frontiers in Blockchain

POLICY AND PRACTICE REVIEWS
published: 08 November 2019
doi: 10.3389/fbloc.2019.00018

Blockchain Compliance by Design: Regulatory Considerations for Blockchain in Clinical Research

Wendy Charles[1], Natalie Marler[2], Lauren Long[2] and Sean Manion[2,3]*

[1] Denver Health, Enterprise Compliance Services, Denver, CO, United States, [2] Science Distributed, Baltimore, MD, United States, [3] Blockchain in Healthcare Global - IEEE Industry Standards and Technology Organization, Piscataway, NJ, United States

As clinical research moves toward real-world data capture with increased data sharing, there is a growing need for patient-centered technologies that ensure data authenticity and promote researcher and patient access. Blockchain is one of an emerging set of distributed ledger technologies with the potential to offer both research data transparency and trust, while offering robust security measures. As blockchain-based systems are being developed for clinical research applications, these systems may be required to follow state and federal research regulations, such as ethical protections for human participants and data privacy. Blockchain developers and research organizations alike are struggling to identify and interpret these regulatory requirements. Further, regulatory agencies and policymakers have not yet provided blockchain stakeholders with clear guidelines to achieve compliance. This article provides an introduction to the clinical research and health information privacy regulations in the United States as well as data design standards and electronic signature laws. We also offer recommendations for blockchain developers, researchers, and research organizations for achieving compliant blockchain solutions in clinical research.

Keywords: blockchain, clinical research, regulatory compliance, data integrity, informed consent, electronic signatures, privacy, security

OPEN ACCESS

Edited by:
Mitchell Brett Parker, Indiana University Hospital, United States

Reviewed by:
Atif Farid Mohammad, University of North Carolina at Charlotte, United States
Jason Goldwater, Atlas Research, United States

****Correspondence:***
Wendy Charles
wendy.charles@cuanschutz.edu

Specialty section:
This article was submitted to Blockchain for Science, a section of the journal Frontiers in Blockchain

Received: *06 August 2019*
Accepted: *24 October 2019*
Published: *08 November 2019*

Citation:
Charles W, Marler N, Long L and Manion S (2019) Blockchain Compliance by Design: Regulatory Considerations for Blockchain in Clinical Research. Front. Blockchain 2:18. doi: 10.3389/fbloc.2019.00018

INTRODUCTION

While clinical research involves increasing reliance on electronic systems for data capture and storage (Food and Drug Administration, 2013), current research data collection and storage systems face limited capabilities to meet emerging technological needs (Efanov and Roschin, 2018). As examples, clinical research systems are not designed to give research participants access to their data, honor specific terms of participant preferences for future uses of their data (Benchoufi et al., 2018), or prevent data alterations (Benchoufi and Ravaud, 2017). Blockchain and other distributed ledger technologies (referred to collectively as "blockchain" henceforth) appear to address many of these operational obstacles in a systematic and secure manner (Hughes et al., 2019).

For readers unfamiliar with blockchain principles, blockchain involves a distributed network where identical copies of the data are stored on multiple electronic devices that cooperate to verify new data transactions. Data are captured on a digital ledger that creates a growing list of events similar to an audit log; blocks are aggregated with a type of cryptography using complex mathematics (Karame and Capkun, 2018; Hughes et al., 2019). When enough events are added to the ledger, the ledger is formed into a block with a unique digital signature corresponding to the data in that block. Each block contains unique cryptographic information about the previous

block to create a permanent link between blocks, making the blocks and data tamper-resistant (Yaga et al., 2018). Blockchains can also utilize "smart contracts," which are not actually "contracts" but computer code designed to execute automatically when specific conditions are met (Chamber of Digital Commerce, 2018). For clinical research applications, blockchain and associated smart contracts can facilitate data fraud detection (Shae and Tsai, 2017), operational efficiencies (Nugent et al., 2016), as well as improving regulatory compliance and enforcement (Choudhury et al., 2018a,b). These blockchain features offer integrity methods and access controls that traditional database systems cannot typically achieve. The integration of blockchain technologies is essential for the next generation of clinical research advancement.

With any system used for clinical research, the technology must comply with current research laws, regulations, and statutes. The applicable laws and regulations for clinical research in the United States depend on the funding source, whether the research involves a covered entity and protected health information and whether the research is funded by, or will be submitted to, a particular regulatory agency. However, blockchain developers and operators are often unfamiliar with clinical research regulations and related data and technology standards (Kakavand et al., 2017). Even for stakeholders aware of regulatory requirements, there is uncertainty about regulatory research interpretations applied to blockchain (De Filippi and Hassan, 2016).

Overall, this article is not intended to advocate for or against uses of blockchain in clinical research, but to provide an application-relevant overview of laws and regulations. While this article focuses primarily on regulations in the United States, the concepts of patient-centric design, data integrity, appropriate informed consent, and privacy apply to all research settings. This article aims to provide blockchain stakeholders with a stronger understanding of responsibilities for compliant design and implementation.

UNITED STATES CLINICAL RESEARCH REGULATORY OVERVIEW

Human Research Protection Regulations

The two primary federal agencies within the U.S. Department of Health and Human Services (HHS) responsible for providing regulatory guidance and enforcement of human subject protections are the Office of Human Research Protections (OHRP) and the Food and Drug Administration (FDA).

Abbreviations: ESIGN, Electronic Signatures in Global and National Commerce; FDA, U.S. Food and Drug Administration; HIPAA, Health Insurance Portability and Accountability Act; HITECH, Health Information Technology for Economic and Clinical Health Act; HHS, U.S. Department of Health and Human Services; IRB, Institutional Review Board; IRS, Internal Revenue Service; ISO, International Organization for Standardization; LAR, Legally Authorized Representative; NIH, National Institutes of Health; NIST, National Institute of Standards and Technology; OHRP, Office for Human Research Protections; OCR, Office for Civil Rights; PHI, Protected Health Information; TEFCA, Trusted Exchange Framework and Common Agreement; UETA, Uniform Electronic Transaction Act.

Office for Human Research Protections

The regulation, Protection of Human Subjects, is often referred to as "The Common Rule." The Common Rule offers a set of regulatory standards for safe and ethical treatment of human research participants and has been adopted by multiple federal agencies conducting human subject research. For health-related research supported or conducted by the National Institutes of Health (NIH) and other related health components, the "common" regulatory protection was incorporated by OHRP as Subpart A of 45 CFR Sect. 46 (2018)[1]. OHRP also requires additional Subparts for protection of pregnant women and fetuses, prisoners, and children not adopted by all other federal agencies. Institutional Review Boards (IRBs), committees of scientists, doctors, and patient advocates that provide ethical review of research, may voluntarily apply OHRP regulations to all research involving human subjects conducted within their organizations (AAHRPP, 2017).

Food and Drug Administration

The FDA regulates clinical research involving investigational drugs, biological products, and medical devices under its jurisdiction as established by the Food and Drug Amendments Act (2007)[2]. The FDA applies 14 regulations to protect human subjects and clinical trial integrity (Food and Drug Administration, 2018a,b). The applicability of these regulations somewhat differs by the nature of investigational product and/or technology.

Most applicable to use of blockchain in clinical research is the FDA regulation 21 CFR Sect. 11 (2018)[3], often referred to simply as "Part 11." This regulation specifies the administrative, procedural, and technical controls for records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted to comply with FDA regulations (21 CFR Sect. 11.1(b), 2018). This part also applies to electronic signatures and records submitted to the FDA, even if such records are not specifically identified in FDA regulations (Food and Drug Administration, 2017a).

HIPAA Privacy and Security Rules

While OHRP and FDA contain protections to guide the ethical conduct of human subject research, the Health Insurance Portability and Accountability Act (HIPAA) addresses permissions and protections for health information. The HIPAA Privacy Rule (45 CFR Sect. 164 Subpart E, 2013)[4] applies to a subset of individually identifiable health information—referred to as protected health information (PHI)—generated or maintained by a covered entity. Covered entities include health care providers, clearinghouses, or health plans that transmit health information electronically for claims or eligibility inquiries (45 CFR Sect. 164.104, 2013). The Privacy Rule establishes the conditions under which PHI may be used or disclosed by covered entities and also specifies how individuals will be

[1] 45 CFR Sect. 46 (2018). Protection of human subjects.
[2] Food and Drug Administration Amendments Act of 2007. Pub. L. 110–85, 121 Stat. 823 (September 27, 2007).
[3] 21 CFR Sect. 11 (2018). Electronic Records, Electronic Signatures.
[4] 45 CFR Sect. 164 (2013). Security and privacy.

informed of uses and disclosures of their health information (45 CFR Sect. 164.508, 2013). The Security Rule (45 CFR Sect. 164 Subpart C, 2013) addresses the administrative, physical, and technical safeguards necessary to protect health data storage and transmission.

When a person or organization generates, receives, processes, maintains, or transmits PHI on behalf of a covered entity, the person or organization is serving as a "business associate" of the covered entity (45 CFR Sect. 160.103, 2013)[5]. As established in the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act", Department of Health and Human Services, 2009), a business associate must follow all standards, requirements, and implementation specifications specified for a covered entity (45 CFR Sect. 164.104(b), 2013). These expectations explicitly include software or hosting companies that store PHI (Office for Civil Rights, 2002). Therefore, it may be necessary for a blockchain company hosting or processing PHI on behalf of a covered entity to follow the HIPAA regulations. Also pertinent, while the HITECH Act primarily added statutory revisions to the American Recovery and Reinvestment Act (2009)[6] to promote the meaningful use of electronic health records, sections 13400–13424 strengthened the OCR's enforcement authority to levy civil and criminal penalties for violations of the HIPAA Privacy and Security Rules.

State Statutes

A state-level review of blockchain and clinical research requirements falls outside of the scope of this article. However, it is important to be aware that state statutes may contain additional pertinent requirements. For current state-level activities involving blockchain legislation, review *Blockchain State Legislation* provided by the National Conference of State Legislatures (Morton, 2019) or *State Regulations on Virtual Currency and Blockchain Technologies* (Kohen and Wales, 2019).

Institutional Review Boards

To protect the rights and welfare of humans participating in regulated research, research protocols and related materials (e.g., informed consent documents, and recruiting materials) are reviewed by IRBs. IRBs must find that the research meets all criteria established by regulation for ethical protections. The criteria are the same for research regulated by OHRP (45 CFR Sect. 46.111, 2018) and FDA (21 CFR Sect. 56.111, 2018)[7].

REGULATORY CONSIDERATIONS FOR BLOCKCHAIN IN CLINICAL RESEARCH

While blockchain-based technologies can be used for many purposes in clinical research, this section analyzes the regulatory oversight for databases, participant permissions, and electronic signatures. For each major category of blockchain use, regulatory considerations are provided separately for each applicable regulatory agency or oversight body.

Regulatory Considerations for Creating a Clinical Research Database

When designing a blockchain intended to store information that could be used for clinical research, regulatory oversight depends on the nature of the design and storage. There are no consistent definitions for terms such as "database," "data bank," "repository," "registry," or "data warehouse" across regulations or the academic literature (Gibbons et al., 2007). While there may be nuanced differences between terms; henceforth, "database" is intended to encompass all equivalent and related terms.

