THOMSON REUTERS
Westlaw®

A proposed agreement for a blockchain-enabled medical staff credentialing process

By J. Mark Waxman, Esq., and Jennifer Rathburn, Esq., *Foley & Lardner*

OCTOBER 29, 2018

The medical credentialing process, whether for a hospital, a hospital system or a health plan, has emerged as a potential early target for the application of blockchain technology and administration.[1] It is a process that allows a secure database to be established over time and on a cumulative basis.

Medical credentialing involves verifying whether a candidate meets the applicable educational and training prerequisites for the position sought — appointment to a hospital's medical staff or the ability to participate as a member of a health care delivery network, such as an independent practice association — and subsequent updating and verification throughout a career.

This process takes time and can be frustrating to complete, but it can be made more efficient by using simple storage techniques and avoiding duplication.

Because blockchains are a form of database that can be verified and updated incrementally, they may be well suited for this credentialing process. Information in the form of "blocks" of credentialing information can be linked together to create the credentialing information "chain," with links to prior blocks and information about when that block was created or contributed into the chain.

Blockchain encryption applications and access limitations can provide security for the database. Thus, blockchain can create secure access across all those participating in the chain.

Each data contributor, or user, may be granted access to the entire ledger, or chain of information. Alternatively, access can be restricted. For example, educational institutions providing information need not have access to the entire chain.

The initial effort to engage blockchain for these purposes was initiated in Illinois in 2017 with a pilot program involving the Hashed Health consortium. The goal of this early effort is to create a blockchain-based registry containing a reliable record of certifications and credentials.

This article proposes a template for an agreement for a credentialing database specifically designed to use blockchain technology as its infrastructure. Because inputs from several states may be required, before parties can embrace a "smart contract," i.e., one fully adopting the blockchain technology, the relevant states may need to enact an enabling statute for such contracts. Hence, a standard contract format is needed pending such a development.[2]

THE TYPICAL CREDENTIALING APPLICATION

Ordinarily, a medical provider seeking to join a medical staff or a network submits a staff application to a hospital or payer through a credentialing organization or office. The office then needs to verify the education, training, licensure and certification, narcotics registration certificates, affiliation history and record of discipline (if any).

It will also obtain reports from any applicable state or federal database (e.g., to ascertain the provider is not on the excluded provider list), and possibly a malpractice claims information report. Professional references may also be required.

As part of the process, the provider will execute a consent and release form authorizing the entity to which the application is directed to "inquire of any individual or entity with whom or which [the provider] has been associated (including medical malpractice carriers) who or which it deems relevant in its assessment of ... professional competence, character and ethical qualifications."[3]

At the same time, the provider will consent to the disclosure of information gathered by that entity to other like entities as a part of their credentialing processes. The provider and the entity receiving the information typically sign releases of liability. The provider may also have the right to review information received and offer corrections or explanations.

Finally, it is important to note the two types of information that may be reviewed during the credentialing process: objective and subjective. The former consists of factual information. For example, was Dr. X disciplined or the subject of a licensing action at a particular institution at a particular moment in time?

The latter includes information that involves the exercise of judgment or discretion. An example of subjective information is

opinions that were expressed at a board or medical staff executive committee hearing. It might also include a review of the underlying facts in a malpractice litigation that formed the basis for a disciplinary decision, and a determination that they indicate significant deficiencies either in technique, or even behavior, which led to an adverse credentialing decision.

Blockchain is likely better suited for the disclosure of objective rather than subjective information. Thus, the goal of the blockchain credentialing process would be to learn and distribute objective information, and through that information indicate that there remains subjective information that would be available through a direct inquiry outside the blockchain process.[4]

If there are no facts indicating that subjective information needs to be reviewed, the blockchain information would be sufficient to efficiently complete the process.

On the other hand, if there are issues that need substantive review, arising, for example, from the obligation of hospital boards making medical staff decisions to do their own substantive review and not to rely on the peer review determinations of other hospitals,[5] further inquiry would be required.

THE BLOCKCHAIN CREDENTIALING PROCESS AGREEMENT

The nature of the agreement and effective date

Initially, a blockchain agreement needs definition to ensure its nature and purposes are clear. There are currently a variety of definitions in circulation.

In Illinois, under the proposed Blockchain Technology Act passed by the House of Representatives, blockchain is defined as "an electronic record created by the use of a decentralized method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information."[6]

In a recently enacted law, Assembly Bill 2658, California adopted the following blockchain definition: "a mathematically secured, chronological, and decentralized ledger or database."

Thus, the title of the blockchain credentialing process agreement, or BCPA, will reflect that the parties agree to use blockchain technology, define what that technology is and specify who will be responsible for operating it.

In Illinois and other states that recognize smart contracts — contracts stored as electronic records that are verified by use of a blockchain — the contract may be facilitated through the blockchain mechanism and the distribution of access identification.

