORK CODES OF ETHICS: IMPLICATIONS FOR MENTAL HEALTH PRACTICE

Cicely Campbell, LCSW-BACS
siriustherapyinfo@gmail.com

Abstract: *Blockchain technology offers secure, decentralized solutions for managing mental health records and identity verification; however, its ethical implications necessitate rigorous scrutiny. This paper evaluates four blockchain ethical design frameworks—Beeck Center's Blockchain Ethical Design Framework, The Institute of Electrical and Electronics Engineers (IEEE) 7000 Value-Based Engineering Model Process, Value-Sensitive Design (VSD), and Ishmaev's (2025) ethical risk analysis—with the National Association of Social Workers (NASW) and Louisiana State Board of Social Work Examiners (LABSWE) Rules, Standards, and Procedures by identifying and defining key ethical principles, analyzing their alignment, and exploring practical implications for trauma-informed, client-centered mental health practice. To foster and guide ethical blockchain integration, we must ensure alignment with social work values of dignity, equity, and autonomy.*

Keywords: *blockchain, ethics, mental health, social work, trauma-informed care, NASW, LABSWE*

*Address correspondence to: Cicely Campbell, LCSW-BACS. Email: siriustherapyinfo@gmail.com

+To cite this article: Campbell, C. "Ethical Alignment of Blockchain Design Frameworks with Social Work Codes of Ethics: Implications for Mental Health Practice ". The Journal of Healthcare Ethics & Administration Vol. 11, no. 4 (Fall 2025): 48-58, https://doi.org/10.22461/jhea.6.7165

INTRODUCTION

With decades of experience as a social worker, I have intimately navigated the evolving landscape of technology integration within mental health practice, from the advent of paper-based records to the widespread adoption of sophisticated electronic systems. The continuous drive for enhanced security, efficiency, and accountability in sensitive areas such as client record-keeping and care coordination has propelled the exploration of novel technological solutions. Among these, blockchain technology, characterized by its decentralized, immutable, and transparent architecture, presents a compelling promise. It offers the potential for unprecedented data integrity and a new paradigm for managing sensitive mental health information.

However the enthusiasm for blockchain's transformative potential must be tempered with rigorous ethical scrutiny. Its adoption in a field as delicate as mental health practice raises profound ethical concerns, particularly regarding the safeguarding of client privacy, ensuring equitable access to care, and upholding the fundamental principle of informed consent. These challenges necessitate a deliberate and values-driven approach to design and implementation.

Guided by the foundational principles of the National Association of Social Workers (NASW, 2021) and Louisiana State Board of Social Work Examiners (LABSWE, 2023) Rules, Standards, and Procedures, this paper undertakes a critical examination. We will first delineate four prominent blockchain ethical design frameworks: the Beeck Center’s Blockchain Ethical Design Framework, IEEE 7000 Value-Based Engineering Model Process, Value-Sensitive Design (VSD), and Ishmaev’s (2025) ethical risk analysis. Subsequently, we will define and elaborate on the core ethical principles articulated in the NASW Code of Ethics and LABSWE Rules, Standards and Procedures. Then provide a detailed analysis of the alignment and divergence between these blockchain design frameworks and established social work ethical principles. Finally, we will explore the tangible implications of this ethical analysis for trauma-informed and client-centered mental health practice, offering a roadmap for the responsible and ethical integration of blockchain technology that upholds social work values.

METHODS

This paper employs a qualitative, interpretive approach to analyze the ethical alignment of blockchain design frameworks with the NASW and LABSWE codes of ethics and standards. The selection of relevant literature and ethical frameworks was conducted through a systematic search strategy.

The literature search primarily focused on identifying prominent ethical design frameworks applicable to emerging technologies, with a specific emphasis on blockchain. Key academic databases, including PubMed, Scopus, and IEEE Xplore were systematically queried using combinations of keywords such as "blockchain ethics," "ethical design framework," “social work and blockchain,” "distributed ledger technology ethics," "blockchain risk analysis," and "technology ethics in healthcare." Additionally, searches extended to reputable organizational reports and white papers from recognized technology and social impact centers (e.g., Beeck Center for Social Impact + Innovation) to capture contemporary industry-specific frameworks that may not yet be extensively indexed in traditional academic databases. Initial screening of titles and abstracts focused on direct relevance to ethical considerations in technology design, particularly for decentralized systems. Full-text articles and reports were then reviewed for their depth of discussion on ethical principles, design methodologies, and applicability to blockchain.