Intended Purpose

A clinical database designed primarily for treatment, payment, or healthcare operations would not be subject to human subject protections or additional Privacy Rule regulations (beyond those already required for health information) even if it may also be used for research (Dokholyan et al., 2009). For example, organizations often use clinical databases to track progression of disease or prevalence of disease in a specific patient population, assess program effectiveness, perform quality improvement projects, track high risk patients, and/or track metrics for efficiencies (Pollak, 2006).

In contrast, databases designed to store, maintain, and distribute identifiable information about human participants for future research purposes may be required to follow the human research protection regulations and/or additional HIPAA regulations. The nature of applicable regulations depends on the degree to which information can identify participants, inclusion of PHI, sensitivity of information stored—such as genetic information—the types of research planned, and the source of funding or planned submissions (Dokholyan et al., 2009).

When designing a blockchain-based research database, developers and operators are encouraged to first write a "parent" protocol that describes how the research database will be created and governed, the nature and amount of identifiable information, and prohibitions against releasing "code keys" that link to participant identities (Office for Human Research Protections, 1997, 2008; Office for Civil Rights, 2017). The protocol should also describe how data could be requested from the database and that agreements will be generated with data recipients regarding data confidentiality (Office for Human Research Protections, 1997). Such a protocol will not only guide database operations, but will assist researchers and IRBs in determining the appropriate regulatory oversight.

Regulatory Oversight

This section provides basic regulatory information applicable to blockchain database creation, distribution, and usage. The requirements for storage, informed consent/authorization, and electronic signatures are provided in subsequent sections.

[5]45 CFR Sect. 160 (2013). General administrative requirements.

[6]American Recovery and Reinvestment Act Pub. L. 111–5, 123 Stat. 115 (February 17, 2009).

[7]21 CFR Sect. 56 (2018). Institutional Review Boards.

Database Creation

When a blockchain research database will be conducted or supported by a federal agency or department (or will be implemented by an organization that voluntarily applies the Common Rule to all research), the database developers and operators are encouraged to review the OHRP decision charts to determine whether the database involves human subjects and would be subject to regulation (Office for Human Research Protections, 2016a). OHRP considers the research to involve human subjects if the data include private, individually identifying information that would allow the researchers to readily identify the individuals in the individuals in the dataset (Office for Human Research Protections, 2008). Conversely, private information is not considered identifiable—and would not constitute human subject research—if the data cannot be associated with specific individuals directly or through access to code keys/systems (Office for Human Research Protections, 2008). Generally, if data constitute human subject research, the researchers should submit a parent protocol for IRB review. The IRB will be particularly attentive to procedural and security mechanisms pertaining to data privacy, confidentiality, and secondary uses [45 CFR Sect. 46.111(a)(7) and (8)]. An IRB approval or determination should be obtained before collecting identifiable data.

Certain types of standalone databases may also be subject to FDA regulations. For example, research databases whose intent is to evaluate the safety or effectiveness of a medical device are subject to FDA regulations (Food and Drug Administration, 2019a) even if there is no intent to submit the data to the FDA [21 CFR Sect. 11.2(a)]. Further, the FDA has issued draft guidance for using registry and electronic health record data as a source of real-world evidence (Food and Drug Administration, 2019b,c) and to support the study of disease diagnostics (Sichtig et al., 2019) and regulatory decision-making (Cirilli, 2019). When submitted as part of a marketing application, though, it is noteworthy that the FDA provides protections of certain data that might otherwise be classified as non-human subject research under OHRP regulations [21 CFR Sect. 50.3(b) and (g); (Riddle, 2018)].

When a covered entity or business associate creates or maintains a research database involving PHI, the database activity itself is considered a research activity under the Privacy Rule (National Institutes of Health, 2004a). While OHRP uses the ambiguous standard of "readily identifiable private information" to determine whether the Common Rule applies, the Privacy Rule involves more stringent criteria. Specifically, HIPAA protections apply unless the organization removes 18 types of identifiers (the "Safe Harbor Method," 45 CFR Sect. 164.514(b)(2), 2013) or utilizes the expert determination method to remove identifiers (45 CFR Sect. 164.514(b)(1), 2013). Therefore, when creating a blockchain database, it is important to define the nature of variables that will be collected to determine whether HIPAA regulations apply.

There may be additional federal agency regulations (e.g., Department of Defense or Department of Justice), state statutes, or organizational rules when creating a database for future research (Riddle, 2018).

Distribution and Usage

Research conducted or supported by HHS The NIH is developing policies to require recipients of NIH funds to supply data that had supported their peer-reviewed publications (National Institutes of Health, 2015). Investigators are particularly interested in receiving access to additional data for analyses and supporting reproducibility of science (Benchoufi and Ravaud, 2017). Further, the NIH plans to ensure that data management plans include clear plans for sharing data in public repositories in machine readable formats (National Institutes of Health, 2015). Therefore, when designing blockchain databases for research supported by the NIH, there should be a mechanism to export data (or provide access to the data) in machine readable format.

When distributing data from a database to researchers, OHRP does not consider the act of providing data to constitute involvement in the research conducted with that data (Office for Human Research Protections, 2008). However, if the owners/operators of the database collaborate on other activities, such as design, interpretation, analysis, or authorship of the research resulting from the data, OHRP would consider these additional activities to constitute involvement in the conduct of that research (Office for Human Research Protections, 2008).

For research funded by the NIH, Certificates of Confidentiality have been issued automatically since 2017 for NIH-funded research collecting or using identifiable, sensitive information (National Institutes of Health, 2017). The Certificate provides additional protections for the privacy of participant names, research information, documents, or biospecimens collected or used in research. When issued a Certificate of Confidentiality, data may only be disclosed when:

- *Required by Federal, State, or local laws (e.g., as required by the Federal Food, Drug, and Cosmetic Act, or state laws requiring the reporting of communicable diseases to State and local health departments), excluding instances of disclosure in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding;*
- *Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual;*
- *Made with the consent of the individual to whom the information, document, or biospecimen pertains; or*
- *Made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research* (National Institutes of Health, 2017).

When sharing identifiable, sensitive data under a Certificate, the entity sharing data must ensure that data recipients must also agree to restrict disclosure of the data—even if their research is not funded directly by the NIH (National Institutes of Health, 2017).

When receiving identifiable data from a blockchain research database, the recipient researchers subject to HHS regulations should write a usage proposal, often called a "secondary use protocol," that describes plans to answer one or more specific research questions and an agreement to protect the data confidentiality (Office for Human Research Protections, 1997).

There will likely be numerous secondary use protocols for each research database. When planning secondary uses of identifiable information, researchers should obtain IRB review and approval prior to obtaining access to the data (Office for Human Research Protections, 2016a, 2018a).

IRB review is not required by regulation, however, when conducting research on de-identified or coded data when the data cannot be linked to the individuals represented in the database, either directly or indirectly with coding systems (Office for Human Research Protections, 2008). Specifically, OHRP does not interpret research involving only coded information to be readily identifiable and therefore would not be defined as human subject research (45 CFR Sect. 46.102(g), 2018) if both of the following are met:

1. *The private information or specimens were not collected specifically for the currently proposed research project through an interaction or intervention with living individuals; and*
2. *The investigator(s) cannot readily ascertain the identity of the individual(s) to whom the coded private information or specimens pertain because, for example:*
    a. *The investigators and the holder of the key enter into an agreement prohibiting the release of the key to the investigators under any circumstances, until the individuals are deceased (note that the HHS regulations do not require the IRB to review and approve this agreement);*
    b. *There are IRB-approved written policies and operating procedures for a repository or data management center that prohibit the release of the key to the investigators under any circumstances, until the individuals are deceased; or*
    c. *There are other legal requirements prohibiting the release of the key to the investigators, until the individuals are deceased* (Office for Human Research Protections, 2008, approximately p. 4).

If a researcher who receives coded information about living individuals learns the identity, or believes it is necessary to identify the individuals, the research would then be subject to human research protection regulations (45 CFR Sect. 46.101, 2018). IRB review of the research would be required. Unless the research is exempt (45 CFR Sect. 46.104(b)(4), 2018), informed consent would be required, but it is most common for IRBs to issue a waiver of informed consent for secondary uses of identifiable information (45 CFR Sect. 46.116(e), 2018).

Research involving PHI When distributing PHI, the covered entity must ensure there is an agreement or assurance in place appropriate for the nature of data being used or disclosed (e.g., participant authorization, data use agreement, business associate agreement, etc.) (National Institutes of Health, 2004a). For PHI that could directly identify an individual, the researchers may obtain authorization from the individuals; but it is customary for a Privacy Board (or an IRB serving as a Privacy Board) to issue a waiver of authorization (National Institutes of Health, 2004a). Research information that has been de-identified by removal of the 18 identifiers (45 CFR Sect. 164.514(b)(2), 2013) or expert determination methods prior to distribution may be used or disclosed without limitation and is not governed by the Privacy Rule (National Institutes of Health, 2004a).

While this section provided regulatory requirements for creation and operations of research databases, researchers may face additional requirements and expectations (Riddle, 2018). We encourage researchers to first check with their IRBs or legal departments to verify local ordinances, state statutes, and institutional policy.

Regulatory Considerations for Electronic Storage Design and Transmission

When designing the backend programming for data storage in a blockchain-based system, certain regulations impose standards for data sharing, electronic storage conditions, and electronic transmissions involving a research database. There are increasing requirements to standardize regulatory data submissions and create standard variable parameters for storing, accessing, and transmitting data within or outside of the database operating framework. Therefore, blockchain design features are becoming increasingly important.

Research Conducted or Supported by HHS

Data Standardization

During a workshop about data sharing, the Institute of Medicine (2013) advocated for data sharing with a focus on data standardization. The IOM noted that standard data elements facilitate data exchange with partners and offer better data integration with other data sets. Accordingly, the NIH has since encouraged use of common data elements (CDEs) for disease registries and other NIH-supported human subject research. CDEs describe the type of data to be collected and provide standardized language or input values. The NIH's goal is to promote data standardization for combining data from multiple sources, including electronic health records. In the NIH CDE online portal, database operators and investigators can find the NIH-supported CDEs (e.g., assessment scales, adverse event reporting, and classification) and resources for developing data fields and protocols to best utilize these CDEs (National Institutes of Health, 2019). Therefore, when designing data fields and definitions for use in blockchain databases, reviewing the NIH CDEs to maximize the value of stored data is recommended.

Electronic Protections

OHRP does not specify any particular method of protecting the integrity of electronic data or data systems, provided that careful attention is used to protect the confidentiality of participants' data (Department of Health and Human Services, 2016). The data management plan should address all methods that will be used to protect confidentiality. Such methods may include coding methods, separation of identifiable information, and protections to prevent inappropriate release of information (Office for Human Research Protections, 2008). With any confidentiality plan, there should be training and supervision of individuals authorized to access the database. An IRB must verify there are adequate provisions to ensure the privacy of subjects and maintain the confidentiality of data (45 CFR Sect. 46.111(a)(7), 2018). Further, 45 CFR Sect. 75.303(a) (2014)

specifies that recipients of NIH-funds must create and maintain policies and procedures that provide appropriate strategies for award management.

