HEALTHCARE AND DIGITAL CREDENTIALS

Technical, Legal, and Regulatory Considerations

fsmb

LEARNING MACHINE

TABLE OF CONTENTS

DISCLAIMER:

This Report is intended to facilitate an open and informed conversation about the subject matter. This Report does not represent the official policy of the Federation of State Medical Boards or any of its member boards. The Federation of State Medical Boards and its members are not bound by any conclusions or recommendations made in this Report and the Federation of State Medical Boards reserves the right to rescind or reconsider the views in this Report as the subject matter continues to evolve.

EXECUTIVE SUMMARY

The Federation of State Medical Boards (FSMB) is a national non-profit focused on providing support services to medical licensing boards throughout the United States and its territories. Among those services is the Federation Credentials Verification Service (FCVS), an NCQA-certified credentials verification platform that is widely used by physicians and physician assistants seeking medical licensure and credentialing. Efforts to improve this service and to ensure the use of current and best practice technologies illustrate that the processes used to create and verify medical credentials, by both FCVS and the industry as a whole, do not utilize available technology to their fullest potential and require change to meet the needs of the healthcare market of the future.

This realization led the FSMB to undertake a series of activities, including the evaluation of existing and emerging technologies for use in its own credentials verification platform, as well as increased engagement with a wide variety of stakeholders to discuss how best to collaborate to create not only individual, but systemic, changes that make the credentialing process more efficient without any sacrifice to the trust between actors or to the detriment of the patient.

This paper surveys Digital Signatures, Open Badges and Blockchain technology and provides commentary rooted in the FSMB's experiences applying these technologies to the licensing and credentialing workflow. Because of the nascent nature of the use of these technologies in the regulatory process, this Report is intended not to provide specific recommendations or be an endorsement of a specific product or products but to evaluate currently available technologies with an eye toward the future of educational credentialing and healthcare regulation. In addition to in-depth technical overviews of the technologies being considered, this Report contains a summary matrix for reference and visual comparisons. Legal and regulatory criteria are included, along with a technical review, as an understanding of the interplay between law and technology is vital to the adoption of new technologies to build the trust framework for a regulated environment.

The FSMB recognizes that technology may enhance systemic trust and foster greater regulatory efficiencies. The FSMB is committed to integrating appropriate technology to alleviate administrative burdens suffered by healthcare professionals and to promote best practices that can be implemented by state medical boards in furtherance of their duty to protect the public. Combined, the attainment of both of these goals may usher in a dynamic regulatory system that not only protects the public from harm, but also provides the public with the highest level of trust in those providing care.

1. INTRODUCTION

Credentials serve an important role in social formation and maintenance of social order. Credentials, which can be presented in any form, express specific information about an individual's identity and their ability. Bundled together, credentials create social value and are essential to meaningful social interaction.

Credentials expressed through a trusted identity framework can be accorded a higher value within a social interaction due to the underlying assumption that someone within the system is managing the creation and transfer of these credentials. Within any high functioning identity framework specifications, rules, and agreements based in both technological capacity and social need are necessary to ensure that the level of trustworthiness required by participants in the identity system and the community relying on the services offered by the identity system is met.[1]

Among the social interactions where a robust, credential-dependent trust framework is most necessary is the delivery of healthcare. The intent of medical licensing and credentialing processes carried out through a variety of parties including academic institutions, state medical and osteopathic boards, federal healthcare agencies, insurance providers, and individual health care facilities is to ultimately verify education, training, and experience levels of a healthcare provider with the highest levels of accuracy and integrity. Verification of these credentials ensures a high level of shared trust between all actors within the healthcare ecosystem. Patients trust that their physicians have been trained and vetted to practice safely. Hospitals, in turn, trust that the physicians they employ will provide a high standard of care.

Among the social interactions where a robust, credential-dependent trust framework is most necessary is the delivery of healthcare.

Historically, verified credentials transmitted and maintained by extensive chain of custody processes have provided a baseline level of systemic trust in medical licensing and credentialing. These processes not only review and validate required artifacts but leave behind audit trails needed to satisfy both internal and external standards that form the normative boundaries for the system in which the credentials are used. State medical boards require that qualifications for licensure be submitted directly to the state board for review or verified independently by a third party to verify the authenticity of credentials presented for the issuance of a medical license.[2] Rooted in requirements of applicable federal regulation[3] and the evolution of common law,[4] a complementary standards framework for healthcare facilities originates from private organizations such as the Joint Commission, Det Norske Veritas Healthcare, the National Committee for Quality Assurance (NCQA) and the National Association Medical Staff Services (NAMSS).

Due to the variety of sources which produce the credentials and the volume of information needed to comply with the various standards, healthcare credentials are among the most difficult of the professions to verify and maintain. Currently, the manual and paper-based nature of these processes, which often includes the use of independent third parties such as Credential Verification Organizations (CVOs) to obtain, maintain, and transmit documents or records, which are often redundant, adds to increased processing times and increased costs shared by both the credential holder and the credential verifier.

The FCVS, a NCQA-certified credentials verification platform, is widely used by physicians and physician assistants seeking medical licensure and credentialing. Each year, FCVS is used in approximately 50% of medical licensing decisions made in the United States. Since 2010, the time to create a FCVS credential has been dramatically lowered from over 60 days on average to under 25 days. A substantial driver of this decrease has been the implementation of digital technologies. Through efforts to improve this service and to ensure the use of current and best practice technologies, it became clear the credentials creation and verification process was not utilizing available technologies to their fullest potential and was not well-suited for future healthcare needs. In addition, an internal survey of current process illustrated that 66% of the time that it takes to create a credential is driven by processes and parties outside of the control of FCVS, warranting discussion of how the FSMB could support the adoption of digital approaches to credentialing throughout the system.

Digitization may foster a regulatory framework that is not only agile and automated but may also be a critical component in efforts to address other challenges within healthcare. The FSMB House of Delegates has repeatedly identified regulatory redundancies as an impediment to license portability[5] and has called for enhancements to FSMB services that would expedite delivery of physician credentials to state medical boards and third parties.[6] Widescale reduction of administrative redundancies has been identified in the 2018 FSMB Report on Physician Wellness and Burnout as a recommendation that would improve physician wellness, a patient safety issue.[7] Furthering the discussion of the digital transformation of credentialing through a vehicle such as this Report is another step forward towards the realization of these policy recommendations and aligns with the FSMB's solid commitment to regulatory excellence.