The BCPA would also recite its purpose. For example:

This Blockchain Credentialing Smart Contract ('the Agreement") is effective as of ____ (the "Effective Date"). Its purpose is to provide for the exchange of information necessary for the application of _____ (hereafter "the Practitioner") for medical staff privileges at health care facilities licensed by and operating in the State of _____ (hereafter the "Facilities") [and for credentialing as a participation [type] provider in networks maintained by those health plans [hereafter the "Plans"] who participate in this Agreement. For purposes of this Agreement:(a) the collective ledger of information provided by the parties under the terms and conditions of this Agreement is referred to herein as the "Chain"; and (b) the Agreement, to the extent allowed by the law of ____will be in a smart contract format, meaning that it will be stored as an electronic record that will be verified by use of the Chain.

The parties

The agreement must indicate the initial parties to it and indicate that consent is provided to allow a defined set of additional "credentialing parties" to become participants. An initial question is whether there needs to be consent by existing parties to have another join the chain and sign on to the agreement.

The statement or listing of parties must indicate whether the party is a single institution, or for purposes of credentialing, is an institution, like a hospital or hospital system, that includes all its affiliates, for example, wholly owned or joint-venture ambulatory surgery centers.

In the case of a managed care plan or other third-party payer, it should specify whether it includes entities for whom the party might provide administrative services, such as the situation where a payer is administering plans under the Employee Retirement Income Security Act, 29 U.S.C.A. § 1001.

The parties should consider whether full access to information maintained in the chain may be given to all participants. While it may be clear that educational institutions will not need or want such access, there may be situations where the information is sought by those who might not qualify for peer review protection under applicable state law.

For example, a medical group or independent practice association may be too small to have a qualifying peer review process or committee.[7] Participation may, therefore, be limited to those entities and processes that qualify for that type of protection under federal or state law.

The BCPA would recite:

The parties to this Agreement are the Practitioner and the following data contributors (all collectively referred to as "the Parties"):

(1) Acute care hospitals, ambulatory surgery centers or other health care facilities who are licensed as health facilities in the State of ____, to whom the Practitioner has sought membership as a member of the [active] medical staff (hereafter referred to as "Facilities");

(2) Licensed insurers, health maintenance organizations, or their agents responsible for credentialing physician participation in health care provider networks as participating providers (hereafter referred to as "Plans");

(3) Licensing agencies with professional licensing responsibility over the Practitioner (hereafter referred to as "Agencies");

(4) Accrediting agencies with jurisdiction over the Practitioner (hereafter referred to as "Accreditors");

(5) Educational institutions from which the Practitioner graduated (hereafter referred to as "Institutions"); and

(6) Affiliates of, or contractors to, a Facility or Plan whose purpose is to facilitate the exchange of information for the purpose of practitioner credentialing for medical staff or practitioner network membership for such Facility or Plan.

As of the Effective Date, the parties to the Agreement are:_____.

The Agreement will add parties when consented to by the Practitioner and the new party has entered into this Agreement in any manner authorized by law. Notice of a new party will be provided by the Practitioner or another party with the Practitioner's consent.

Term and termination provisions

The agreement would be initiated upon the initial practitioner application or upon the entry into the agreement by the practitioner and one or more parties. It may specify its duration and how and by whom the agreement and a party's participation can be terminated. The following may be appropriate:

The Term of this Agreement will commence as of the Effective Date. The Agreement shall continue in force until it is terminated by the Practitioner, who shall provide ___days' notice to each of the Parties to the Agreement.

The Agreement will terminate upon Notice from the Practitioner to the parties to the Agreement.

A party to this Agreement other than the Practitioner may terminate its own participation in this Agreement upon ___days' prior Notice. In the event of such a termination, the Information provided shall be retained by the remaining parties to this Agreement until the earlier of either their termination as a party to this Agreement, or the termination of the Agreement.

In the event any Party terminates its participation in the Chain, it will take commercially reasonable steps to destroy all passwords or access identifiers with respect to access to the Chain.

Information to be provided, access and consent

The agreement is designed to facilitate the sharing of relevant credentialing information. It would provide that such information would be documented in the blockchain and that every party to the agreement, except perhaps for educational and accrediting entities, would be able to access it. The parties would want to address information veracity.

To achieve these purposes, the agreement would provide as follows:

Blockchain-contributed information. The Parties agree to contribute the following information (the "Information") from their files and records to the chain:

(1) Records of attendance or membership, including dates of admission and graduation, and the degrees, certificates, fellowships, internships and residencies completed;

(2) Medical staff privileges granted and, if applicable, revoked;

(3) Participation as a participating provider in a delivery system or network granted;

(4) Any adverse disciplinary actions initiated or taken with respect to any privilege or license;

(5) Demographic information;

(6) Professional licensure information;

(7) NPI number;

(8) Narcotics registration certificates;

(9) Professional affiliations;

(10) Records of continuing professional education;

(11) Malpractice coverage;

(12) Exclusion from any federal or state health care program;

(13) Health screens and immunizations; and

(14) Malpractice claims.