Research Regulated by the FDA

The regulation 21 CFR Sect. 11 (2018) defines the criteria by which the FDA considers electronic records and electronic signatures to be reliable and equivalent to paper records. This regulation applies to electronic records represented in digital form created, modified, transmitted, retrieved, or stored under any FDA regulation and for electronic records submitted to the FDA under the Federal Food, Drug, and Cosmetic Act, and the Public Health Service Act, including records not specifically identified in FDA regulations (21 CFR Sect. 11.1(b), 2018).

Data Standards

When designing databases for storing data for FDA submissions, the study data must be presented in a format that is compatible for FDA processing and review (Food and Drug Administration, 2014a). Data standards are provided in the FDA Data Standards Catalog (Food and Drug Administration, 2014a) and the FDA continues to develop standards for pharmaceutical studies (Food and Drug Administration, 2018c). When designing data management systems, the sponsor must determine which standards to select and document the submission plan in a Study Data Standardization Plan. The plan should be located in the investigation plan for Investigational New Drug studies (Food and Drug Administration, 2014a) as the FDA uses this plan to identify standardization issues early in the process.

When electronic data are collected or entered for an FDA-regulated study, data element identifiers (metadata) should be linked to data elements to allow agency staff and other authorized staff to reconstruct the investigation and examine the audit trail (Food and Drug Administration, 2013). While a blockchain database is well-suited to provide an audit trail, it is important to design functionality to access the data element identifiers or produce an audit trail that it is readily available in a human readable format (Food and Drug Administration, 2013).

Electronic Protections

When using electronic systems during an FDA-regulated clinical investigation, sponsors should describe and provide the intended uses in the data management plan or protocol. This description should include a diagram of the electronic data flow and the security measures to protect the electronic records (Food and Drug Administration, 2013) 21 CFR Sect. 11, Subpart B, 2018). There should also be a risk-based assessment that considers data protections and reliability (International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use, 2016).

Both the system designer and organizations using the systems must implement technical controls, administrative controls, and procedural controls (Food and Drug Administration, 2013). As examples, there are stringent electronic protection criteria including audit controls, data backups, access controls, quality controls, and ensuring access to regulatory authorities (Food and Drug Administration, 2013). With regard to technical access controls, the FDA states that a list should be maintained of authorized data originators, which could include systems and devices in addition to research staff or research participants (Food and Drug Administration, 2013). In addition to traditional log-on codes, keys, or passwords for access, the FDA allows electronic thumbprints or other identifiers based on biometrics. Regardless of access method, controls should be in place to ensure that only the intended user could gain access with those credentials (Food and Drug Administration, 2013). A full listing of electronic controls is outside the scope of this article, but resources can be accessed from the FDA website[8] (Food and Drug Administration, 2019c refer to the section on Electronic Data Controls).

Research Involving PHI

As OCR is performing an increasing number of audits (2016) (Office for Civil Rights, 2016) and assessing ever-larger fines and penalties, it is critical to ensure adequate protections and documentation of compliance mechanisms.

Data Standards

To increase interoperability for PHI stored in blockchain databases, the database designers should consult the code sets adopted by HHS for diagnoses, procedures, and treatments. The Centers for Medicare and Medicaid (CMS) include the following code sets: International Classification of Diseases (ICD-10); Healthcare Common Procedure Coding System (HCPCS), Current Procedure Terminology (CPT), Code on Dental Procedures and Nomenclature (CDT), and National Drug Codes (NDC) (Centers for Medicare Medicaid Services, 2018). Links to all coding systems are available on the CMS website[9].

Hash Standards

While OHRP and FDA do not offer hash standards for clinical research data, the National Institute of Standards and Technology (NIST) recommends standards regarding how hashes can be used with PHI. Because blockchain uses cryptography, it is noteworthy how NIST commented on hashes:

> *"De-identified information can be re-identified (rendered distinguishable) by using a code, algorithm, or pseudonym that is assigned to individual records. The code, algorithm, or pseudonym should not be derived from other related information* about the individual, and the means of re-identification should only be known by authorized parties and not disclosed to anyone without the authority to re-identify records. A common de-identification technique for obscuring PII [Personally Identifiable Information] is to use a one-way cryptographic function, also known as a hash function, on the PII.*
>
> **This is not intended to exclude the application of cryptographic hash functions to the information." (McCallister et al., 2010, p. 22).*

OCR specifies that while codes should not be created from PHI for the de-identification provisions in 45 CFR Sect. 164.514(b)(1) (2013), covered entities are not prohibited from transforming

[8]https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-trials-guidance-documents

[9]https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Code-Sets/index.html (2018).

PHI using cryptographic hashes using the expert determination method. However, the keys may not be disclosed to the data recipients (Office for Civil Rights, 2012).

Trusted Exchange Framework and Common Agreement (TEFCA)

The 21st Century Cures Act (2016)[10] includes efforts to promote interoperability of electronic health record systems. Specifically, Title IV of the Cures Act defines the requirement for health IT developers of certified technology to publish application programming interfaces (APIs) to drive access to clinical data. Office of the National Coordinator for Health Information Technology (2019) then developed a Trusted Exchange Framework and Common Agreement (TEFCA) of distinct components for technical and legal requirements for sharing health information. A primary goal is to allow health information to follow the patient and to be accessible when and where it is needed. While TEFCA is still early in development, it is valuable for developers of blockchain databases to be aware that published APIs will be available to connect blockchain databases to other electronic health systems and to design programming using TEFCA standards to maximize interoperability.

Electronic Protections

There are stringent regulatory requirements for protecting PHI in the HIPAA Security Rule (45 CFR Sect. 164, Subpart C, 2013) involving technical safeguards, administrative safeguards, and physical safeguards. Well-suited for blockchain systems, there are regulations for audit controls, encryption requirements for transmitting PHI, and patient access to PHI that would not compromise the integrity of the research (45 CFR Sect. 164.312(a) and (e)(2), 2013). If reasonable and appropriate, there should be encryption to protect PHI during transmission and at rest (Office for Civil Rights, 2017). It is also important to note that individuals have the right to request an amendment of their PHI (45 CFR §164.526 (a)(1), 2013). Therefore, with PHI stored on a blockchain, there should be a mechanism by which the programming would allow a covered entity to append the revised information.

A blockchain-based system alone can only satisfy the vendor's programming requirements for meeting HIPAA safeguards, but the covered entity must also meet responsibilities with each safeguard. For example, to meet the regulatory requirements for access control, integrity, authentication, and transmission security (45 CFR Sect. 164.312(a)–(e), 2013) covered entities must implement policies and procedures to protect against unauthorized access to electronic PHI (Office for Civil Rights, 2013). In addition, while a blockchain stores new data events on a ledger in a manner similar to an audit log, the information must be viewable in a human readable format. The covered entity must also document the blockchain's audit control capabilities and implement policies and procedures to examine the audit logs for unauthorized activities involving electronic PHI [45 C.F.R. Sect. 164.312(b)]. To verify that security standards are effective, covered entities are required to perform comprehensive risk analyses (45 C.F.R. Sect. 164.306, 2013), and detect, report, and document security incidents [45 CFR Sect. 164.308(a)(1)(ii)(D), 2013]. This process requires ongoing effort and cooperation among all parties.

An additional safeguard requirement involves plans for governance and access controls for the blockchain nodes (devices) that will manage the ledgers. All participating entities in the network must validate the data transaction. The data should be accessible to all necessary parties while protecting the PHI in accordance with the governance or encryption strategies (Agbo et al., 2019).

State Laws

States are increasingly addressing data privacy protections and breach notifications in legislation comparable to the European Union's General Data Protection Regulation (2016)[11] and some elements are stricter than HIPAA regulations. For example, the Protections for Consumer Data Privacy Act (Colorado, 2018)[12] requires data breaches to be reported to Colorado residents in 30 days (while HIPAA allows 60 days), and personally identifiable data must be maintained for the shortest period necessary and must be destroyed thereafter. California passed the California Consumer Privacy Act (2018)[13] to provide California residents with more rights regarding uses and sales of their personal information with limited exceptions for research. Therefore, when considering blockchain system data privacy protections, it is important to gain familiarity with a range of state requirements for tracking data usage by individual, reporting breaches, and some states' requirements for data destruction.

Other Design and Storage Considerations

While this article focuses on U.S. regulations and standards, blockchain programmers should also be aware of international efforts to shape standards for blockchain development. The current architectural blockchain choices have been designed largely to advance proprietary interests or security and data integrity, rather than integration with other systems (Anjum et al., 2017). It is unknown whether federal agencies will adopt specific standards, but standardization will be necessary to enable blockchain platforms to be interoperable (Anjum et al., 2017).

The Institute of Electrical and Electronics Engineers (IEEE) has created multiple standards projects to shape the development and adoption of blockchain technologies (IEEE Blockchain, 2019). A healthcare and life sciences working group is developing a common framework for implementation, scalability, and privacy for blockchain interactions (IEEE Standards Association, 2019). As part of its mission, this working group specifies: "*DLT tokens, smart contracts, transactions, assets, networks, off-chain data storage and access architectural patterns, and both permissioned and permission-less DLT are included in the framework*" (IEEE Blockchain, 2019). There are also initiatives

[10] 21st Century Cures Act. Pub. L. 114–225, 130 Stat. 1033 (December 13, 2016).

[11] General Data Protection Regulation, European Parliament and the Council of the European Union, Reg. 2016/679, L. 119/1 (April 27, 2016).

[12] Protections for Consumer Data Privacy, Colorado Revised Statutes, 6-1-713 (May 29, 2018).

[13] California Consumer Privacy Act, California Civil Code, Section 1798.100 (June 28, 2018).

specific to building consensus about the uses of blockchain for clinical trials (IEEE Standards Association, 2018).

Similarly, the International Organization for Standardization (ISO) formed a technical committee (TC) 307 on blockchain and distributed ledger technologies. Within this committee there are working groups to develop standards for terminology (CD 22739), privacy and personally identifiable information protections (DTR 23244), security risks, threats and vulnerabilities (DTR 23245), reference architecture (CD 23257), and interactions between smart contracts in blockchain and distributed ledger technology systems (International Organization for Standardization, 2019). This ISO technical committee has decided to defer creating standards for legally binding smart contracts, digital assets, interoperability, and governance (Anjum et al., 2017; International Organization for Standardization, 2019).

Regulatory Considerations for Informed Consent to Participate in Research or Authorize Use of PHI

Regulations for Uses of Information for Screening and Recruiting

There is great interest in using blockchain-based databases for identifying and screening prospective participants (Angeletti et al., 2017a,b). However, the use of a blockchain-based database to identify prospective participants to participate in clinical research may be subject to regulations and require IRB oversight.