As technology and healthcare evolve, so too does the ability of key stakeholders to provide a more efficient, secure, and verifiable trust framework without sacrificing the essential elements necessary to create a high level of trust between the patient and provider. In addition, there is a growing movement to disintermediate the creation and management of credentials and provide individual ownership of one's own credentials. Digital credentials, in a variety of forms, can abstract the complexity of the licensing and credentialing process and reduce it to a seamless digital function which creates and maintains the trust framework that is the necessary foundation for a modern healthcare system.

Digitization may foster a regulatory framework that is not only agile and automated but may also be a critical component in efforts to address other challenges within healthcare.

1.1 ELECTRONIC TRANSACTIONS: LEGAL AND REGULATORY STANDARDS FOR CREDENTIALS

LEGAL REQUIREMENTS FOR ELECTRONIC AND DIGITAL SIGNATURES

Assessing the use of digital credential mechanisms in the context of healthcare must first begin with an inquiry into the fundamental question of whether the applicable laws, regulations, and standards allow for the transaction to occur in an electronic form. Credentials are governed not only by laws establishing the elements required for a legally valid transaction, but also by laws addressing privacy and security, such as the Family Educational Rights and Privacy Act (FERPA), and in the case of credentials arising out of the European Union, the General Data Protection Regulation (GDPR). For digital credentials to be fully integrated into the existing workflow it must be clear that functional elements such as authenticity, primary source attestation, secure electronic delivery, and audit trails are present. Without assurances of these foundational elements, the baseline level of trust in the system, predicated on rules developed for a paper-based transaction, would be eroded.

Within the United States, the Uniform Electronic Transaction Act (UETA) and the Electronic Signatures in Global and National Commerce Act (ESIGN) establish legal and functional equivalency between paper-based transactions and digital transactions. Importantly, this combination of state and federal laws governing electronic transactions does not specify that a specific technology is required for Electronic Signatures.[8] The laws allow the parties in the transaction to mutually agree to the use of any method of authentication that suits the needs and security concerns inherent to the particular transaction. The digital medium used does not affect the legal significance of the transaction.

Under UETA and ESIGN an Electronic Signature is "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record." Specifically within healthcare, Electronic Signatures have been found valid under Health Insurance Portability and Accountability Act (HIPAA) rules so long as mechanisms are put in place that protect the legality and security of the document as well as any protected health information contained within. Electronic Signatures can take a variety of forms, ranging from a digitized image of a handwritten signature attached to a document, clicking "I Accept" in a wraparound agreement, or a digital signature using public key cryptography. For the later, UETA differentiates between Electronic Signatures and Digital Signatures and defines a Digital Signature as an Electronic Signature that has the same legal validity as a manual (wet) signature. To have legal validity, a Digital Signature must have the following characteristics: (1) It is unique to the person using it; (2) It is capable of verification; (3) It is under the sole control of the person using it; and (4) It is linked to data in a manner such that if the data is changed, the digital signature is invalidated.

International standards mirror the criteria for legality utilized by UETA. In 2014, the European Parliament passed and the European Council approved the eIDAS Regulation (910/2014), which repealed the eSignature Directive that set forth the guidelines for electronic transactions across the EU's internal market. Under eIDAS, an Electronic Signature is defined as "any data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign." This could involve a signatory drawing their signature on a tablet with their fingertip or a click agreement. Any eSignature that is not Advanced or Qualified is considered Standard. A signature is "advanced" if it meets the following criteria: (1) It uniquely identifies and links its signatory; (2) The private key used to create the Electronic Signature is under the sole control of the signatory; (3) If the data is tampered with after the message has been signed, the signature must identify that this has happened; and (4) Invalidating the signature in the event its accompanying data has changed.[9]

THIRD PARTY STANDARDS WITHIN HEALTHCARE

Concurrent with the legal requirements setting out the acceptability of an electronic transaction, healthcare entities that create, manage, or rely upon credentials often seek to comply with private standards organizations within the United States. Compliance with these standards creates some systemic harmony but also allows for reimbursement and provides a defense against claims of negligent credentialing. More importantly, just as the law does not discriminate against a transaction if completed entirely through verifiable digital formats, these standards do not prohibit creation or acceptance of digital credentials for the aforementioned purposes so long as there are assurances of procedural and data integrity.

As a means of protecting patients from practitioners who fraudulently represent their qualifications and experience, licensing boards and health care organizations have historically asked for credentials to be provided directly from the "primary source" - that is, the university or other institution granting the

credential or a recognized entity which is able to verify the record of employment. By the late 1990s, Joint Commission standards required primary source verification for all licensed independent practitioners, a requirement that shortly expanded to include most healthcare providers, including nurses and other affiliated health professionals. Primary source verification confirms that an individual possesses a valid license, certification, or registration to practice a profession when required by law or regulation. The Joint Commission's Accreditation Manual defines primary source verification as "verification of an individual practitioner's reported qualifications by the original source or an approved agent of that source. Methods for conducting primary source verification of credentials include direct correspondence, documented telephone verification, secure electronic verification from the original qualification source, or reports from credentials verification organizations (CVOs) that meet Joint Commission requirements."

These standards do not prohibit creation or acceptance of digital credentials for the aforementioned purposes so long as there are assurances of procedural and data integrity.

"Secure electronic verification from the original qualification source" remains undefined, but applying principles of electronical transaction laws, a credential produced in a digital format should be acceptable so long as the integrity of the digital credential can verified. It is critical for the elemental nature of trust within healthcare that the relying institution can determine that the credential is authentic, unaltered, and secure.

Similarly, NCQA standards focus on procedural integrity and the ability to authenticate information that is essential to public safety. NCQA standards require an organization to verify elements such as licensure history and DEA certification at the time credentialing reports are reported out to a third party. Acceptable documentation that meets the standards includes faxed, digital, electronic, scanned, or photocopied signatures. Signature stamps are not acceptable unless the practitioner is physically impaired. As with the Joint Commission standards, digital credentials discussed in this paper are capable of meeting this standard.