The criteria for the inclusion of blockchain ethical design frameworks were multifaceted, aiming for a comprehensive representation of approaches to embedding ethics into the technology's architecture and governance. Frameworks were selected if they: (a) explicitly provided a structured approach or methodology for integrating ethical considerations into the *design and development* lifecycle of blockchain or related distributed ledger technologies (e.g., Beeck Center, 2020; Friedman et al., 2006; IEEE, 2021; Ishmaev, 2025); (b) directly addressed the unique ethical challenges posed by blockchain's inherent characteristics, such as immutability, decentralization, and cryptographic principles (e.g., Ishmaev, 2025); (c) demonstrated a focus beyond mere legal compliance, emphasizing proactive, values-driven design principles (e.g., Beeck Center, 2020; Friedman et al., 2006; IEEE, 2021); and (d) originated from established academic research, professional engineering bodies, or reputable non-profit organizations recognized for their work in technology ethics. This approach led to the selection of the Beeck Center's Blockchain Ethical Design Framework, IEEE 7000 Value-Based Engineering Model Process, Value-Sensitive Design (VSD), and Ishmaev's (2025) ethical risk analysis, as they collectively offer distinct yet complementary perspectives—from social impact and engineering standards to human values integration and blockchain-specific risk assessment. This deliberate selection ensured a robust analytical foundation for evaluating their alignment with social work ethical principles.

BLOCKCHAIN ETHICAL DESIGN FRAMEWORKS

The emerging landscape of blockchain technology necessitates robust ethical considerations, leading to the development of specialized design frameworks aimed at embedding values and mitigating risks.

The Beeck Center Blockchain Ethical Design Framework (2020), developed by Georgetown University, provides a practical lens for ensuring ethical blockchain use in social impact initiatives. This framework is structured around five key principles. *Problem Framing* emphasizes the critical need to define the social problem clearly, ensuring that blockchain solutions genuinely address a societal need rather than merely serving as a technological solution in search of an application. For instance, in mental health, this means identifying whether blockchain truly improves access to mental health records for underserved communities, not just adopting it because it's a new technology. Secondly, *Stakeholder Mapping* requires the comprehensive identification and active involvement of all affected parties in the design process, including clients, clinicians, administrators, and particularly marginalized groups, to ensure the resulting system is inclusive and responsive to diverse needs. Thirdly, *Equity and Inclusion* prioritizes equitable access for all populations, particularly those historically underserved, by proactively addressing systemic barriers such as digital literacy gaps or economic disadvantages that might impede participation. Fourthly, *Transparency and Accountability* mandates that system processes are auditable, understandable, and transparent to all stakeholders, thereby fostering trust and enabling oversight. Finally, *Participatory Governance* advocates for involving stakeholders in decision-making processes, aiming to democratize control and mitigate potential power imbalances that could arise from centralized technological authority.

IEEE 7000 Value-Based Engineering Model Process(IEEE, 2021) offers a more formalized standard for embedding ethical values directly into the engineering design process of autonomous and intelligent systems. This approach integrates ethical considerations throughout the system development lifecycle. Its core components include *Value Discovery*, which involves systematically identifying and articulating the values of all stakeholders, such as client autonomy and privacy, to serve as foundational design drivers. Following this, *Ethical Requirements Elicitation* translates these discovered values into concrete, technical specifications that guide the system's architecture and functionality, for example, by designing specific privacy protections into the system. The standard also emphasizes continuous *Stakeholder Engagement*, ensuring that diverse groups are actively involved in iterative design processes, allowing for feedback and refinement based on real-world needs and ethical implications. Furthermore, *Ethical Risk Assessment* is a crucial component, requiring a thorough evaluation of potential harms, such as data breaches or algorithmic bias, and the implementation of robust mitigations. Lastly, *Traceability of Ethical Design Choices* mandates comprehensive documentation of all ethical decisions made throughout the design process, ensuring accountability, transparency, and replicability.