Research Conducted or Supported by HHS

The process of recruiting prospective participants is viewed as the beginning of the informed consent process. Prior to the revised 2018 version of the Common Rule, OHRP required researchers to obtain a waiver of informed consent to determine eligibility or recruit participants without informed consent (Office for Human Research Protections, 2019). However, under the revised Rule, the IRB can approve a recruitment plan in the protocol to obtain information through verbal or written communication with prospective participants or obtain identifiable information by accessing records or storing identifiable specimens (Office for Human Research Protections, 2019). This allows researchers to screen, determine eligibility, and contact prospective participants without informed consent or a waiver of informed consent (45 CFR Sect. 46.116(g), 2018). For these screening and recruiting activities, the 2018 Rule is now consistent with interpretations and guidance of FDA regulations.

Research Regulated by the FDA

An IRB can determine that interacting with prospective participants or identifiable information for screening and recruiting does not require informed consent (21 CFR Sect. 56.109(c), 2018) because informed consent is not normally required for these activities outside of research (Food and Drug Administration, 1998a).

Research Involving PHI

The Privacy Rule allows covered entities to use or disclose PHI for activities "preparatory to research" (45 CFR Sect. 164.512(i)(1)(ii), 2013), which allows researchers to access PHI from medical records or other health sources to determine whether there are enough eligible patients or records to conduct the research or to identify which patients may meet the eligibility criteria for enrollment in a study (National Institutes of Health, 2004b). To access PHI to prepare research, the covered entity must receive verification from the researcher (typically in writing) that the researcher will review PHI only to prepare a protocol/study, that no PHI will be removed from the covered entity during the review, and use of PHI is necessary to prepare the research (45 CFR Sect. 164.512(i)(1)(ii), 2013).

When used for recruitment, the preparatory to research provision allows a researcher to review PHI to identify, but not contact, prospective participants (National Institutes of Health, 2004b). However, the Privacy Rule does provide some conditions by which prospective participants could be contacted:

- If the researcher is a member of the covered entity's workforce or is contracted as a business associate, the researcher may contact the potential participant for the purposes of seeking authorization as part of the covered entity's health care operations.
- If the researcher is a health care provider, he or she may discuss treatment alternatives with his or her patients, which could involve participating in a clinical research study, as part of the patient's treatment.
- If an IRB or Privacy Board has issued a partial waiver of HIPAA Authorization, the covered entity may disclose the necessary PHI to a researcher who is not part of the covered entity so the researcher could contact prospective participants (National Institutes of Health, 2004b).

While the preparatory to research provision is a mechanism by which a covered entity can grant access to PHI for research preparation, researchers should note that this is not the only approval needed. Access to identifiable information for non-exempt human subject research must first be reviewed and approved by an IRB (National Institutes of Health, 2004b).

Regulations for Obtaining Informed Consent From Participants

This section focuses on research where there is interaction with prospective participants to invite them to provide medical records and answer health or behavioral questions for information to be stored and searched in a blockchain. This section also provides regulatory considerations for presenting and retaining informed consent electronically.

When there is a need to collect information that may identify participants, participants may need to be informed about the types of planned research, the risks of providing their information, and whom they should contact if they no longer want their information to be stored in the database or used in secondary use analyses. The nature of informed consent (or opportunities to waive the requirement for informed consent) depends on the risks to participants and the nature of regulatory oversight.

Research Conducted or Supported by HHS

One of the most critical protections for human subjects involves obtaining informed consent before including participants in research. The HHS regulation, 45 CFR Sect. 46, originated from the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). The Belmont report emphasized the importance of providing adequate information for prospective participants to choose what will or will not happen to them.

Informed consent for a particular project Legally effective informed consent must be obtained prior to participation in non-exempt human subject research (including some research databases) and must include all elements listed in 45 CFR Sect. 46.116 (2018). If the research is conducted under a Certificate of Confidentiality, the consent form should specify the protections provided by a Certificate and the limits of protections (National Institutes of Health, 2017).

HHS updated its guidance about informed consent in 2016 to clarify that the written form may be electronic version, provided that the participants (or legally authorized representatives, LARs) are given a copy of the consent document in a form or format that they can retain (Office for Human Research Protections, 2016b). Because some individuals may face challenges with technology, participants should be given the option to review either paper or electronic informed consent information for part or all of the informed consent process (Department of Health and Human Services, 2016).

When obtaining informed consent, OHRP provides guidance about the need to verify the identity of the participant (or LAR) who will be participating in the research. This guidance may be particularly pertinent for remote or internet-based enrollment mechanisms. OHRP recommends that researchers apply a risk-based approach to identity verification (Office for Human Research Protections, 2016b). Generally, the need to verify identity increases with the risks that individuals may face during participation. An IRB may also waive the requirement for informed consent when the research meets specific conditions (45 CFR Sect. 46.116(e) or (f), 2018).

Consent for future uses It is recommended that the informed consent document contains language enabling participants to opt-in or opt-out of storage of their data for future research purposes. The revised Common Rule also allows a new type of informed consent, called "broad consent," to allow management or use of identifiable information or biospecimens intended for secondary research (45 CFR Sect. 46.116(d), 2018). Under this provision, individuals can allow their current research information or clinical health information to be used for future research, not part of the current study (Office for Human Research Protections, 2019).

The broad consent form includes most of the same elements required for a research study (45 CFR Sect. 46.116(a), 2018), but also describes the types of research that may be performed in sufficient detail that the future research would fall within the description. Briefly, additional elements require a description of the private information that could be included, if these could be shared (and with whom), how long information or specimens may be stored (45 CFR Sect. 46.116(d)(2)-(4), 2018). As appropriate, participants should be told that they will not be informed when their information or biospecimens are used in specific research studies and that research results—including clinically-relevant information—might not be shared with them (45 CFR Sect. 46.116(d)(5)-(6), 2018). Last, the broad consent must include information about whom to contact with questions about: rights as a research participant, questions about storage and use, and research-related harms (45 CFR Sect. 46.116(d)(7), 2018). While an IRB can approve a waiver or alteration of some of the general or basic elements of informed consent, an IRB cannot waive or alter the elements for broad consent (Office for Human Research Protections, 2019).

A primary difficulty of obtaining broad consent for future or secondary research is the necessity to honor the individual's consent or refusal to some or all types of research (Office for Human Research Protections, 2019). An IRB cannot override the individual's refusal. However, secondary research may be performed if the individual's data are not identifiable, which is outside of the scope of the Common Rule (Office for Human Research Protections, 2016a). Therefore, if conducting secondary research based on broad consent with a blockchain database, it is imperative to design programming, such as smart contracts, to manage participants' consent or refusal to some or all types of research involving identifiable private information. The smart contracts could also withhold identifiable information and apply coding, when required, so that the secondary research would no longer be regulated by the Common Rule.

Child research participants who reach the age of majority If parents or guardians initially provide parental permission for children to participate in research—including research databases—OHRP expects that when the children reach the age of majority, the children-turned-adults must be asked to provide their own informed consent for remaining in the research activity (Office for Human Research Protections, 2018b). An IRB could also waive this requirement (45 CFR Sect. 46.116(e) or (f), 2018).

Research Subject to FDA Regulations

Informed consent must be documented by a written consent form (or an electronic form) that contains basic elements nearly identical (21 CFR Sect. 50.25, 2018) to those required by OHRP. The individual signing the consent form must receive a copy of the form (21 CFR Sect. 50.27(a), 2018) and an electronic copy would also meet this requirement. While FDA regulations do not specify that the subject receive a copy of the form that was signed, the FDA recommends providing a copy of the signed version (Food and Drug Administration, 2014b). Further, for research no greater than minimal risk, such as research using medical records or secondary research consistent with the drive toward real-world evidence (Food and Drug Administration, 2019b), the FDA will now exercise enforcement discretion when an IRB waives the requirement for informed consent or documentation of informed consent (Food and Drug Administration, 2017b).

As online and remote participation in FDA-regulated trials is becoming a viable method of expanding access to clinical

investigations, the investigator remains responsible for ensuring legally-effective informed consent. If using websites or electronic media to provide research-specific information, the content should also be available in a printed paper version (Food and Drug Administration, 2017b).

If the consent process is not personally witnessed by the research team, there must be a method to verify that the individual providing consent is the same person (or the LAR for the person) who will be participating in the research (21 CFR Sect. 11.100(b), 2018). The researchers must first verify the identity of the individual before allowing or certifying any element of the individual's electronic signature (see 21 CFR Sect. 11.100(b), 2018). Verification methods may include reviewing government-issued identification, biometric methods, videoconferencing, and use of personal questions or security questions (Department of Health and Human Services, 2016). Investigators are not permitted to delegate this responsibility to an electronic system (Department of Health and Human Services, 2016).

Child research participants who reach the age of majority If a child participant reaches the legal age of majority during research—including participation in databases—the investigator must obtain the informed consent of the child-turned-adult (21 CFR Sect. 50, subpart B, 2018)[14] prior to performing any additional research activities involving that participant (Food and Drug Administration, 2014b) 21 CFR Sect. 50.20, 2018). The IRB may waive this requirement for research no greater than minimal risk, such as for the investigator's continued or secondary analysis of identifiable information in a database (Food and Drug Administration, 2017b).

Research Involving PHI

Authorization to use PHI for a particular project Authorization to use an individual's PHI for a research project must be documented with a written authorization form (or an electronic authorization form). The authorization information must be in plain language and describe the nature of the PHI to be used in a specific and meaningful manner containing all of the required elements (45 CFR Sect. 164.508(c), 2013). After a research participant signs an authorization form, the covered entity must provide the participant with a copy of the signed authorization form (45 CFR Sect. 164.508(c)(4), 2013), which could be an electronic version of the signed form.

Authorization to future use of PHI for undetermined research Unlike research involving a specific project with a clear scope where participants must be informed about specific planned uses of their PHI, authorization for future research does not need to list each future study if unknown. This is particularly pertinent when individuals provide authorization for their PHI to be stored in a blockchain-based database for future analyses. Instead, the authorization form must describe the type of future research in such a manner that it would be reasonable for participants to understand and expect that their PHI would be used for future research of that nature (Office for Civil Rights, 2018).

Child research participants who reach the age of majority When child research participants reach the age of majority in a research project—including a research database—the parent's or guardian's authorization for research use and disclosure of the child-turned-adult's PHI remains valid (Office for Civil Rights, 2018). While a child-turned adult gains authority to revoke this authorization, there is no need to obtain re-authorization from the child-turned adult or a waiver of authorization from a privacy board for use or disclosure consistent with the existing authorization (Office for Civil Rights, 2018).

State Statutes

In order for informed consent to be legally effective, the informed consent process and information must be compliant with applicable federal, state, and local laws (Food and Drug Administration, 2014b). While most state statutes specify informed consent content requirements consistent with federal regulations (or remain silent about informed consent content for research), some states require consent elements that exceed federal regulations (Neth, 2016; Fernandez Lynch et al., 2018), such as the California Experimental Subject's Bill of Rights (California Department of Justice, 2018).