The National Association of Medical Staff Services (NAMSS) represents medical staff professionals who oversee the credentialing and privileging processes for medical staff applicants. These professionals primary source verify medical staff information through queries of mulitple data banks and government records in accordance with government regulations and health system accrediting organization standards, such as those established by the Joint Commission. In the furtherance of their work to improve the quality and availability of the data used by medical staff professionals to determine the fitness of medical staff, NAMSS recognizes the potential benefits of digital credentials. In 2014, it released a report examining best practices and essential data elements in the facility credentialing process, identifying the 13 essential criteria for credentialing an initial practitioner applicant. The report stated that "technology should be utilized to ensure static data does not need to be re-verified once it has been confirmed once by the primary source." A subsequent roundtable hosted in 2018 stressed integrity of process over any specific technology or platform.

It is worth noting that these private standards are only a sample of the various elements that are associated with risk management and review of professional credentials in the context of healthcare. Generally, the acceptability of private standards should mirror the themes of non-discrimination and accepted

authenticity of digital documents and transactions commonplace in the commercial context. Addressing the first principle issue - the ability to trust credentials as presented - is a foundational component of digital credentialing and should not discriminate against processes of creating, presenting, and retaining credentials through an authenticable, reliable, and transferable medium.

Addressing the first principle issue - the ability to trust credentials as presented - is a foundational component of digital credentialing and should not discriminate against processes of creating, presenting, and retaining credentials through an authenticable, reliable, and transferable medium.

2. DIGITAL CREDENTIALS TYPES

2.1 DIGITAL SIGNATURE + PKI

In both the United States and European Union, Digital Signatures form a subset of the broader category of Electronic Signatures, or eSignatures. An Electronic Signature is any digital symbol attached to or logically associated with a record for the purposes of signature. Examples of Electronic Signatures include: 1) the signatory typing their name on the signature line of a digital document; 2) the signatory affixing an image of their handwritten signature on the signature line of a digital document; and 3) the signatory clicking “I Accept” to accept the terms of an agreement.

Digital Signatures, by contrast, are a type of Electronic Signature that uses digital keys, to “seal” a document with the issuer’s unique digital key. Cryptographically signing a document involves a process using strings of letters and numbers which protect the integrity of the credential. This process starts by creating a signature of the contents with the issuer’s private key to seal the document, effectively reducing the ability of others to tamper or modify the credential once it is issued. A specific type of digital key was developed in the 1970’s to secure electronic communication and distribute the required keys. This method is called Asymmetric Cryptography because each key is generated as a mathematically linked pair; one is kept private, and one is open to the public.

The wider validity of Digital Signatures is derived cryptographically. Electronic Signatures, by contrast, consist of an electronic mark made by a signatory under legitimate conditions defined within a jurisdiction. Electronic Signatures are considered legally valid in the same way as handwritten (wet) signatures - by force of law rather than by providing assurances based solely upon the integrity of the underlying cryptography. Additional procedural layers provide a layer of third-party trust within communication channels using Digital Signatures. These layers are referred to as a Public Key Infrastructure (PKI). The key organization within any PKI is the Certificate Authority (CA). The role of Certificate Authorities (CA) in PKI is to certify that an organization owns a specific public key.

This allows others to rely upon signatures corresponding to the certified public key. During the verification process, a verifier can verify that the signed value was indeed generated by the private key corresponding to the associated public key. The role of Certificate Authorities is explained in more detail in the section below.

Digital Signatures with PKI do three things that are essential if their use will be found acceptable by regulators and other relying parties within healthcare: 1) authenticate the message signatory; 2) verify the message integrity; and 3) and prevent the signatory from denying that they signed the message. While there are ways of enforcing digital audit trails and tamper evidence for Electronic Signatures, these methods do not have the same strength as cryptographic security, and therefore do not provide additional trust in the document.

CERTIFICATE AUTHORITIES

Digital Signatures depend on trusted Certificate Authorities, or Trust Service Providers, to function properly. A Certificate Authority (CA) is a third-party service which certifies ownership of public keys by issuing Digital Certificates. Many will be familiar with CAs in the context of SSL and TLS certificates, which are used to authenticate websites, servers, and clients. SSL and TLS certificates are issued by a Certificate Authority and are the foundation of secure web browsing and ecommerce. Each web browser has a built-in list of approved Certificate Authorities from whom it accepts Digital Certificates.

In principle, anyone can act as their own Certificate Authority, issuing their own Digital Certificates. In practice, however, this complex operation is usually outsourced to well-known Trust Service Providers. For instance, when you go to a site that uses HTTPS for internet connection security, the website's server uses a certificate to prove the website's identity to browsers, like Chrome. SSL and TLS certificates can be purchased through known vendors like Comodo and Symantec, which act as certificate authorities. Although there are alternative models for PKI, such as the Web of Trust or Simple PKI (SPKI), the Certificate Authority model is most widely used. Relying on one party to complete verification, however, has several drawbacks– primarily cost and centralization. Further, only a few CA vendors control this space. If any one of them were to be hacked, and faked credentials were issued, it would create serious problems for trusting digital certificates on a mass scale.

DIGITAL SIGNATURES USE CASES (DOCUSIGN)

DocuSign, one of the world's foremost providers of Digital Signatures, focuses on a subset of data integrity verification and authentication - legally binding agreements between people. Accordingly, DocuSign bills its solution as a "System of Agreement" to record consensus. While documents signed through DocuSign employ the same cryptographic primitives as other types of digital credentials, the DocuSign product and user interface are optimized for human signatures on agreements. Accordingly, the most frequent uses for DocuSign include contracts, wills, waivers, consent forms, letters of agreement, memoranda of understanding, and other two- or multi-way human agreements enforceable in a court of law. Other major applications of DocuSign include documentation timestamping and archiving.

Starting in 2013, the FSMB began to utilize DocuSign to streamline the post-graduate training verification process for FCVS. As part of its improvements to the FCVS service, a larger percentage of graduate medical education (GME) verification requests were converted for use with the DocuSign process. While it should be noted that many vendors provide similar functionality to DocuSign, this Report focuses on DocuSign because of the FSMB's extensive use of their product.