Value-Sensitive Design (VSD), as articulated by Friedman et al. (2006), represents a theoretically grounded approach that aims to integrate human values into the design of technology from its inception. VSD is distinguished by three types of investigations: conceptual, empirical, and technical. In practice, it focuses on several key areas. Foremost is *Human Values Integration*, which strives to embed values like privacy, fairness, and human autonomy directly into the system architecture and functionalities, rather than treating them as afterthoughts. *Inclusivity and Fairness* are central tenets, ensuring that the technology serves diverse populations equitably and does not perpetuate or create new forms of discrimination. A strong emphasis is placed on *Privacy and Autonomy*, particularly protecting user control over personal data, which is critically important in mental health contexts given the sensitive nature of information. VSD also stresses *Iterative Stakeholder Engagement*, recognizing that continuous involvement of stakeholders throughout the design process is essential for refining designs and ensuring they remain aligned with human values. Ultimately, VSD advocates for *Embedded Ethics in Design*, making ethical considerations an intrinsic, rather than external, part of the entire technological development process.

Finally, Ishmaev’s (2025) Ethical Risk Analysis specifically addresses the unique ethical risks inherent in blockchain technologies, moving beyond general ethical design principles to focus on blockchain's distinct characteristics. This framework highlights several critical considerations. *Risk-Benefit Asymmetry Awareness* urges designers to acknowledge that the benefits of blockchain (e.g., secure records) may not equally offset its risks (e.g., data permanence) for all users, particularly vulnerable populations, necessitating a careful balance. *Consent-Based Participation* is paramount, ensuring that users have genuine ability to opt in or out of blockchain systems with clear, comprehensive, and informed consent, especially given the technology's often complex nature. The principle of *Transparency in Power Distribution* calls for explicit disclosure regarding who controls data and how, aiming to prevent exploitation or the creation of new power monopolies within decentralized systems. *Ethical Resilience* emphasizes designing systems that can adapt and respond effectively to unforeseen ethical challenges or shifts in societal values over time, acknowledging the dynamic nature of technology and ethics. Lastly, *Critical Reflection on Governance* encourages continuous evaluation of the system's governance models to ensure ongoing fairness, equity, and accountability, mitigating the potential for unintended ethical consequences. Consider a hypothetical blockchain-based patient portal for mental health records. Applying Ishmaev's lens would involve recognizing the *risk-benefit asymmetry* where the portal's immutable records, while beneficial for continuity of care, could pose a disproportionate risk to a trauma survivor who might later wish to expunge specific, triggering information from their permanent record (SAMHSA, 2014). It would also entail ensuring *consent-based participation* by designing the system so a client's consent to use the portal is not only informed but also truly voluntary, with clear, easy-to-understand options for opting out or revoking access to specific data elements, rather than an all-or-nothing approach. Furthermore, establishing *transparency in power distribution* requires clearly communicating to clients and clinicians who holds the keys to encrypted data, how access permissions are managed, and who can initiate or verify transactions on the blockchain, thereby preventing hidden power dynamics. Building *ethical resilience* into the portal's design necessitates allowing for future adaptations, such as the integration of new privacy-enhancing technologies or evolving legal interpretations of data rights, ensuring the system can ethically evolve without requiring a complete overhaul. Lastly, engaging in *critical reflection on governance* involves regularly reviewing the portal's governance structure—for example, who validates new entries or changes to access rules—to ensure it remains fair, prevents undue influence by any single entity, and continues to prioritize client well-being over technological rigidity. By applying this analytical lens, designers can proactively identify and address potential ethical pitfalls before widespread deployment, ensuring blockchain solutions genuinely serve the best interests of mental health clients.