States may also specify which individuals are permitted to provide informed consent to participate in research or provide permission for another person to be enrolled in research. First, state laws govern the age of majority for making legal decisions, and some states have an age of majority >18 (FindLaw, 2016). Because state laws with an age of majority >18 years may still confer some rights and responsibilities to individuals at the age of 18, it is important to investigate the laws of the states where informed consent will be obtained. Additionally, U.S. state laws govern control of minors' control of their health information for health activities for which they can provide treatment consent (e.g., access to birth control, testing for sexually transmitted diseases) (Julianelle, 2018). Last, state laws specify how individuals are classified as LARs. It is also important to know that LARs' authority to provide permission may differ for clinical treatment vs. clinical research (DeMartino et al., 2017). Overall, sponsors and investigators should seek legal guidance to ensure they meet specific informed consent requirements for the states where they plan to conduct research.

Considerations of Compensation

When participants are presented with the opportunity to participate in research, it is common to create incentives for initial or ongoing participation. A unique aspect of participation in a blockchain-based database or registry is the possibility of providing incentives with cryptocurrency or utility tokens in lieu of monetary payments. For example, two companies, Embleema and HealthWizz, pay users with virtual tokens for sharing medical data with researchers, providers, and/or pharmaceutical companies (Lovett, 2018). Regardless of equivalent monetary value, there must be consideration of how information about the tokens will be presented to prospective participants during the

[14] 21 CFR Sect. 50 (2018). Protection of Human Subjects.

consent process and how the incentive cryptocurrency/tokens will be valued for compensation and taxation.

Ethical Considerations

Plans for incentive payments are reviewed by the IRB as part of the overall review of the research study. IRBs are charged with determining whether a proposed payment could present an undue influence, impacting prospective participants' ability to make a decision about voluntary participation (21 CFR Sect. 50.20, 2018; 45 CFR Sect. 46.116, 2018). Unlike coercion, which involves perceived pressure to participate, undue influence can occur when there is an excessive offer of payment or reward such that participants may feel that they cannot decline the offer, even when it is not in their best interests to participate in the research (Office for Human Research Protections, 2016b; Food and Drug Administration, 2018d). The IRB requests the amount and schedule of all payments at the time of initial review. Therefore, the investigator must submit his or her method of valuing the cryptocurrency/virtual tokens and ensure a fair approach for all participants. This task becomes complicated if there will be fluctuating value over gradual subject enrollment.

Blockchain companies may also desire to pay participants by providing tokens good for discounts toward purchases of their products once the products are ready for marketing. However, IRBs may raise concern that discounts (or coupons) toward future purchases could create the inappropriate impression that a favorable study outcome is anticipated (Food and Drug Administration, 1998b). Further, participants may feel pressured to purchase the product even if they would not have ordinarily done so.

Federal Tax Obligations

In 2014, the Internal Revenue Service (IRS) provided guidance about tax principles for transactions involving "virtual currency" (Internal Revenue Service, 2014). When a taxpayer receives virtual currency as payment, he or she must include the fair market value of the currency in U.S. dollars on the date of receipt (Internal Revenue Service, 2014). If payments equal or exceed $600 in a calendar year, the payment(s) must be reported to the recipient and IRS on Form 1099-MISC. In the 2019 instructions for Form 1099-MISC, the IRS expanded the criteria in Box 3 to explicitly include the requirement to report "*a payment or series of payments made to individuals for participating in a medical research study or studies*" (Internal Revenue Service, 2019, p. 6).

Institutional Requirements

When enrolling participants from a well-established research organization, it is valuable to consider that the organization may require use of its own consent template. It is common for organizations to require specific wording pertaining to access to patient advocates, contact information for their own IRB, or customized HIPAA authorization language. There may also be policies about the process of obtaining informed consent, use of witnesses and foreign language interpreters, or determining which individuals may serve as LARs for research decisions involving participants who lack decisional capacity (AAHRPP, 2013). Some organizations also insist on processing payments to research participants for budget and grant management purposes (45 CFR Sect. 75, 2014)[15].

Withdrawing Consent or Revoking Authorization

After an individual agrees to participate in research and/or allow their PHI to be used for research, the individual also has the right to change his or her mind. This is a particularly important consideration for research data stored in an immutable blockchain (Tosh et al., 2017).

Research Conducted or Supported by HHS

The informed consent process is based on the principle of voluntary participation, and participants are told that they may "*discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled*" (45 CFR Sect. 46.116(b)(8), 2018). If an individual decides to discontinue participation, the investigator must stop obtaining identifiable private information about that person from every source used for the research (Office for Human Research Protections, 2010). For data that has already been collected from a participant who withdrew (or was terminated by the investigator), OHRP interprets 45 CFR Sect. 46 to permit investigators to keep and analyze those data if consistent with the protocol analyses approved by the IRB (Office for Human Research Protections, 2010). Continued storage and data analysis is allowed even if the subject's information is identifiable and private.

Research Subject to FDA Regulations

Similar to research conducted or supported by HHS, an FDA-compliant consent form informs participants that they may withdraw from participation at any time (21 CFR Sect. 50.25(a)(8), 2018). However, the discontinuation does not affect data that had already been collected up to the point of discontinuation. To ensure that the FDA can perform a complete safety and efficacy evaluation of a regulated project, the FDA has specified by policy that all data collected to the point of participant discontinuation must be retained and included in appropriate analyses (Food and Drug Administration, 2008).

Research Involving PHI

Similar to the concept of the concept of withdrawing informed consent, the Privacy Rule established an individual's right to revoke authorization for uses and disclosures of his or her PHI (45 CFR Sect. 164.508(c)(2), 2013). However, when an individual revokes his or her authorization for research, this does not require removal of data from the database or prevents necessary uses for other purposes. A covered entity or business associate could not collect any additional PHI, but could continue using existing PHI to maintain the integrity of the research (45 CFR Sect. 164.508(b)(5)(i), 2013). As examples, the researchers could still account for the individual's enrollment and withdrawal from the research, maintain existing analyses, and perform quality assurance reviews (Office for Civil Rights, 2018). In a blockchain-based research database, the immutable nature of PHI on-chain would be unlikely to create non-compliance with this HIPAA

[15]45 CFR Sect. 75 (2014). Uniform administrative requirements, cost principles, and audit requirements for HHS awards.

provision, provided that participants are told in advance about the exceptions to revocation and any revocation is noted.

Smart Contracts

Blockchain research databases are likely to include smart contracts programmed to automate processes based on conditional triggers. Smart contracts are not currently addressed in federal research regulations or HIPAA Security regulations, but are increasingly addressed in state legislation regarding the legal authority of electronic transactions using smart contracts (Morton, 2019).

When designing smart contracts for use in blockchain-based research systems, there are some practical challenges in research worth noting. While a person's informed consent could trigger smart contracts to increase efficiency of research operations, research is often a dynamic process whereby protocols, consent forms, or operational steps are amended as needed for safety or scientific purposes. It is important, then, to ensure that smart contracts can also be quickly reprogrammed to implement these amendments. Also, smart contracts are not necessarily "smart." Programmers could make coding mistakes that need to be fixed to ensure the study proceeds as approved (Orcutt, 2018a,b; Swihart et al., 2019). There should be a thorough process of validation testing as well as a mechanism to update code, as needed, to maintain the scientific integrity of the study.

Regulatory Considerations for Electronic Signatures

In 1999, the National Conference of Commissioners on Uniform State Laws (1999) offered the Uniform Electronic Transactions Act (UETA), which clarified components of a legal electronic signature. However, UETA was adopted by only 47 states plus Puerto Rico, the District of Columbia, and the U.S. Virgin Islands (Uniform Law Commission, 2019). To create consistent electronic signature standards across the United States, Congress passed the Electronic Signatures in Global and National Commerce (ESIGN) Act (2000)[16]. This Act required all states to follow provisions of UETA and preempted states from creating their own e-signature laws unless they follow the original version of UETA, or specified alternative procedures or requirements that are consistent with ESIGN (McQuinn and Castro, 2019).

While the terms "electronic signature" and "digital signature" are often used synonymously, there are some subtle differences. An electronic signature is defined by UETA as "*electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record*" (1999, p. 5) and by the FDA as "*a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature*" (21 CFR Sect. 11.3(b)(7), 2018). There is no requirement for use of any particular technology, but there should be controls to verify intent and that the signature is unique to a specific individual.

[16]Electronic Signatures in Global and National Commerce Act. Pub. L. 106–229, 114 Stat. 464 (June 30, 2000).

NIST defines a digital signature is a form of electronic signature where:

> *. . . a set of rules and a set of parameters allow the identity of the signatory and the integrity of the data to be verified. Digital signatures may be generated on both stored and transmitted data. Signature generation uses a private key to generate a digital signature; signature verification uses a public key that corresponds to, but is not the same as, the private key. Each signatory possesses a private and public key pair. Public keys may be known by the public; private keys are kept secret. Anyone can verify the signature by employing the signatory's public key. Only the user that possesses the private key can perform signature generation* (National Institute of Standards and Technology, 2013, p. i).

In the U.S., the ESIGN Act (2000) provides the national legal basis to accept electronic signatures as a substitute for paper signatures, which is the basis for OHRP and HIPAA regulations allowing electronic signatures. However, systems subject to FDA regulations should ensure compliance with all requirements in 21 CFR Sect. 11, Subpart C (2018).

Research Conducted or Supported by HHS

Electronic signatures are allowed if the signatures are legally authorized in the jurisdiction where the research will be conducted (Office for Human Research Protections, 2016b). If the electronic signature is properly and legally obtained, the research record containing the signature can be used as the original version for purposes of research recordkeeping (Office for Human Research Protections, 2016b). OHRP does not specify any technologies or methods by which electronic signatures can be created. Instead, OHRP has entrusted IRBs with reviewing planned use of electronic signatures by considering the technology by which signatures are created and authenticated, and if (for human research participation) a paper consent/permission form can be generated for review by the participant or LAR (Office for Human Research Protections, 2016b). Because the appropriate use of electronic signatures in HHS-sponsored research depends on the jurisdiction where the research is conducted, OHRP cautions organizations, researchers and IRBs to remain aware of relevant laws for electronic signatures in those jurisdictions (Office for Human Research Protections, 2016b).

Research Regulated by the FDA

The FDA allows electronic signatures be equivalent to handwritten signatures if the system complies with all requirements under 21 CFR Sect. 11.10 (2018). The regulations in this regulation allow many different methods or technologies to create electronic signatures, including username and password combinations, ID cards, and biometrics; but many research systems meet the standards for digital signatures (Food and Drug Administration, 2014a). If electronic signatures are used to sign informed consent forms, copies provided to the participant (or LAR) could be paper or electronic, and an electronic version could be provided by email or on a storage device.

If using biometrics for an electronic signature, the FDA doesn't specify any particular biometric method (Food and

Drug Administration, 2017a). The biometrics should be uniquely identified with the participant and must be designed in such a manner that they cannot be used by anyone else (21 CFR Sect. 11.200(b), 2018). Also, biometric electronic signatures must also include the details associated with the signing (21 CFR Sect. 11.50(a), 2018), must be linked to the signed electronic records (see 21 CFR Sect. 11.70, 2018), and must be available in any human readable format of the research record [21 CFR Sect. 11.50(b)] (Food and Drug Administration, 2017b).