Other examples of Digital Signatures use cases for academic credentials are diplomas and transcripts. Some educational institutions, like Stanford University, have begun to use digitally signed PDFs for this purpose. The service CeCredential Trust, owned by Paradigm, has commercialized the technology used by Stanford and now offers it to universities throughout the United States. Parchment, an established US

vendor of diploma and transcript services, similarly offers PDF credentials digitally signed with Adobe Blue Ribbon security. Credentials provided through these platforms are currently recognized for licensing decisions by state medical boards.

SIGNATURE VERIFICATION

In the case of DocuSign, verification is provided by virtue of DocuSign acting as host and Certificate Authority for both parties. DocuSign not only acts as a Certificate Authority for their customers, but also provides a Trust Service Provider (TSP) Program for those customers who want or are legally required to use a different Certificate Authority. The TSP Program allows documents to be signed via the DocuSign interface using key pairs generated and managed by Certificate Authorities other than DocuSign.

When the document format of a digitally signed document is a PDF, verification must be completed using Adobe software, as Adobe owns the PDF standard. In those cases, verification of a document is completed using Adobe Acrobat on the desktop or Adobe LiveCycle as part of an automated process on a server. To verify the document, the desktop user opens a PDF using Adobe Reader or Adobe Acrobat. When a document has a valid signature, a blue ribbon in a blue bar shows above the document in the Adobe viewer.

In addition to desktop verification of a PDF using Digital Signature vendor software, some providers, like CeCredential Trust, also provide dedicated online credential lookup portals for schools that license their verification service. Verifying a credential on one of these portals generally requires knowing some of the recipient's personally-identifiable information, for example, their last name, date of graduation, or the last four digits of their social security number.

CONCLUSION

Digital Signatures meet legal and regulatory requirements and are the most established form of digital credentials at this time. Digital Signatures will continue to have a role to play in improving the efficiency of the credentialing process in the near to mid-term. However, exploring additional developing technologies expands upon baseline improvements, as they may offer alternatives for those entities looking to remake their credentialing and verification systems for the longer term.

2.2 OPEN BADGES

Open Badges refers to a technical standard for bundling information about an individual's achievement, embedding it into a portable image file, and validating that file through web-based verification. This format was designed to convey a singular skill or achievement through a verifiable digital image and hosted set of data.

Open Badges arose in 2011 to meet the needs of an increasingly fragmented and informal education and labor marketplace. Adoption has been highest for micro-credentialing, non-formal learning, and professional development use cases. Initially spearheaded by the Mozilla Foundation with a grant from the MacArthur Foundation, the Open Badges standard has been maintained by the IMS Global Learning Consortium since January 1, 2017.

Open Badges are image files in SVG or PNG format connected to a hosted JSON dataset and Issuer Profile. The specification also allows for badges to be cryptographically signed by the issuer using a Digital Signature (see Section 2.1); however, this is not required. In practice, most issuing authorities do not sign badges. There is speculation that this omission is due to the additional effort entailed in managing and maintaining the signing keys for validation. With this in mind, the remainder of this Report will refer exclusively to hosted but unsigned badges unless otherwise noted.

Open Badges employ a data schema with required fields optimized for specific educational use cases, such as "description," "image," and "criteria narrative." Extensions to Open Badges allow for expanding this limited data set to include other types of data such as text, array, url, boolean, and more. Extensibility provides a great deal of flexibility but does require significant coordination between parties if the extensions are intended to be used as a standard. An example of this in medical credentialing would be standard forms used to verify residency training.

The IMS Global Learning Consortium hosts a free, independent Open Badge 2.0 verifier at https://openbadgesvalidator.imsglobal.org. IMS also provides a process by which vendors may be certified for compliance with the Open Badges 2.0 standard. Certification of vendors must be renewed on an annual basis by passing the certification process and paying an annual fee.

The Open Badges framework relies on trusted institutions to issue, host, and secure badges for future verification. While this is acceptable in many situations, the reliance on a single, trusted source may cause issues if badges are lost or modified by either the issuer or an attacker after issuance of an Open Badge. Hosting of badges publicly also removes the option of storing sensitive data within an Open Badge, as this information would be viewable by the public.

OPEN BADGES USE CASES

The above characteristics and security profile make Open Badges well-suited for the use cases it was designed for – low-stakes educational credentials, sometimes referred to as "micro-credentials." In this context, "low-stakes" is not a value judgment but a description of the social weighting of the credential. A low-stakes credential is not relied upon for high-stakes engagements such as performing surgery, piloting an aircraft, or validating identity to receive government benefits or cross a border. Instead, low-stakes credentials index personal and professional achievements that may or may not "stack up" over time to a high-stakes credential.

For example, the information contained within an educational transcript is considered private to the student and the institution. Accordingly, this use case is likely not well-suited for a hosted Open Badge solution. Detailed information found on transcripts may contain sensitive information like individual grades, birth dates, and other information that should not be floating publicly on the World Wide Web. Documents with sensitive personally identifiable information (PII) must remain private unless expressly disclosed to an intended viewer. Similarly, because badge images and badge content are hosted separately, an attacker could alter a badge image to point to another person's transcript, and the badge would still validate. This attack vector should be precluded for sensitive digital records.

A more appropriate use for Open Badges is recording professional achievements, course completion, distinction awards, professional skill development, and attainment of personal goals. A report funded by the U.S. Department of Education's Office of Vocational and Adult Education (OVAE) found that Open Badges show particular promise for certifying the skills of adult learners in basic education programs or who have obtained specialized skills in unique settings that do not create formal credentials, such as in the case of skills obtained during the course of military service.[10] Badges would memorialize the training or skill, and the badge itself would create value within an extended context. Within healthcare, completion of coursework as part of Continuing Medical Education (CME) may be an appropriate use of Open Badges. Examples of badging use cases can also be found at Boston University[11] and the American Occupational Therapist Association.[12]

OPEN BADGE VERIFICATION

To verify an open badge, the relying party accesses a Badge Validator website and inputs the badge's URL, JSON, or JWS cryptographic signature (if the badge has been signed, which is rare). The Validator checks the Badge's hosted JSON data to verify it has not been changed. It also verifies whether a badge has expired or been revoked. Examples of Open Badge 2.0-compliant validators include the Badgr Validator (https://badgecheck.io/) and the IMS Global Validator (https://openbadgesvalidator.imsglobal.org).