SOCIAL WORK ETHICAL STANDARDS

The professional practice of social work is underpinned by a robust ethical framework, ensuring that interventions prioritize client well-being, social justice, and professional integrity. The National Association of Social Workers (NASW) Code of Ethics (2021) articulates six core values that guide this practice. *Service* mandates that social workers prioritize helping people in need and addressing social problems, which in the context of mental health, often translates to ensuring equitable access to care and resources. *Social Justice* compels social workers to challenge social injustice, advocating for vulnerable and oppressed individuals and groups and actively working to eliminate oppression, especially concerning issues like mental health disparities. The principle of *Dignity and Worth of the Person* requires social workers to treat each person in a caring and respectful fashion, mindful of individual differences and cultural and ethnic diversity, and to promote clients' socially responsible self-determination. Central to effective practice is the *Importance of Human Relationships*, recognizing that relationships between people are an important vehicle for change and fostering strong therapeutic alliances. *Integrity* dictates that social workers should behave in a trustworthy manner, consistently acting honestly and responsibly in all professional activities. Finally, *Competence* obligates social workers to practice within their areas of competence and to develop and enhance their professional expertise, critically including continuous education on emerging technologies relevant to practice.

Complementing the national guidelines, the Louisiana State Board of Social Work Examiners (LABSWE) Code of Conduct (2023) aligns closely with the NASW principles while incorporating state-specific mandates and an intensified focus on technological practice. This code reinforces the imperative for *Compliance with Laws*, requiring social workers to adhere strictly to all applicable federal and state regulations, such as HIPAA and FERPA, which are paramount when managing sensitive digital health information. Furthermore, LABSWE explicitly addresses *Ethical Technology Use*, emphasizing that all technologies employed in practice must support client welfare, protect confidentiality, and be utilized responsibly. The code also stresses *Accountability in Digital Recordkeeping*, mandating that social workers maintain secure, accurate, and accessible client records, recognizing the unique challenges and responsibilities associated with electronic documentation. Lastly, the LABSWE code strongly advocates for *Continued Professional Development*, underscoring the necessity for social workers to engage in ongoing training and education to remain competent in an ever-evolving technological landscape, thereby ensuring they are equipped to navigate the complexities of new tools like blockchain while upholding ethical standards.

ALIGNMENT OF FRAMEWORKS WITH SOCIAL WORK ETHICS

Table 1 maps ethical principles across blockchain frameworks and social work codes, highlighting areas of alignment and gaps.

Table 1: Alignment of Ethical Principles Across Frameworks and Codes

Principle	Beeck Center	IEEE 7000	VSD D	Ishmaev (2025)	NASW	LABSWE
Service/Problem Framing	✓	✓	✓	✓	✓	✓
Social Justice/Equity	✓	✓	✓	✓	✓	✓
Dignity/Privacy/Autonomy	✓	✓	✓	✓	✓	✓
Human Relationships	✓	✓	✓	✓	✓	✓

Integrity/Transparency	✓	✓	✓	✓	✓	✓
Competence/Education	✓	✓	✓	✓	✓	✓
Legal Compliance	✗	✗	✗	✗	✗	✓

DETAILED ALIGNMENT ANALYSIS

The comparative analysis of blockchain ethical design frameworks against established social work ethical codes reveals significant areas of congruence, alongside critical points of divergence that necessitate careful consideration for mental health practice. This section elaborates on the alignment and disparities, providing a more nuanced understanding of how these technological design principles interact with professional social work values.

The principles of Service and Problem Framing demonstrate strong alignment across all frameworks and social work codes. Both the blockchain frameworks (Beeck Center's 'Problem Framing,' IEEE 7000's 'Value Discovery,' VSD's 'Human Values Integration,' and Ishmaev's 'Risk-Benefit Asymmetry Awareness') and the NASW's core value of 'Service' emphasize the imperative to address genuine needs and solve pressing problems. For instance, blockchain's potential to streamline crisis intervention by securely and rapidly sharing crucial client data across disparate providers directly addresses critical gaps in care continuity, potentially saving lives by enabling more efficient and informed responses during emergencies (Hripcsak et al., 2014). However, the divergence arises if blockchain is adopted primarily for its novelty or perceived technological advancement rather than a demonstrated, client-centered need. Social work ethics demand that technology serve the client, not the other way around, necessitating rigorous problem framing that prioritizes the client's lived experience and identified needs.