Each Party represents and warrants that it is providing the most current, as of the time it provides it, information available in its practitioner credentialing (or similar in content

or purpose) files regarding the Practitioner's professional credentials and qualifications. In the event of a change in that information, it will update the Chain with such new information within ___days of obtaining or receiving it.

Each Party expressly states that, with the exception of information generated from its own records based upon events that occurred as the result of conduct by that Party (e.g. a peer review proceeding or adverse action taken by that Party, as opposed to information about actions taken by other parties which it receives as a result of entering into this Agreement), it has not engaged in any independent investigation or evaluation of the information it provides, and as a result shall not be liable for any misrepresentation or inaccuracy.

Ownership, use and disclosure of information

As in the case of any information relating to medical staff applications, the ownership of the information is with the party that created it, and it should not be used for any other purpose. This should preserve the applicable peer review protection privileges.

In addition, representations would be appropriate with respect to access and internal distribution of information. Finally, to the extent that protected health information, or PHI, about the practitioner might be involved in a thorough review process (e.g., if the practitioner was in a diversion program), it would not be disclosed.

This makes it particularly important that the initial credentialing inquiry be sufficient to discern whether this type of information would be material to the consideration by the entities involved. (For example, have you participated in any programs to address practice issues in the last five years?)

The following provisions implement this concept:

Each Party shall be the owner of the Information that it provides. Any Information it receives as the result of this Agreement or its participation in the Chain shall be used solely for the purposes of credentialing and credential verification, as requested by the Practitioner. The information received may not be used for any other purpose, or made available to any third party.

In order to safeguard the information that is the subject of this Agreement, each Party agrees that access to the Chain is subject to: (a) administrative, technical and physical safeguards designed to protect against misuse or unauthorized access or disclosure, and (b) protections against allowing transmission without reasonable encryption; and/or other measures that are custom and practice with respect to such information and efforts made to protect such information under any applicable peer review or medical information protection, data privacy or security statute or regulation, and applicable peer review confidentiality policies.

Each Party will take commercially reasonable steps to ensure that information documented in the Chain does not contain Protected Health Information ("PHI").

Each Party to this Agreement expressly consents that each other Party, with the exception of the Educational Parties to the Agreement, may access the information provided for the purposes set forth herein, and further, provide it through the Chain to any other Party to this Agreement. The Educational Parties shall not have access to any Information, and their role is limited to the provision of Information to the Chain.

Peer review and privilege

One of the questions likely to arise when participating in a credentialing arrangement facilitated by a blockchain-based information ledger is whether any existing privileges and protections under either the Health Care Quality Improvement Act, 42 U.S.C.A. § 11101, or HCQIA, or any applicable state law will be compromised.

In the ordinary course, at the state level, "neither the proceedings nor the records of organized committees" of the medical staff or any peer review body responsible for evaluating and improving the quality of care rendered in a hospital are subject to discovery. See, e.g., Cal. Evid. Code § 1157.

Initially, the answer should be "no" — as long as the exchange and storage of the information is truly for activities that fall within the definition of a professional review action under the HCQIA, 42 U.S.C.A. § 11151(9). To potentially reinforce this notion, while the protections of the state(s) where the agreement is being implemented must be reviewed and considered, it may nevertheless be helpful to add language to both affirm the purpose and give comfort to the participants, such as the following:

Professional review purpose. The purpose of the parties in entering this Agreement is solely to facilitate the exchange of information necessary for the parties to engage in initial and ongoing professional review actions within the scope and protections of the Health Care Quality Improvement Act, 42 U.S.C.A. § 11101 et seq. ("HCQIA"). In addition, the parties agree that they will conduct any professional review activities in a manner consistent with the requirements of HCQIA, so as to preserve its protections for all of the parties to this Agreement.

In the event of legal process, in the form of a subpoena, or otherwise, seeking discovery or to force a party to disclose information it may have as a result of entering into this Agreement, such party shall:

(1) Provide notice as soon as practicable to the parties to this Agreement; and

(2) Resist the provision of information received as a result of participating in this Agreement through the retention of counsel and the filing of such actions as counsel may advise consistent with the goals of this section.

Limitation of liability and indemnity

Entities that furnish information for credentialing purposes typically disclaim any liability based on information they furnish that was provided to them by a third party. This disclaimer would be reflected in the agreement.

On the other hand, the parties need to address situations where a failure to provide accurate information leads to denial of a credential or a termination of participation on a medical staff or in a provider network.

The parties may choose to disclaim liability as the result of a failure to provide accurate information with respect to facts or events originating at the provider of the information, when it is the product of gross negligence or intentional conduct.