Validators that comply with the Open Badge 2.0 standard can be considered vendor independent because they are compliant with the most recent version of the open standard. However, badge vendors are not required to comply with any digital badging standard. For this reason, badge vendors generally direct customers to use their own validators for badges that have been issued using that vendor's system. For these badges, verification is dependent upon the continued existence of that vendor and their support of that particular badge implementation.

CONCLUSION

The Open Badges 2.0 specification supports many of the technical requirements needed to support independent verification of credentials; however, the full specification is not usually implemented. If implemented appropriately, i.e., with Digital Signatures, selective hosting, and metadata extensions, Open Badges could effectuate an evolution in credentialing and be used to document events, such as progress towards compliance with continuing medical education requirements or completion of training or education specific to an individual hospital or institution.

Open Badges could effectuate an evolution in credentialing and be used to document events, such as progress towards compliance with continuing medical education requirements or completion of training or education specific to an individual hospital or institution.

2.3 BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY

Blockchains are distributed ledgers that keep a synchronized record of transactions across their network of "nodes." Each transaction is timestamped and appended to the previous record of transactions making it, in principle, uneditable. This creates several advantages for the verification of claims:

Independent, Decentralized Verification. A robust, decentralized network is a durable way to verify credentials that require long-term validation. Strong cryptography coupled with a global verification network, such a blockchain, also creates the capacity for instant and free verification of claims. A decentralized global verification network is not nearly as vulnerable to institutional collapse, corruption, hacking, natural disasters, or disasters of war as is a centralized database. Opportunities for falsification and fraud along several attack vectors are virtually eliminated.

Independent Timestamping. A decentralized network on the blockchain model provides a permanent and trusted timestamp by design. To undermine a blockchain timestamp would require massive computational effort—rewriting the entire blockchain—to tamper with data before a certain point. The blockchain provides an independent timestamp for when each credential was conferred to a recipient. This gives issuers the ability to rotate their signing keys without undermining the ability of third parties to reliably verify records issued by previously-used keys. Verifying a credential requires checking that it originated from a particular Issuer while that issuing key was valid, which requires knowledge of the timestamp. Blockchains provide this knowledge.

Ownership of Digital Assets. Blockchains record transactions in which something of value is transferred from one party to another. As Michael Casey and Paul Vigna state in *The Truth Machine: The Blockchain and the Future of Everything*: "Blockchains point the entire digital economy towards something called the 'Internet of Value.' Whereas the first versions of the Internet allowed people to send information directly to each other, in the Internet of Value people can send anything of value to each other, be it currencies, assets, or valuable data that was previously too sensitive to transmit online."[13] With blockchains, digital assets can no longer be duplicated; meaning, they can be safely transferred between owners. This also makes fraud via impersonation much more difficult, as anyone attempting to use someone else's asset will not be able to prove ownership of that asset. The definition of "asset" extends to credentials and other official records.

Blockchains are beginning to be used for records verification worldwide due to their ability to serve as resilient, convenient notaries of unique, high-stakes claims. Some Open Badge providers, like Credly, are beginning to anchor badges to blockchains, and some Digital Signatures providers, like DocuSign, are offering or looking to offer blockchain timestamping for PDF records. However, blockchain technology has also inspired the development of record types that are natively anchored to the chain and maximize the blockchain benefits of asset ownership, portability, and vendor-independent verification.

BLOCKCERTS

The breakthrough promise of blockchain technology is the ability of individuals to directly own, share, and validate their digital assets. These digital assets may include money, like cryptocurrency, or other assets, like credentials. Credentials that may be owned and shared using blockchain technology include land titles, intellectual property, wills, insurance documentation, identity records, e.g., driver's licenses and passports, health records, verified resumes, employment verifications, and academic credentials. Although legacy digital record formats like PDFs and Digital Badges may be timestamped to a blockchain for later verification, the characteristics of the blockchain network have prompted the development of new records formats that take full advantage of the blockchain's unique asset ownership characteristics.

Blockcerts is a global open standard for blockchain records that employs many of the characteristics of Open Badges and PDFs while enabling more certain and flexible digital ownership, parsing, sharing, and verification of claims. Because it is rooted in the educational space and is currently the most widely-adopted open standard for blockchain-based records, the FSMB applied the Blockcerts standard in its evaluation of using blockchain technology for credentialing in a pilot project completed in late 2017.

Blockcerts arose as part of a project by the MIT Media Lab to anchor academic credentials to a blockchain. The intent of the project was to enable decentralized verification of credentials through the use of an independent verification infrastructure—a blockchain. The Media Lab invited engineers from software firm Learning Machine to contribute to the project, and in 2016 the first version of the Blockcerts open standard was launched at blockcerts.org. The Blockcerts reference libraries are published under an MIT Free and Open Source Software (FOSS) license, making the code free to use by any developer or institution to build their own applications for issuing, receiving, storing, and verifying Blockcerts.

Like Open Badges, Blockcerts is also a technical standard for bundling information about an individual, embedding it into a portable file, and validating the file through a standard technical infrastructure. Blockcerts is a digital document type that unifies data and display in a single file (JSON). It also allows for the incorporation of rich data and flexible displays into the record. This means that any record type may be issued as a Blockcert. Each Blockcert file includes the recipient's cryptographic identifier (public key), is cryptographically signed by an issuer, and its hash is registered on a blockchain for decentralized verification.

The process of anchoring a Blockcert hash to a public blockchain, for example, Bitcoin or Ethereum, involves paying a small transaction fee to the blockchain network. This is because public blockchains are like toll roads - they are funded by those who use them in a decentralized manner. Private blockchain networks, on the other hand, generally do not require transaction fees, as they are funded in a centralized manner by a governing body. Blockcerts may be anchored to both public and private chains. Implementations on Bitcoin, Ethereum, and Hyperledger are in production as of March 2019.

Finally, the Blockcerts open standard also offers a free, open source mobile app, available for both iOS and Android. The Blockcerts Wallet acts as a private portfolio of records owned exclusively by the recipient. It allows recipients to generate keys, connect with issuers, receive and hold credentials, and easily share them and demonstrate ownership when needed.