When evaluating electronic signature methods to obtain informed consent in FDA-regulated clinical research, organizations, IRBs, and investigators should consider how they will meet their responsibilities to fulfill their portions of the administrative, procedural, and technical controls. The FDA allows these parties to rely on the system vendor's assertion how signatures are created and that the system meets the technical requirements of 21 CFR Sect. 11, but the vendor, organization, and investigators have responsibilities for creating documentation of controls, and implementing policies for training, identity verification, and ongoing maintenance (Food and Drug Administration, 2017a).

Research Involving PHI

HIPAA authorizations for use of PHI for research can be obtained electronically if the electronic signature is valid under applicable laws (Office for Civil Rights, 2008). Most organizations follow electronic signature standards that comply with National Institute of Standards and Technology (2013) guidelines for cryptographic algorithms, key establishment, and cryptographic key generation; however, HIPAA does not require a particular methodology and the requirements are intended to be technology neutral (Office for Civil Rights, 2013). Further, Office for Civil Rights (2013) expects that electronic signatures will be covered in the organization's security documentation and risk assessments.

Legality of Blockchain Signatures

The more technical and secure method of a digital signature (as opposed to an electronic signature) is most similar to the nature of blockchain technology, as the blockchain stores validation information with each event, such as a date/time stamp and identify of the person. National Institute of Standards and Technology (2013) has published many standards pertaining to secure hashes and public/private key cryptography. Even though it seems that blockchains meet a higher technical standard of electronic signature, there is still uncertainty about their legality. To give blockchain signatures legal certainty, a few states, such as Delaware and Arizona, have passed laws ensuring the legitimacy of blockchain records and signatures (Svikhart, 2017; McQuinn and Castro, 2019).

ASSESSMENT OF POLICY/GUIDELINES OPTIONS AND IMPLICATIONS

Actionable Recommendations

Because blockchain for clinical research offers many attractive features, blockchain is gaining substantial interest and momentum in the United States and internationally (Agbo et al., 2019). As with many developing technologies, it is difficult for regulatory agencies to keep pace with regulatory assessments and guidance on blockchain. Hence, we recommend several legal, regulatory, and logistical issues that should be addressed in order for blockchain developers and clinical researchers to create a clearer path for implementation and compliance.

1. **Education for researchers and regulators.** Blockchain developers and operators who are new to health and research regulations need education on regulatory basics (Kakavand et al., 2017). One of the primary goals of this paper is to provide an outline and entry to that education. Further detail can be gained through appropriate organization training. Regulators also need education on blockchain technology: what it is, what it is not, and what it can do for research and compliance.
2. **Engagement between researchers and regulators.** Researchers and regulators should engage in early and open dialogue to allow the plans of the research groups to be informed by the regulators and to ensure compliance in their blockchain design. Regulators can be involved in shaping this design as well as shaping their own interpretations of the technology in regulatory determination and future policy.
3. **Sandbox for design and development.** Researchers and regulators should continue engagement in sandboxed regulatory and technology environments where goals, plans, and concerns can be mutually discussed and the best pathway forward agreed upon as the technology is developed. This will be the most effective way of achieving research goals in compliance with regulatory constraints.
4. **Administrative blockchain pilots.** Blockchain developers and operators should design, develop, and run administrative pilots (i.e., with policies and regulatory documentation) to advance capabilities and problem identification before any use of identifiable information. This will additionally allow regulators to see the value of the technology while gaining familiarity and comfort.
5. **Clinical research pilots.** Blockchain developers and operators should run clinical research pilots previously designed in a regulatory and technology sandbox environment. Ideally, early pilot projects should contain multiple sites in order to maximize the value of the application of the technology and to foster cross site research and regulatory dialogue.
6. **Clear and consistent data privacy protections**. National legislators should evaluate and potentially override the patchwork of confusing and sometimes contradictory state-level consumer protection requirements that may prevent uses of immutable ledger technologies. Policymakers should generate privacy legislation that offers strong electronic protections but doesn't hinder technological innovation.
7. **Interoperability standards**. To promote interoperability of blockchain solutions for clinical research and health care data, there must be standardization of data format, structure, authentication, validation, transmissions, and security. While standards are being developed, we encourage regulatory agencies to bring together market players across

blockchain industry sectors for bi-directional participation in interoperability standards.

DISCUSSION

Blockchain publications to date have generally focused on the technical components of blockchain performance (Agbo et al., 2019), and publications pertaining to clinical research describe the promise and pilot testing of use cases (e.g., Nugent et al., 2016; Risius and Spohrer, 2017; Shae and Tsai, 2017; Dai et al., 2018). There have been few discussions of the regulatory framework in which the blockchains would operate. Throughout this article, we have encouraged blockchain developers, operators, and researchers to build the regulatory compliance requirements into their processes so they can meet required controls and safeguards. Further, when blockchain systems are used to collect, store, and distribute data for research purposes, regulatory agencies also expect detailed compliance documentation, such as initial and ongoing testing, validation, methods for updates and upgrades, training, physical security, access controls, and policies that pertain to all of these things. Blockchain developers should also provide appropriate documentation to organizations using the technology for the organizations' due diligence.

While blockchain has the potential to solve many technical challenges in clinical research, blockchain will not solve all research challenges. First, blockchain is not intended to replace central databases used in clinical research. Research participants and research staff make many data entry errors, reflecting the conundrum of "garbage in, garbage out" (Learney, 2019). To ensure that research data are accurate, blockchain prototypes are exploring integrating the immutable blockchains with other off-chain database systems (Shae and Tsai, 2017; Dai et al., 2018; Maslove et al., 2018) where stored data, such as images, are linked to the chain by uniform resource locators (Patel, 2018). Additionally, many emerging clinical research blockchain applications are not yet addressing the data standardization and scalability available in traditional databases (McGhin et al., 2019). Last, as we have pointed out in this article, as developers are racing to create blockchain applications, they have been slow to design legal and regulatory requirements into the design plans (Kakavand et al., 2017).

Due to the multiple entities that must collaborate, create policies and training, and document ongoing updates, testing and validations necessary to achieve regulatory compliance, we caution blockchain developers and operators that there is no such thing as a "HIPAA Compliant" or "FDA Part 11 Compliant" product (Reinhardt, 2019). At best, a vendor can accurately promote a product as being "capable of supporting" or "compatible with" the covered entity's or organization's efforts toward compliance. In the words of Reinhardt (2019):*"It's much easier [for vendors] to say 'Our cloud-based software is HIPAA compliant' than to say 'As a Business Associate, we adhere to all the rules and regulations of HIPAA and HITECH and will sign a Business Associate Agreement with you in order to help you maintain compliance as a Covered Entity. There are, of course, multiple other things you need to do to maintain compliance that we can't necessarily help you with."'* We urge all parties to be vigilant about their regulatory responsibilities and communicate these responsibilities accurately.

In conclusion, blockchain for clinical research involves a promising set of technologies that may advance data integrity and efficiencies in clinical research. However, blockchain-based technologies cannot be used or adopted for regulated clinical research unless they can demonstrate compliance with the applicable regulations. We encourage blockchain developers, operators, research organizations, investigators, and IRBs to become more familiar with the necessary regulatory requirements for blockchain in clinical research and build these into the programming and policies, as appropriate. Compliance is not a one-time effort, but requires ongoing communication, testing, validations, and risk assessments to ensure appropriate protections of human subjects.

DEFINITIONS

Authorization: A detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual (45 CFR Sect. 164.508).

Biometrics: "A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable" [21 CFR Sect. 11.3(b)(3)].

Blockchain: A distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules (Yaga et al., 2018).

Business Associate: "A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity" (45 CFR Sect. 160.103).

Certificate of Confidentiality: "Protect the privacy of research subjects by prohibiting disclosure of identifiable, sensitive research information to anyone not connected to the research except when the subject consents or in a few other specific situations" (National Institutes of Health, 2019).

Covered entity: "A health plan, health care clearinghouse, and health care providers that transmit health information electronically for defined HIPAA transactions, such as claims or eligibility inquiries" (45 CFR Sect. 160.102).

Digital signature: A form of electronic signature where a set of rules and a set of parameters allow the identity of the signatory and the integrity of the data to be verified. "Signature generation

uses a private key to generate a digital signature; signature verification uses a public key that corresponds to, but is not the same as, the private key. Anyone can verify the signature by employing the signatory's public key. Only the user that possesses the private key can perform signature generation" (National Institute of Standards and Technology, 2013, p. i).

Electronic signature:

- UETA: "An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record" (1999).
- FDA: "A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature" [21 CFR Sect. 11.3(b)(7)].

Hashing: "A method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, text, or image). It allows individuals to independently take input data, hash that data, and derive the same result—proving that there was no change in the data. Even the smallest change to the input (e.g., changing a single bit, such as adding a comma) will result in a completely different output digest" (Yaga et al., 2018).

Identifiable private information: "Private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information" [45 CFR Sect. 46.102(e)(5)].

Institutional Review Board (IRB): "Any board, committee, or other group formally designated by an institution to review biomedical research involving humans as subjects, to approve the initiation of, and conduct periodic review of such research" [21 CFR Sect. 50.3(i)].

Legally authorized representative (LAR): "An individual or judicial or other body authorized under applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure(s) involved in the research" [21 CFR Sect. 50.3(l)].

Protected health information (PHI): "Individually identifiable health information transmitted or held by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral" (45 CFR Sect. 160.103).

Secondary research: "Research with materials originally obtained for non-research purposes or for research other than the current research proposal. The exemption can only be used when there is broad consent from the subjects for the storage, maintenance, and secondary research use of their identifiable materials" (Office for Human Research Protections, 2018a).

Smart contract: "A collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network." "The smart contract is executed by nodes within the blockchain network; all nodes must derive the same results for the execution, and the results of execution are recorded on the blockchain" (Yaga et al., 2018, p. 32).

AUTHOR CONTRIBUTIONS

All authors contributed to conception and design of the manuscript, manuscript revision, and approved the submitted version. WC organized the literature and wrote the first draft of the manuscript. NM and SM wrote and edited sections of the manuscript. LL edited the manuscript.

ACKNOWLEDGMENTS

We would like to gratefully acknowledge the expert regulatory interpretations of Jeffrey Cooper, M.D. at WIRB Copernicus Group Clinical that shaped our wording precision and direction. We are also thankful for the contributions of Leah Farrell-Carnahan, Ph.D., Loretta Polite, and John Reusing, who aided the initial efforts of the authors.

REFERENCES

AAHRPP (2013). *Tip Sheet 26: Reviewing Research Involving Adult Participants With Diminished Functional Abilities*. Washington, DC: Association for the Accreditation of Human Research Protection Programs, Inc. Available online at: http://www.aahrpp.org/TipSheetDownload.ashx?fileName=Tip_Sheet_26_Reviewing_Research_Involving_Adult_Participants_with_Diminished_Functional_Abilities.pdf (accessed July 13, 2019).