Similarly, the ethical principles concerning Social Justice and Equity exhibit substantial overlap. The Beeck Center's 'Equity and Inclusion' and VSD's 'Inclusivity and Fairness' directly resonate with social work's fundamental 'Social Justice' mandate. These frameworks actively champion the inclusion of marginalized groups and the reduction of systemic barriers. In practical terms, this means that any blockchain system designed for mental health must proactively address potential access barriers for underserved populations, such as those with limited digital literacy, lack of reliable internet access, or economic disadvantages, as failure to do so could exacerbate existing health disparities (Kruse et al., 2017). A key contrast emerges where blockchain's decentralized nature might inadvertently create new forms of digital exclusion if not explicitly designed with equity as a core requirement, moving beyond mere "access" to genuine "inclusion."

The safeguarding of Dignity, Privacy, and Autonomy presents both profound alignment and critical tension. While blockchain frameworks like VSD ('Privacy and Autonomy') and IEEE 7000 ('Ethical Requirements Elicitation' for privacy protections) advocate for embedding privacy-by-design, blockchain's inherent immutability poses a significant challenge to the social work principles of client dignity and self-determination, particularly in trauma-informed care. The inability to easily amend or delete records on an immutable ledger conflicts directly with a client's right to control their sensitive information and potentially expunge painful or triggering past data, which is crucial for fostering agency and healing in trauma work (SAMHSA, 2014). Here, methods like off-chain storage for sensitive data or advanced cryptographic techniques (e.g., zero-knowledge proofs) become imperative to reconcile the blockchain's design with the client's right to modify or revoke consent for their data, preventing a permanent digital footprint that could re-traumatize.

The Importance of Human Relationships within social work practice finds resonance in the stakeholder engagement components of the Beeck Center's 'Stakeholder Mapping' and 'Participatory Governance,' VSD's 'Iterative Stakeholder Engagement,' and IEEE 7000's 'Stakeholder Engagement.' These frameworks advocate for actively involving diverse groups, including clients, in the design and implementation processes. This participatory approach aligns with the social work value of fostering therapeutic alliances and empowering clients by ensuring their voices, preferences, and lived experiences directly shape the technology intended to serve them (Unertl et al., 2016). The contrast arises if blockchain development proceeds without genuine, continuous client involvement, leading to systems that are technologically sound but clinically misaligned or alienating.

Integrity and Transparency are areas where blockchain's core functionalities offer a strong advantage for social work practice. Blockchain's inherent auditability and the verifiable nature of its ledger inherently enhance accountability, aligning seamlessly with the social work principle of 'Integrity' and the need for trustworthy professional actions. However, while blockchain offers transparency of process, the 'transparency' for a trauma survivor must be carefully managed. The immutable and publicly verifiable nature of some blockchain implementations could inadvertently compromise the privacy and safety of individuals, especially survivors of abuse, who require discreet and confidential access to care (Bloom, 2013). Thus, a nuanced approach to transparency is required, distinguishing between system transparency (how the technology works) and data transparency (who can access what data), with the latter always prioritizing client safety and consent.

The principle of Competence and Education, highlighted by both NASW and explicitly mandated by LABSWE, finds indirect but critical support in frameworks like IEEE 7000, which implicitly requires ethical fluency for its value-based engineering approach. However, blockchain frameworks generally do not explicitly detail the necessity of extensive professional training. This represents a significant gap. For social workers to ethically and effectively utilize blockchain systems, comprehensive, tailored education on the technology's capabilities, limitations, and specific ethical implications is paramount (Topol, 2019). Without such targeted competence development, clinicians risk misinterpreting data, compromising client welfare through improper use, or inadvertently violating privacy regulations.

Finally, Legal Compliance, explicitly mandated by the LABSWE Code of Conduct, represents a distinct area where blockchain ethical frameworks often demonstrate a significant omission. While these frameworks focus on ethical *design*, they typically do not explicitly address the complex web of jurisdictional legal and regulatory requirements, such as HIPAA and FERPA, which are non-negotiable in mental health practice. This places a substantial burden on individual agencies and practitioners to ensure that blockchain solutions adhere to all relevant laws. Non-compliance risks severe penalties, data breaches, and profound client harm (HIPAA Journal, 2022). Therefore, a critical contrast exists in the scope: social work codes embed legal compliance as an ethical imperative, whereas blockchain frameworks tend to focus on broader ethical principles, necessitating a proactive integration of legal expertise into the blockchain design and implementation process within healthcare.