DIFFERENCES BETWEEN BLOCKCERTS AND TRADITIONAL OPEN BADGES

Blockcerts was developed based on the Open Badges specification for digital records, described in Section 1.2. However, Blockcerts makes several changes to the Open Badges specification which allow it to be used for the verification of a wider range of high-stakes claims and private data.

Flexible Form Factor. A flexible document display is embedded in the Blockcert JSON file. This offers more flexibility than relying on a single, static image and also allows the record type to generate many types of reliable displays. Accordingly, Blockcerts can be easily used to represent any designed form factor such as diplomas, transcripts, professional certifications, licenses, and others.

Display Integrity. The Blockcert code generating the credential display is cryptographically signed by the issuer. This means the integrity of the visual Blockcert display is also verified during the verification process. By contrast, Open Badges use an image display to point to the real credential, which is defined as a hosted JSON dataset. This separates display and data, allowing for changes to the display of the badge without affecting verification. For workflows that need a reliably human-readable version of designed credentials, Blockcerts are preferable.

Digital Signatures. While few Open Badges are digitally signed in practice, Blockcerts are digitally signed by default. This ensures document integrity and issuer authenticity verification. Where badges are signed, it is the image that is signed as opposed to the hosted JSON dataset which holds the badge data.

Offline Sharing and Verification. Signing Blockcerts allows for ongoing verifiable display of records whether they are hosted or not. A Blockcert may, of course, be hosted for easier online sharing via a link. However, if the hosted version of the Blockcert is removed, the Blockcert can still be viewed and verified using only the JSON file. Because the file is self-contained with all of the information necessary for verification, dropping that record into the open source Blockcerts Universal Verifier is sufficient to verify every part of the record. The ability to verify an offline record is also important because online hosting is not desirable for records that contain sensitive information, for example, passports, academic transcripts, and medical records.

Recipient Ownership. Blockcerts embeds the cryptographic keys of recipients into their credentials so they can demonstrate ownership. Currently, Open Badges do not support this type of control.

BLOCKCERTS VERIFICATION

There are several ways for a relying party to verify a Blockcert:

1. Hosted Blockcerts may be verified by clicking a “Verify” button embedded in the certificate web view
2. The URL of the hosted Blockcert may be pasted into the Blockcerts Universal Verifier at blockcerts.org
3. The Blockcert file may be uploaded to the Blockcerts Universal Verifier at blockcerts.org
4. The Blockcert QR code may be scanned by a QR code reader
5. Blockcerts may be verified directly in a Blockcerts Wallet

To verify a Blockcert, the open source Blockcerts Verifier generates a new hash of the local document — the document being verified — and compares it to the hash of the original document, which has been stored on the blockchain. The Verifier detects the correct blockchain and transaction. When both hashes match, the relying party knows that nothing in the document has been tampered with. Like the Open Badge Validator, the Blockcerts Verifier also validates the issuer's profile and Digital Signature and confirms whether a record has expired or been revoked.

Like Open Badges, the current version of Blockcerts as of May 2019 relies on issuers to host some information about themselves in the place of a Certificate Authority. It is considered a best practice for issuers to host their own profiles directly, rather than relying on a software provider, which creates a vendor dependency. Along these lines, issuing institutions may also host their own lists of revoked Blockcerts.

Although vendor dependency is removed when issuers host their own profiles, issuer hosting does create a dependency on the issuer for ongoing credential verification. Should an issuer go out of business or find themselves subject to conflict or natural disaster, the issuer profile would need to be hosted in a safe location to maintain credential verifiability. The next generation of Verifiable Credentials being developed by the W3C includes new technologies like Decentralized Identifiers (DIDs) that will remove lingering issuer dependencies. For this reason, Blockcerts will eventually employ this new credential verification technology. Section 1.5 provides a fuller description of Verifiable Credentials. This is worth noting for future consideration but does not provide functionality that would be available for a current technology selection.

BLOCKCERTS USE CASES

The current state of Blockcerts is appropriate for use cases where secure credentials are required. There are many examples not related to healthcare credentialing, but we will focus on ones that are. These examples include:

- Education: Diploma, Transcript, Enrollment Verification, Licensing Examination Results, Education Verification, Clinical Training Verification
- Ongoing: License to Practice Medicine, Professional Credentials, i.e., employment

The above list of use cases is not exhaustive. Any record that must be verified with the highest degree of certainty can be issued as a Blockcert. In the future, this technology could potentially evolve to be sufficient for personal identification use cases, like passports. This will require additional technologies such as Decentralized Identifiers (DIDs), Guardianship, Key Recovery, W3C's Verifiable Credentials, biometrics, and a fully-featured recipient mobile wallet.

NOT ALL "BLOCKCHAIN CREDENTIALS" ARE BLOCKCERTS

The prominence and availability of Blockcerts open reference libraries has prompted some digital credentials providers to adopt portions of its codebase to anchor records or claims to a blockchain. However, these providers are typically not implementing the recipient ownership, blockchain-agnosticism, and independent verification features of Blockcerts. This lowers the longevity and utility of the blockchain-anchored credential by preserving the dependency of both issuing authorities and recipients on the software vendor's own infrastructure for ongoing credential access and verification. Accordingly, any institution intending to implement blockchain credentialing for high-stakes records

should verify whether or not their provider is fully compliant with open standards. This can be easily checked by testing whether or not a blockchain credential issued by the provider verifies in the Blockcerts Universal Verifier at blockcerts.org.

Any institution intending to implement blockchain credentialing for high-stakes records should verify whether or not their provider is fully compliant with open standards.

A NOTE ON CREDENTIAL WALLETS

In order to cryptographically claim ownership of a Blockcert record, a recipient must download the free Blockcerts mobile app "Blockcerts Wallet" and respond to an invitation from the issuing institution. Responding to the issuer's invitation — generally by clicking a link in an email — sends the issuer the recipient's public key, which is then embedded in their Blockcert as a recipient identifier.