AAHRPP (2017). *Tip Sheet 2: Determining Whether an Activity Is Research Involving Human Participants*. Washington, DC: Association for the Accreditation of Human Research Protection Programs, Inc. Available online at: https://admin.aahrpp.org/Website%20Documents/Tip_Sheet_2_Determining_Whether_an%20_Activity_is_Research_Involving_Human_Participants.PDF (accessed June 21, 2019).

Agbo, C.C., Mahmoud, H.Q., and Eklund, M.J. (2019). Blockchain technology in healthcare: a systematic review. *Healthcare* 7:56. doi: 10.3390/healthcare7020056.

Angeletti, F., Chatzigiannakis, I., and Vitaletti, A. (2017a). "Privacy preserving data management in recruiting participants for digital clinical trials," in *Proceedings of the First International Workshop on Human-Centered Sensing, Networking, and Systems* (New York, NY: ACM), 7–12. doi: 10.1145/3144730.3144733

Angeletti, F., Chatzigiannakis, I., and Vitaletti, A. (2017b). "The role of blockchain and IoT in recruiting participants for digital clinical trials," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, eds. D. Begušic and International Conference on Software Telecommunications and Computer Networks & IEEE Communications Society (Piscataway, NJ: IEEE Communications Society). doi: 10.23919/SOFTCOM.2017.8115590

Anjum, A., Sporny, M., and Sill, A. (2017). Blockchain standards for compliance and trust. *IEEE Cloud Comput.* 4, 84–90. doi: 10.1109/MCC.2017.3791019.

Benchoufi, M., Porcher, R., and Ravaud, P. (2018). Blockchain protocols in clinical trials: transparency and traceability of consent. *F1000Res* 6:66. doi: 10.12688/f1000research.10531.5

Benchoufi, M., and Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials* 18:335. doi: 10.1186/s13063-017-2035-z.

California Department of Justice (2018). *Informed Consent Form (ICF) Checklist (human research) Requirements From California Health & Safety Code 24173 et. Seq and Title 45 CFR Part 46.* Available online at: https://oag.ca.gov/sites/all/files/agweb/pdfs/research/consent-checklist.pdf (accessed June 19, 2019).

Centers for Medicare and Medicaid Services (2018). *Code Sets Overview*. Baltimore, MD. Available online at: https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Code-Sets/index.html (accessed June 27, 2019).

Chamber of Digital Commerce (2018). *"Smart Contracts" Legal Primer*. Washington, DC.

Choudhury, O., Dhuliawala, M., Fay, N., Rudolph, N., Sylla, I., Fairoza, N., et al. (2018a). *Auto-Translation of Regulatory Documents Into Smart Contracts*. IEEE Blockchain Technical Briefs. Available online at: https://blockchain.ieee.org/newsletter/september-2018/auto-translation-of-regulatory-documents-into-smart-contracts (accessed October 23, 2018).

Choudhury, O., Sarker, H., Rudolph, N., Foreman, M., Fay, N., Dhuliawala, M., et al. (2018b). Enforcing human subject regulations using blockchain and smart contracts. *Blockchain Healthc. Today* 1:14. doi: 10.30953/bhty.v1.10.

Cirilli, D. (2019). *The FDA and Flatiron Health Expand Real-World Data Cancer Research Collaboration*. New York, NY. Available online at: https://flatiron.com/press/press-release/the-fda-and-flatiron-health-expand-real-world-data-cancer-research-collaboration/ (accessed June 22, 2019).

Dai, H., Young, H.P., Durant, T.J.S., Gong, G., Kang, M., Krumholz, H.M., et al. (2018). TrialChain: a blockchain-based platform to validate data integrity in large, biomedical research studies. *arXiv*, 1807.03662. Available online at: https://arxiv.org/abs/1807.03662

De Filippi, P., and Hassan, S. (2016). Blockchain technology as a regulatory technology: from code is law to law is code. *First Monday* 21. doi: 10.5210/fm.v21i12.7113

DeMartino, E.S., Dudzinski, D.M., Doyle, C.K., Sperry, B.P., Gregory, S.E., Siegler, M., et al. (2017). Who decides when a patient can't? Statutes on alternate decision makers. *N. Engl. J. Med.* 376, 1478. doi: 10.1056/NEJMms1611497

Department of Health and Human Services (2009). HIPAA administrative simplification: enforcement *Fed. Regist.* 74, 56123–56131. Available online at: https://www.federalregister.gov/documents/2009/10/30/E9-26203/hipaa-administrative-simplification-enforcement

Department of Health and Human Services (2016). *Use of Electronic Informed Consent in Clinical Investigations - Questions and Answers: Guidance for Institutional Review Boards, Investigators, and Sponsors.* Available online at: https://www.fda.gov/media/105557/download (accessed June 14, 2019).

Dokholyan, R.S., Muhlbaier, L.H., Falletta, J.M., Jacobs, J.P., Shahian, D., Haan, C.K., et al. (2009). Regulatory and ethical considerations for linking clinical and administrative databases. *Am. Heart J.* 157, 971–982. doi: 10.1016/j.ahj.2009.03.023.

Efanov, D., and Roschin, P. (2018). "The all-pervasiveness of the blockchain technology," in *8th Annual International Conference on Biologically Inspired Cognitive Architectures*, eds A. V. Samsonovich and V. V. Klimov (Moscow: Procedia Computer Science), 116–121. doi: 10.1016/j.procs.2018.01.019

Fernandez Lynch, H., Joffe, S., and Feldman, E.A. (2018). Informed consent and the role of the treating physician. *N. Engl. J. Med.* 378, 2433–2438. doi: 10.1056/NEJMhle1800071.

FindLaw (2016). *State Legal Ages Laws*. Thomson Reuters. Available online at: https://statelaws.findlaw.com/family-laws/legal-ages.html (accessed June 15, 2019).

Food and Drug Administration (1998a). *Screening Tests Prior to Study Enrollment*. Rockville, MD. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/screening-tests-prior-study-enrollment (accessed June 15, 2019).

Food and Drug Administration (1998b). *Institutional Review Boards Frequently Asked Questions: Guidance for Institutional Review Boards and Clinical Investigators*. Rockville, MD. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/institutional-review-boards-frequently-asked-questions (accessed June 9, 2019).

Food and Drug Administration (2008). *Guidance for Sponsors, Clinical Investigators, and IRBs: Data Retention When Subjects Withdraw From FDA-Regulated Clinical Trials*. Rockville, MD. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-retention-when-subjects-withdraw-fda-regulated-clinical-trials (accessed June 19, 2019).

Food and Drug Administration (2013). *Electronic Source Data in Clinical Investigations*. Silver Spring, MD. Available online at: https://www.fda.gov/media/85183/download (accessed June 14, 2019).

Food and Drug Administration (2014a). *Providing Regulatory Submissions in Electronic Format — Standardized Study Data: Guidance for Industry*. Silver Spring, MD. Available online at: https://www.fda.gov/media/82716/download (accessed June 14, 2019).

Food and Drug Administration (2014b). *Informed Consent: Guidance for IRBs, Clinical Investigators, and Sponsors*. Silver Spring, MD. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/informed-consent#children (accessed June 8, 2019).

Food and Drug Administration (2017a). *Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 - Questions and Answers: Guidance for Industry (draft)*. Silver Spring, MD. Available online at: https://www.fda.gov/media/105557/download (accessed June 14, 2019).

Food and Drug Administration (2017b). *IRB Waiver or Alteration of Informed Consent for Clinical Investigations Involving No More Than Minimal Risk to Human Subjects: Guidance for Sponsors, Investigators, and Institutional Review Boards*. Silver Spring, MD. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/irb-waiver-or-alteration-informed-consent-clinical-investigations-involving-no-more-minimal-risk (accessed June 14, 2019).

Food and Drug Administration (2018a). *Impact of Certain Provisions of the Revised Common Rule on FDA-Regulated Clinical Investigations: Guidance for Sponsors, Investigators, and Institutional Review Boards*. Silver Spring, MD. Available online at: https://www.regulations.gov/contentStreamer?documentId=FDA-2018-D-3551-0001&attachmentNumber=1&contentType=pdf (accessed June 8, 2019).

Food and Drug Administration (2018b). *Regulations: Good Clinical Practice and Clinical Trials*. Available online at: https://www.fda.gov/science-research/clinical-trials-and-human-subject-protection/regulations-good-clinical-practice-and-clinical-trials (accessed June 8, 2019).

Food and Drug Administration (2018c). Standardized data for pharmaceutical quality/chemistry manufacturing and control; public meeting. *Fed. Regist.* 83 FR 42506, 42506–42507. Available online at: https://www.federalregister.gov/documents/2018/08/22/2018-18080/standardized-data-for-pharmaceutical-qualitychemistry-manufacturing-and-control-public-meeting

Food and Drug Administration (2018d). *Payment and Reimbursement to Research Subjects*. Rockville, MD. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/payment-and-reimbursement-research-subjects (accessed June 14, 2019).

Food and Drug Administration (2019a). *Medical Device Databases*. Available online at: https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/medical-device-databases (accessed July 20, 2019).

Food and Drug Administration (2019b). *Submitting Documents Using Real-World Data and Real-World Evidence to FDA for Drugs and Biologics: DRAFT Guidance for Industry*. Silver Spring, MD: U.S. Department of Health and Human Services. Available online at: https://www.fda.gov/media/124795/download (accessed May 10, 2019).

Food and Drug Administration (2019c). *Clinical Trials Guidance Documents*. Available online at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-trials-guidance-documents (accessed July 14, 2019).

Gibbons, S.M.C., Kaye, J., Smart, A., Heeney, C., and Parker, M. (2007). Governing genetic databases: challenges facing research regulation and practice. *J.L. Soc.* 34, 163–189. doi: 10.1111/j.1467-6478.2007.00387.x

Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V., and Akella, V. (2019). Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inf. Manag.* 49, 114–129. doi: 10.1016/j.ijinfomgt.2019.02.005

IEEE Blockchain (2019). *Standards*. Piscataway, NJ. Available online at: https://blockchain.ieee.org/standards (accessed June 29, 2019).

IEEE Standards Association (2018). *IEEE Initiative to Build Consensus on Optimizing Clinical Trials and Enhancing Patient Safety With Blockchain*. Piscataway, NJ. Available online at: https://standards.ieee.org/news/2018/blockchain_clinical_trials_forum.html (accessed June 29, 2019).

IEEE Standards Association (2019). *P2418.6 - Standard for Blockchain for Healthcare and Life Sciences*. Piscataway, NJ. Available online at: https://standards.ieee.org/project/2418_6.html (accessed June 29, 2019).

Institute of Medicine (2013). *Sharing Clinical Research Data: Workshop Summary*. Washington, DC: National Academies Press.

Internal Revenue Service (2014). *Notice 2014-21: Taxation of Virtual Currency*.