DISCUSSION: IMPLICATIONS FOR MENTAL HEALTH PRACTICE

The intricate analysis of blockchain ethical design frameworks against social work codes of ethics reveals profound implications for the responsible integration of this technology into mental health practice. Effective adoption necessitates a steadfast commitment to a trauma-informed and client-centered approach, ensuring that technological advancements genuinely serve client well-being and uphold professional ethical and legal standards. The following expanded implications, supported by examples and references, provide a practical guide for ethical blockchain implementation in mental health.

Revocable consent mechanisms and preserving client autonomy are paramount concerns arising from blockchain's immutability and its potential to undermine client autonomy, particularly for trauma survivors who may require the ability to modify or completely delete sensitive records. Traditional blockchain models, which make data deletion inherently difficult, directly conflict with the client's right to self-determination and control over their personal narrative, a cornerstone of trauma-informed care. Therefore, it is imperative for social workers to actively advocate for and design blockchain systems that incorporate robust revocable consent mechanisms. This could involve leveraging advanced cryptographic techniques such as zero-knowledge proofs, which allow for data verification without direct exposure of the sensitive information itself, or implementing hybrid models where highly sensitive data is stored off-chain with granular access controls (Sasson et al., 2014). For instance, a blockchain-based telehealth platform, designed with ethical principles in mind, could empower clients with the capability to revoke access to specific session notes or even their entire diagnostic history, thereby ensuring they retain ultimate control over their digital health footprint, mirroring successful patient-controlled health record systems (Roehrs et al., 2017).

Hybrid governance models can balance decentralization with clinical oversight. While blockchain's decentralized nature offers the promise of reduced reliance on centralized authorities and enhanced data sovereignty, its application in mental health practice cannot bypass the critical need for clinical oversight and professional accountability. The complexities of mental health care demand expert human judgment, ethical review, and accountability structures that pure decentralization might not inherently provide. Thus, the most ethically sound approach involves the adoption of hybrid governance models. These models judiciously combine the benefits of blockchain's distributed consensus mechanisms—such as immutable record-keeping and transparent transaction logs—with established professional accountability frameworks, including clinical supervision, peer review, and regulatory body oversight. For example, a blockchain system designed for inter-agency care coordination, similar to prototypes like MedRec (Azaria et al., 2016), could integrate explicit social worker oversight protocols. This ensures that while data sharing is efficient and secure, it consistently respects client boundaries, maintains confidentiality, and aligns with the NASW's principle of the importance of human relationships, where professional judgment guides technological use.

Cultural competence and accessibility ensure equitable digital inclusion. The ethical imperative of social justice and the value of human dignity dictate that blockchain systems implemented in mental health practice must be designed with explicit consideration for cultural competence and universal accessibility. This aligns directly with social work's social justice mandate and VSD's inclusivity principle. It means proactively addressing potential barriers for diverse populations, including those facing language barriers, individuals with disabilities who require assistive technologies, and communities with limited digital literacy or inadequate access to reliable internet infrastructure. A truly ethical blockchain-based record system, for instance, would integrate multilingual interfaces, offer alternative communication methods, and explore offline access options for data, much like successful global health initiatives prioritize localized and accessible digital tools (WHO, 2020). This proactive design ensures that the technology genuinely serves to bridge disparities rather than inadvertently widening them by creating new forms of digital exclusion for rural or non-English-speaking clients.

Legal and regulatory alignment are necessary. To navigate the mandates of compliance, which is perhaps one of the most critical and often overlooked implications for blockchain in mental health, is the absolute necessity of rigorous legal and regulatory alignment. While blockchain ethical frameworks offer valuable design principles, they frequently lack explicit integration with the complex web of jurisdictional laws governing health information. In mental health practice, compliance with regulations like HIPAA, FERPA, and state-specific privacy laws is not merely a recommendation but a non-negotiable legal and ethical mandate. The burden of ensuring compliance falls squarely on the implementing agencies and individual clinicians. Therefore, social workers must actively collaborate with legal experts during the entire lifecycle of blockchain system design and deployment to ensure that these technologies inherently meet or exceed all regulatory standards. For example, a mental health agency considering blockchain for record-keeping must opt for encrypted, permissioned blockchains with strict access controls and audit trails to demonstrably comply with HIPAA's security and privacy rules, as evidenced in successful pilot projects by healthcare consortia (Zhang et al., 2018). Failure to do so exposes agencies to severe legal penalties and, more importantly, risks profound harm to client trust and welfare due to potential data breaches.