The parties should decide whether to include an indemnification provision and if so, the scope of it. The scope of that indemnity might reach to claims that arise as the result of the intentional provision of false information.

Administrative provisions

The agreement should address standard administrative issues such as assignments, notice, disputes and the like. For example, it may include the following:

Assignment and delegation. No Party may assign this Agreement to any other party without the express consent of the Practitioner. The duties and obligations with respect to the provision of Information under this Agreement may be delegated to a controlled affiliate or a subcontractor who is responsible for maintenance or storage of the information to be provided under this Agreement and who is bound by the terms and conditions of this Agreement. Notice of such a delegation shall be given prior to any such delegation. For purposes of this Agreement, a "controlled affiliate" is one in which the Party has a majority of ownership or has the ability to appoint or remove 50 percent or more of the governing body. In the event of a delegation, the applicable Party remains fully responsible for its performance obligations under this Agreement.

Successors. This Agreement is binding upon and shall inure to the benefit of any successors or permitted assigns of each Party hereto.

Dispute resolution. The Parties agree that any cause of action arising out of or related to the download or use of Information, or the making, termination or implementation of this Agreement must be filed within one (1) year after the cause of action arose; otherwise, such cause of action is permanently barred. This agreement shall be governed by and interpreted in accordance with the laws of the State of _____. All disputes under this Agreement will be resolved in the applicable state or federal courts of _____. The Parties hereby agree that in any dispute resolution proceeding, they will not pursue, and there may not be awarded in any judgment, any consequential, exemplary or punitive damages.

Integration and severability. This Agreement represents the entire agreement between the Parties with respect to the furnishing of Information for the purposes set forth herein, and supersedes all other discussions, proposals between the Parties with respect to its subject matter. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that the Agreement will otherwise remain in full force and effect and enforceable.

No beneficiaries or other arrangements created. No agency, partnership, joint venture, or employment relationship is created as a result of the Agreement, and there are no third-party beneficiaries of this Agreement.

Notice. Notice under this Agreement may be provided by an entry into the Chain for the purpose of providing notice. Notice shall be effective ___days after such entry. Notice shall also be provided by providing notice by Certified or Express Mail and through digital means to the following addresses. Mail or digital notice shall be effective upon receipt by the Party to whom the Notice is directed.

CONCLUSION

Developing a blockchain agreement in the health care arena, whether in the form of a smart contract or otherwise, necessarily involves many processes and potential regulatory hurdles. In this case, the use of such an agreement in the credentialing realm is viable and generally poses a limited number of issues.

Foremost perhaps is whether information shared in this fashion would retain its protected status and whether participants, from the practitioner to the data contributors, can overcome what may be a natural reluctance to move

forward in this type of endeavor. Perhaps the first step is to try using a version of this proposed agreement within a closed type of system environment, such as a multi-hospital system within a given state.

NOTES

[1] *See, e.g.,* National Association Medical Staff Services, or NAMSS, draft paper: Blockchain Technology & Healthcare Credentialing: An Introduction, April 2017.

[2] Whether entry into a blockchain agreement meets the conditions for application of digital signature laws such as the Electronic Signatures in Global and National Commerce Act, 15 U.S.C.A. § 7001, or the Uniform Electronic Transactions Act (Unif. Law Comm'n 1999), absent more specific enactments, such as in California, is an open question.

[3] *See, e.g.,* Indian Health Service Statement of Understanding and Release, form of November 19, 2008 (https://www.ihs.gov/IHM/pc/part-3/p3c1/).

[4] This would also apply to situations where the initial inquiry indicates the possibility that a medical staff diversion or wellness process has occurred.

[5] *See Smith v. Selma Cmty. Hosp.*, 80 Cal. Rptr. 3d 745 (Cal. Ct. App., 5th Dist. 2008).

[6] HB5553, Illinois General Assembly. *See also* Ariz. Rev. St. § 44-7061(E)(1).

[7] *See, e.g.,* Cal. Bus. & Prof. Code § 805(a)(1)(B).

This article first appeared on the Practitioner Insights Commentaries web page on October 29, 2018.

ABOUT THE AUTHORS

J. Mark Waxman (L) is a partner and business lawyer with **Foley & Lardner**, where he is former chair of the Health Care Industry Team. He focuses on the health care delivery system and the role of new technology, entrepreneurship and new delivery approaches. He is based in the firm's Boston and San Diego offices and can be reached at mwaxman@foley.com. **Jennifer Rathburn** (R) is a partner based in the firm's Milwaukee office. She focuses her practice on counseling clients on data protection programs, data incident management, breach response and recovery, monetization of data, and other privacy and security issues. She can be reached at jrathburn@foley.com. The authors wish to thank James Lahana, Esq., for his very helpful review and comments.