With recipient ownership comes the added responsibility of maintaining these records. User familiarity with credential wallets will become important, while standards and portability between wallets will be necessary if the credentials are to be truly durable. This was the rationale behind building the Blockcerts Wallet on open standards and publishing the Wallet code as open source reference libraries. Any wallet built using the Blockcerts Wallet standard will be able to receive, store, share, and verify Blockcerts issued by any software vendor and institution, and to facilitate records transfer between other standards-compliant wallets.

Of course, Blockcerts is not the only model for a credential wallet. Credential wallet software is currently undergoing rapid development by many different providers. Some wallets use the Blockcerts open standard; some (Civic, ODEM) use proprietary vendor wallet software; and others are building wallets that employ the Verifiable Credentials open standard (uPort, VeresOne, Sovrin). Although still a draft specification, Verifiable Credentials is undergoing rapid development. Blockcerts will transition to a Verifiable Credentials model as it is made production-ready (see Section 2.5). This will ensure that Blockcerts are transferable between all Blockcerts-based and Verifiable Credentials-based wallets.

Finally, best practices in wallet operational security will prevent attack vectors on credential wallets. High-profile stories of individuals having their private keys compromised and their digital assets stolen arise from a failure to adhere to these best practices. For example, wallets that allow recipients to define their own private keys suffer from the same shortcomings as passwords: individuals often select insecure keys that are easily guessed by attackers. Similarly, mnemonic seeds that can be used to regenerate private keys in a new wallet must be highly secure (long, random) to be effective. In addition, wallets that reveal private keys to authorized users create the risk that the users will store those private keys in an insecure manner. For the above reasons, Blockcerts Wallet never reveals a user's private key; does not allow them to choose their mnemonic seed; and generates the user's private key on their behalf.

INSTITUTIONS USING BLOCKCERTS

While anchoring records to a blockchain is still a relatively new approach, many fully deployed examples of Blockcerts usage exist across geographic regions. Incorporation of Blockcerts is occurring at national, organizational, and individual institution levels.

- On a national scale, the Republic of Malta has been issuing Blockcerts through select institutions since 2017 and recently began issuing Blockcerts credentials to all educational institutions in the country, which includes over 120 institutions covering vocational training, primary K-12 education, and higher education institutions. The Government of Canada began issuing Blockcerts to credential highly-skilled public sector employees called “Free Agents” as part of a 2019 pilot program with the new Talent Cloud initiative.
- Organizations responsible for establishing consensus in the academic or medical communities have integrated Blockcerts into their processes. The Accreditation Council for Graduate Medical Education (ACGME) began issuing Blockcerts to gradutes of medical programs as part of a 2019 pilot. The Caribbean Examinations Council (CXC), which serves test takers across 19 countries in the Caribbean and Latin America, began issuing examination results as Blockcerts in 2018.
- Individual institutions, spanning from research universities like MIT to community colleges such as Central New Mexico Community College, have begun to issue diplomas through Blockcerts. Beginning in 2018, MIT issues Blockcerts for all graduating students, including undergraduate, graduate, and doctoral-level graduates.

This early adoption of Blockcerts for educational records and professional development overlaps with the emerging values of digital identity movements like Self-Sovereign Identity (SSI) and GoodID, led by the Omidyar Network, World Economic Forum, and World Bank ID4D Initiative. These identity movements value individual empowerment by adhering to principles such as recipient control and consent, record interoperability, privacy by default, and more. As educational institutions look for ways to empower their students and graduates, many of them find that these same principles provide useful guidelines for records management while improving the potential success of their students entering the global workforce.

Specific to the healthcare credentialing use case, Blockcerts may be a viable solution to addressing many of the critiques of the current process, including portability and the need to reduce redundancy. The pilot project completed by the FSMB in late 2017 illustrated that Blockcerts can provide the level of certainty and validity needed to implement blockchain technologies in the medical licensing and credentialing process. Ensuring that credentials are authentic and resistant to forgery is crucial for system-wide adoption of the standard. Equally as important is the acceptance by relevant parties such as state medical boards, hospital credentialing staff, and insurance companies. Improvements to wallet functionality may alleviate concerns that physicians may have a wallet that is specific to one or more documents and may be a step that not only improves the portability of credentials but facilitates systemwide adoption.

2.4 DIGITAL CREDENTIALS COMPARISON TABLE

	Digital Signatures (Docusign)	Open Badges	Blockcerts
In Use Since	1977 Continuously evolving in multiple permutations with increasing levels of security.	2011 Most current standard as of report publication is Open Badges 2.0.	2016
Format	PDF Fixed layout flat document containing text and image data together in a human-readable display format.	PNG and JSON Fixed image format usually confined to a simple shape. This image may point to hosted JSON data about the badge.	JSON Contains both text and image data and can generate any type of display for web, mobile, and print.
Data	Flexible data format.	The standard OB framework contains a core set of data, expandable with OB extensions.	Flexible data format. Currently starts with OB core dataset.
Timestamping	Yes	Yes	Yes
Data Integrity & Tamper Evidence	Yes Digital signatures display tamper evidence of both display and supporting metadata.	No Hosted assertions could be modified by the issuer and still pass verification.	Yes Digital signatures and blockchain hashing display tamper evidence of both display and supporting metadata.
Credentials Type/Ideal Use Cases	Legal agreements between multiple parties; high-stakes credentials; diplomas and degrees; academic transcripts; wills; professional licenses; property titles; vital records (birth/death/marriage certificates); proof of insurance.	Micro-credentials representing a single skill or achievement: course completion, skill attainment, or milestone achievement.	High-stakes credentials; diplomas and degrees; academic transcripts; verification of past education; professional licenses; property titles; vital records (birth/death/marriage certificates); ID cards; driver's licenses; passports; proof of insurance.
Shareable (Online & Peer to Peer)	Yes	Yes	Yes

	Digital Signatures (Docusign)	Open Badges	Blockcerts
Revocable	No. An authority's signing keys may be revoked, but this will not revoke, or invalidate, the Digital Signatures used to sign documents that have already been digitally signed by that authority.	Yes	Yes
Expirable	No. Certificates documenting ownership of signing keys may expire, but Digital Signatures already made by the owner of those signing keys do not.	Yes	Yes
Legally Enforceable	Yes	Unsigned badges are not legally enforceable. Badge signatures sign only the PNG (image file), not the badge data.	Yes
Dependency	Certificate Authority, verification service provider, issuing institution.	Badging vendor and issuing institution (hosted badge, issuer profile, and revocation list).	Issuing institution (hosted issuer profile and revocation list).
Self Sovereign[14]	No. Recipient keys (identifiers) are not used. Doesn't verify without the verification service provider.	No. Recipient keys (identifiers) are not used. Verifies in a vendor-independent manner only if compliant with OBI 2.0 standard.	Yes. Recipient keys (identifiers) used. Vendor-independent verification in the Blockcerts Universal Verifier.