To effectively address this gap and proactively embed legal compliance, checkpoints must be integrated into each phase of the blockchain design and implementation lifecycle. Beginning with the conception and planning phase, a thorough jurisdictional legal analysis is paramount to identify all relevant data privacy, security, and health information laws (e.g., HIPAA, state-specific mental health privacy laws, international regulations like GDPR if applicable) in all operational or client-residing jurisdictions (LABSWE, 2023). This phase mandates the continuous involvement of legal experts specializing in health data privacy and emerging technologies from the project's inception, informing initial problem framing and conducting an early legal risk assessment related to blockchain's inherent characteristics such as data immutability and consent mechanisms (Ishmaev, 2025). During the design and architecture phase, legal requirements must be directly translated into technical specifications, including designing for privacy-enhancing technologies (PETs), ensuring data minimization, and implementing robust encryption and granular access controls (Friedman et al., 2006; IEEE, 2021). For immutability concerns, solutions like off-chain storage for sensitive Protected Health Information (PHI) with cryptographic hashes on-chain are crucial to allow for data modification or deletion without altering the core ledger, addressing challenges like the "right to be forgotten" while maintaining chain integrity (Sasson et al., 2014). This phase also necessitates the design of explicit, granular, and easily revocable consent mechanisms that meet the highest legal standards (e.g., GDPR's explicit consent; European Union, 2016; Roehrs et al., 2017), alongside architectural provisions for comprehensive, tamper-proof audit trails for all data access and modifications to fulfill legal requirements for accountability (Beeck Center, 2020).

In the development and implementation phase, secure coding standards are essential to prevent vulnerabilities, with integrated automated and manual compliance testing throughout development to verify adherence to legal requirements. Meticulous documentation of all design decisions and code implementations that specifically address legal mandates must be maintained, creating a clear audit trail for regulatory scrutiny. Upon deployment and during operational phases, agencies must develop and rigorously enforce operational policies and procedures for data access, incident response, data retention, and secure data destruction that are fully aligned with all applicable laws, while establishing a schedule for periodic legal reviews to ensure continued compliance as laws evolve. A robust incident response plan, including clear protocols for identifying, containing, and reporting data breaches within legally mandated timelines (e.g., HIPAA's breach notification rule, GDPR's 72-hour notification; HIPAA Journal, 2022), is also critical.

Finally, in the maintenance and decommissioning phase, clear policies for data retention and secure destruction or archiving must adhere to legal retention periods, alongside protocols for the secure decommissioning of system components. Planning for the long-term management of data on immutable ledgers, particularly how "right to be forgotten" requests or data retention limits will be managed for sensitive off-chain data linked to the blockchain, is also essential. By systematically integrating these legal compliance checkpoints into each phase of the blockchain design lifecycle, mental health agencies can move beyond merely acknowledging the regulatory gap to proactively building systems that are both ethically sound and legally compliant, thereby safeguarding client welfare and professional integrity.

However, the most meticulously designed systems are only as effective as the professionals who utilize them, underscoring the critical need for robust clinician training and competence. Clinician training and competence empower the workforce. The explicit mandate for ongoing education and technological competence within the LABSWE Code of Conduct underscores a crucial implication: the imperative for robust blockchain literacy among social workers and other mental health professionals. Without targeted, comprehensive training, clinicians are at significant risk of misinterpreting system functionalities, misusing the technology, or inadvertently compromising client welfare due to a lack of understanding of blockchain's unique ethical and technical nuances. While frameworks like IEEE 7000 implicitly support ethical fluency, the specifics of clinician education are often not detailed. Therefore, professional organizations and agencies must develop and implement tailored training programs that equip social workers with the necessary knowledge and skills. These programs, drawing inspiration from established health informatics training (AMIA, 2023), should cover not only the technical aspects of blockchain but, more importantly, its specific ethical challenges, privacy implications, and the practical application of ethical decision-making within a blockchain-enabled practice environment.