Internal Revenue Service (2019). *Instructions for Form 1099-MISC*.

International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use (2016). *ICH Harmonized Guideline Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2)*. Geneva, Switzerland.

International Organization for Standardization (2019). *ISO/TC 307: Blockchain and Distributed Ledger Technologies. Standards Catalogue*. Available online at: https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0 (accessed June 29, 2019).

Julianelle, P. (2018). *State Laws on Minor Consent for Routine Medical Care*. School House Connection. Available online at: https://www.schoolhouseconnection.org/state-laws-on-minor-consent-for-routine-medical-care/ (accessed June 15, 2019).

Kakavand, H., Kost De Sevres, N., and Chilton, B. (2017). The blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies. *SSRN* doi: 10.2139/ssrn.2849251

Karame, G., and Capkun, S. (2018). Blockchain security and privacy. *IEEE Secur. Priv.* 16, 11–12. doi: 10.1109/MSP.2018.3111241

Kohen, M.E., and Wales, J.S. (2019). *State Regulations on Virtual Currency and Blockchain Technologies*. Available online at: https://www.carltonfields.com/insights/publications/2018/state-regulations-on-virtual-currency-and-blockchain-technologies (accessed June 10, 2019).

Learney, R. (2019). "Blockchain in clinical trials," in *Blockchain in Healthcare: Innovations That Empower Patients, Connect Professionals and Improve Care, 1st Edn,* eds D. Metcalf, J. Bass, M. Hooper, A. Cahana, and V. Dhillon (Orlando, FL: Merging Traffic), 87–108.

Lovett, L. (2018). *10 Digital Health Companies Using Cryptocurrency as Incentives*. mobihealthnews. Available online at: https://www.mobihealthnews.com/content/10-digital-health-companies-using-cryptocurrency-incentives (accessed June 14, 2019).

Maslove, D.M., Klein, J., Brohman, K., and Martin, P. (2018). Using blockchain technology to manage clinical trials data: a proof-of-concept study. *JMIR Med. Inform.* 6:e11949. doi: 10.2196/11949.

McCallister, E., Grance, T., and Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* National Institute of Standards and Technology. Report number: 800–122. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-122

McGhin, T., Choo, K.K.R., Liu, C.Z., and He, D. (2019). Blockchain in healthcare applications: research challenges and opportunities. *J. Netw. Comput. Appl.* 135, 62–75. doi: 10.1016/j.jnca.2019.02.027.

McQuinn, A., and Castro, D. (2019). *A Policymaker's Guide to Blockchain*. Washington, DC: Information Technology & Innovation Foundation.

Morton, H. (2019). *Blockchain State Legislation*. Denver, CO: National Conference of State Legislatures. Available online at: http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx (accessed June 10, 2019).

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1979). *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. Washington, DC: U.S. Government Printing Office.

National Conference of Commissioners on Uniform State Laws (1999). *Uniform Electronic Transaction Act*.

National Institute of Standards and Technology (2013). *Digital Signature Standard (DSS)*. Gaithersburg, MD: Information Technology Laboratory.

National Institutes of Health (2004a). *Research Repositories, Databases, and the HIPAA Privacy Rule*. Department of Health and Human Services. Available online at: https://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf (accessed November 18, 2018).

National Institutes of Health (2004b). *Clinical Research and the HIPAA Privacy Rule*. Department of Health and Human Services. Available online at: https://privacyruleandresearch.nih.gov/clin_research.asp (accessed November 18, 2018).

National Institutes of Health (2015). *Plan for Increasing Access to Scientific Publications and Digital Scientific Data From NIH Funded Scientific Research*. Bethesda, MD. Available online at: https://grants.nih.gov/grants/NIH-Public-Access-Plan.pdf (accessed June 15, 2019).

National Institutes of Health (2017). *Notice of Changes to NIH Policy for Issuing Certificates of Confidentiality*. Bethesda, MD. Available online at: https://grants.nih.gov/grants/guide/notice-files/NOT-OD-17-109.html (accessed June 26, 2019).

National Institutes of Health (2019). *Common Data Element (CDE) Resource Portal*. Bethesda, MD: National Library of Medicine. Available online at: https://www.nlm.nih.gov/cde/ (accessed June 15, 2019).

Neth, K. (2016). *The United States of Consent: Mapping State-Specific Consent Form Requirements*. Seattle, WA: Quorum Review. Available online at: https://www.quorumreview.com/the-united-states-of-consent-mapping-state-specific-consent-form-requirements/ (accessed June 15, 2019).

Nugent, T., Upton, D., and Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Res* 5:2541. doi: 10.12688/f1000research.9756.1.

Office for Civil Rights (2002). *Is a Software Vendor a Business Associate of a Covered Entity?*. Washington, DC. Available online at: https://www.hhs.gov/hipaa/for-professionals/faq/256/is-software-vendor-business-associate/index.html (accessed June 30, 2019).

Office for Civil Rights (2008). *How Do HIPAA Authorizations Apply to an Electronic Health Information Exchange Environment?*. Washington, DC. Available online at: https://www.hhs.gov/hipaa/for-professionals/faq/554/how-do-hipaa-authorizations-apply-to-electronic-health-information/index.html (accessed June 29, 2019).

Office for Civil Rights (2012). *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance With the Health Information Portability and Accountability Act (HIPAA) Privacy Rule*. Available online at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (accessed June 15, 2019).

Office for Civil Rights (2013). *Summary of the HIPAA Security Rule*. Washington, DC. Available online at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed June 23, 2019).

Office for Civil Rights (2016). *HIPAA Privacy, Security, and Breach Notification Audit Program*. Washington, DC. Available online at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (accessed June 27, 2019).

Office for Civil Rights (2017). *Research*. Washington, DC: Department of Health and Human Services. Available online at: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html (accessed June 10, 2019).

Office for Civil Rights (2018). *Guidance on HIPAA and Individual Authorization of Uses and Disclosures of Protected Health Information for Research*. U.S. Department of Health and Human Services. Available online at: https://www.hhs.gov/sites/default/files/hipaa-future-research-authorization-guidance-06122018%20v2.pdf (accessed June 12, 2019).

Office for Human Research Protections (1997). *Issues to Consider in the Research Use of Stored Data or Tissues*. Rockville, MD. Available online at: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/issues-to-consider-in-use-of-stored-data-or-tissues/index.html (accessed June 21, 2019).

Office for Human Research Protections (2008). *Coded Private Information or Specimens Use in Research, Guidance*. Rockville, MD. Available online at: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html (accessed June 15, 2019).

Office for Human Research Protections (2010). *Withdrawal of Subjects From Research Guidance*. Available online at: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/guidance-on-withdrawal-of-subject/index.html (accessed June 15, 2019).

Office for Human Research Protections (2016a). *Human Subject Regulations Decision Charts*. Rockville, MD. Available online at: https://www.hhs.gov/ohrp/regulations-and-policy/decision-charts/index.html (accessed June 15, 2019).

Office for Human Research Protections (2016b). *Informed Consent FAQs*. Rockville, MD. Available online at: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/informed-consent/index.html (accessed June 14, 2019).

Office for Human Research Protections (2018a). *Companion Q&As About the Revised Common Rule*. Available online at: https://www.hhs.gov/ohrp/sites/default/files/Revised-Common-Rule-Q%26As-08-20-2018.pdf (accessed August 3, 2019).

Office for Human Research Protections (2018b). *Research With Children FAQs*. Rockville, MD. Available online at: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/children-research/index.html (accessed June 14, 2019).

Office for Human Research Protections (2019). *Revised Common Rule Q&As*. Available online at: https://www.hhs.gov/ohrp/education-and-outreach/revised-common-rule/revised-common-rule-q-and-a/index.html (accessed June 10, 2019).

Office of the National Coordinator for Health Information Technology (2019). *Introduction to the Trusted Exchange Framework and Common Agreement (TEFCA)*. Washington, DC.

Orcutt, M. (2018a). *Ethereum's Smart Contracts are Full of Holes*. Cambridge, MA: MIT Technology Review. Available online at: https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/ (accessed February 20, 2019).

Orcutt, M. (2018b). *How Secure Is Blockchain Really?*. Cambridge, MA: MIT Technology Review. Available online at: https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/ (accessed February 1, 2019).

Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* 25, 1398–1411. doi: 10.1177/1460458218769699

Pollak, J. (2006). *HIPAA Questions and Answers Relating to Research Databases*. Baltimore, MD: Johns Hopkins Medicine. Available online at: https://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/faq_databases.html (accessed June 21, 2019).

Reinhardt, R. (2019). *Your Software and Devices Are Not HIPAA Compliant*. Fuquay-Varina, NC: Tame Your Practice. Available online at: https://www.tameyourpractice.com/blog/your-software-and-devices-are-not-hipaa-compliant/ (accessed June 30, 2019).

Riddle, J. (2018). *Final Rule Material: Secondary Research With Identifiable Information and Biospecimens*. Available online at: https://about.citiprogram.org/wp-content/uploads/2018/07/Final-Rule-Material-Secondary-Research-with-Identifiable-Information-and-Biospecimens.pdf (accessed June 21, 2019).

Risius, M., and Spohrer, K. (2017). A blockchain research framework. *Bus. Inf. Syst. Eng.* 59, 385–409. doi: 10.1007/s12599-017-0506-0

Shae, Z., and Tsai, J.J.P. (2017). "On the design of a blockchain platform for clinical trial and precision medicine," in: *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, eds A. Musaev, J.E. Ferreira, T. Higashino, and IEEE Computer Society (Atlanta, GA: IEEE Computer Society). doi: 10.1109/ICDCS.2017.61

Sichtig, H., Minogue, T., Yan, Y., Stefan, C., Hall, A., Tallon, L., et al. (2019). FDA-ARGOS is a database with public quality-controlled reference genomes for diagnostic use and regulatory science. *Nat. Commun.* 10:3313. doi: 10.1038/s41467-019-11306-6

Svikhart, R.T. (2017). Blockchain's big hurdle. *Stan. L. Rev. Online* 70, 100–111. Available online at: https://www.stanfordlawreview.org/online/blockchains-big-hurdle/

Swihart, J., Winston, B., and Bowe, S. (2019). *Zcash Counterfeiting Vulnerability Successfully Remediated*. Denver, CO: Zcash. Available online at: https://z.cash/blog/zcash-counterfeiting-vulnerability-successfully-remediated (accessed February 20, 2019).

Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C., and Njilla, L. (2017). "Consensus protocols for blockchain-based data provenance: challenges and opportunities," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, ed S. Chakrabarti (Piscataway, NJ: IEEE), 469–474. doi: 10.1109/UEMCON.2017.8249088

Uniform Law Commission (2019). *Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal eSign Act, Blockchain Technology and "Smart Contracts"*. Chicago, IL. Available online at: https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=d2026984-1040-3c6f-62c8-a676b12d7bff&forceDialog=0 (accessed June 11, 2019).

Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018). *Blockchain Technology Overview*. NIST Interagency/Internal Report. National Institute of Standards and Technology, Gaithersburg, MD, United States.

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.