Trauma-Informed Design: Prioritizing Safety and Empowerment A foundational principle for any technology implemented in mental health, especially one dealing with sensitive client data, is adherence to trauma-informed care principles: safety, trustworthiness, choice, collaboration, and empowerment (SAMHSA, 2014). This translates directly into the design of blockchain systems. User interfaces must be intuitive, non-triggering, and promote a sense of control for clients with trauma histories. This includes considerations for data input, access, and presentation. For example, a blockchain-based crisis hotline platform could utilize anonymized or pseudonymized identifiers to protect caller identities and ensure their privacy and safety, a feature commonly implemented in secure, encrypted telehealth systems (Kruse et al., 2017). This deliberate design choice directly aligns with the NASW's principle of 'Dignity and Worth of the Person,' by prioritizing the client's sense of security and agency within the technological interaction.

Equity in implementation is critical to bridging the digital divide. To genuinely uphold social work's commitment to social justice and avoid exacerbating existing disparities, the implementation of blockchain technology must actively prioritize equitable access and benefit for marginalized communities. The promise of decentralized systems can only be realized if the infrastructure, digital literacy, and financial resources are equitably distributed. Social workers are uniquely positioned to advocate for policies and funding that ensure accessible and affordable blockchain solutions in underserved areas. This could involve community mental health centers partnering with technology developers to deploy blockchain systems in rural or low-income communities, much like mobile health clinics have successfully extended care access to historically underserved populations (HHS, 2021). Without such proactive measures, blockchain, despite its potential, risks becoming another technology that disproportionately benefits the privileged, further entrenching inequities in mental health care access.

CONCLUSION

Blockchain technology holds transformative potential for mental health practice, enhancing security and coordination. However, its ethical adoption requires alignment with NASW and LABSWE values, emphasizing client dignity, equity, and autonomy. By integrating principles from Beeck Center, IEEE 7000, VSD, and Ishmaev's frameworks, social workers can advocate for systems that prioritize trauma-informed care and cultural competence. Real-world examples, such as MedRec and patient-controlled health records, demonstrate blockchain's feasibility when ethically designed. As veteran social workers, we must lead this effort, ensuring technology serves as a tool for healing and justice.

REFERENCES

American Medical Informatics Association. (2023). *Health informatics training programs*. AMIA.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *2016 2nd International Conference on Open and Big Data*, 25–30.

Beeck Center. (2020). *Blockchain ethical design framework for social impact*. Georgetown University.

Bloom, S. L. (2013). *Creating sanctuary: Toward the evolution of sane societies*. Routledge.

Friedman, B., Kahn, P. H., & Borning, A. (2006). Value sensitive design and information systems. In *Human-computer interaction in management information systems* (pp. 348–372). HIPAA Journal. (2022). *Healthcare data breach statistics*. HIPAA Journal.

Hripcsak, G., et al. (2014). Next-generation phenotyping of electronic health records. *Journal of the American Medical Informatics Association*, 21(1), 5–10.

Ishmaev, G. (2025). Ethics of blockchain technologies. *arXiv preprint arXiv:2504.02504*.

Kruse, C. S., et al. (2017). Mobile health solutions for the aging population: A systematic narrative analysis. *Journal of Telemedicine and Telecare*, 23(4), 439–451.

Louisiana State Board of Social Work Examiners. (2023). *Standards of practice and code of conduct*.

National Association of Social Workers. (2021). *Code of ethics*.

Roehrs, A., et al. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, 71, 70–81.

Sasson, E. B., et al. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. *2014 IEEE Symposium on Security and Privacy*, 459–474.

Substance Abuse and Mental Health Services Administration. (2014). *SAMHSA's concept of trauma and guidance for a trauma-informed approach*. SAMHSA.

Topol, E. (2019). *Deep medicine: How artificial intelligence can make healthcare human again*. Basic Books.

Unertl, K. M., et al. (2016). Integrating community-based participatory research and informatics approaches to improve the engagement and health of underserved populations. *Journal of the American Medical Informatics Association*, 23(1), 60–73.

World Health Organization. (2020). *Digital health for all: A global strategy 2020–2025*. WHO.

Zhang, P., et al. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, 16, 267–278.