2.5 AN EYE TOWARD THE FUTURE

The future of credentialing and technological standards employed to ensure validity and authenticity remain fluid. The following two sections highlight two areas of note, especially relevant to those looking at long-term viability of their chosen mode of digitization.

W3C VERIFIABLE CREDENTIALS

While this Report is focused on available technologies, it is important to note how the space is evolving to help ensure choices today aren't outmoded in the future. Therefore, this Report anticipates the ongoing work of the World Wide Web Consortium (W3C) for Verifiable Credentials. The weight of major players (Microsoft, Mastercard, Sovrin, Learning Machine) contributing to or committing to use the Verifiable Credentials schema suggests that it will be a major standard for digital credentials in the future.

The W3C is the primary international standards organization for the World Wide Web. Originally formed by Tim Berners-Lee in 1994, the standards organization has grown to 476 members as of October 2018. In 2013, the W3C Credentials Community Group began work in the credentials space with the intent of enabling the secure expression of verifiable information via the Web. This initiative was soon followed by the Rebooting Web of Trust Community and W3C Verifiable Claims Working Group, since renamed Verifiable Credentials.

The Verifiable Credentials draft specification includes a bundle of concepts, approaches, and base technologies like Digital Signatures to provide a lightweight structure for expressing a wide range of digital credentials. The goal is not to create a new type of digital credential. Rather, it is to provide flexible structure for adherence, enabling any type of digital credential to be shared on the Web. This effort is guided by a belief that online credentials should be privacy respecting, cryptographically secure, and machine verifiable.

In many ways, Open Badges and Blockcerts are precursors to Verifiable Credentials, as they both formalized certain approaches for creating digital credentials. As they continue to evolve, it is likely that both will support the new Verifiable Credentials specification, since these approaches are compatible in purpose and data models, and all would gain additional benefits from alignment. In fact, Blockcerts has already pledged to remain aligned with Verifiable Credentials as the draft specification becomes finalized.

2.6 DEVELOPING LEGAL AND REGULATORY STANDARDS

Legal and regulatory standards for Digital Signatures in both the US and EU heavily reference traditional cryptography and PKI infrastructure, particularly with reference to the discretion and influence exercised by Certificate Authorities. With a Decentralized PKI model as employed by blockchains, some of the functions previously performed by a Certificate Authority can pass to a decentralized infrastructure. These functions include timestamping, key storage, and certificate expiration and revocation.

In anticipation of this change, the European Parliament passed a "Resolution on Distributed Ledger Technologies and Blockchains" on October 3, 2018. It articulated the value of disintermediation for multiple sectors and industries: identity, healthcare, education, supply chain management, and many others.

This Resolution anticipates future regulation of Distributed Ledger Technology (DLT) and the changing role of Trust Service Providers under a decentralized framework. Its Section 17 explicitly references Blockcerts as a valuable application of blockchain-based certification.

In the United States, multiple states, including Arizona, Tennessee, and Nevada have passed legislation to ensure the legal validity of smart contracts and Digital Signatures anchored in blockchains. However, the Uniform Law Commission and the Digital Chamber of Commerce, a blockchain advocacy group, argue that existing law provides sufficient legal grounds for the acceptance of blockchain-based smart contracts and Digital Signatures.[15] How these are treated in the legal system remains to be seen, but it is likely, given the similarities in the technologies involved, that cases will prove analogous to those already litigated over Digital Signatures.

3. RECOMMENDATIONS & CONCLUSION

The processes of issuing and maintaining these credentials, like many administrative functions, is deeply rooted in the past and may not be viable for the needs of the current and future healthcare environment. The current state of physician licensing and credentialing is inefficient, has security concerns, and gives ownership of an individual's credentials to institutions and not the individual. Many of the existing inefficiencies and security concerns can be improved with current, proven technologies. Adoption of these technologies and new processes to support them today will pave the way for adoption of future technologies, such as the W3C Verifiable Credentials standard.

There must be industry-wide willingness to evaluate process and implement changes that specifically address existing inefficiencies and barriers.

To achieve the promise of the technologies highlighted in this Report, there must be industry-wide willingness to evaluate process and implement changes that specifically address existing inefficiencies and barriers. These barriers not only slow down the process for the physician and the end-users of physician credentials but also compromise public safety. Current data silos within healthcare propagate gaps in the data available to regulators and credential specialists, ultimately inhibiting access to the very data necessary to provide insight or evaluation into a physician's ability to provide safe and effective care to a patient. If the shared goal of public protection is to be fully realized, data must flow seamlessly across organizations, networks, federal and state regulators, and the system as a whole. Recognizing the need to change is always the first step in a successful systemic improvement plan. In recent years, the FSMB has joined together with its member state medical boards and other interested stakeholders to not only study issues such as license portability, physician wellness and burnout, and the duty to report sexual boundary issues, but to effectuate real change. In this spirit, the FSMB urges its colleagues in the House of Medicine, as well as national regulators and accreditation bodies, to recognize the need to improve and to engage in collaborative efforts to explore digital credentials.

Digital credentialing could usher a wave of evolution in how each organization operationalizes its commitment to public protection. Digital credentials may catalyze a shift from the current model of public protection focused on technical compliance and complaint-driven enforcement. The value of current, portable, and trusted digital credentials is essential to the success of risk-based regulatory frameworks, where systematized frameworks and procedures prioritize regulatory activities and interventions in proportion to risk. For example, digital credentials may free up state licensing staff or medical staff

professionals from the daunting collection and review of paper-based documents and allow their efforts to focus on staff management, ongoing compliance and enforcement efforts, and improved quality standards. The research in this paper shows that there are multiple technical solutions that meet legal and regulatory requirements and at the same time deliver document portability, independence, and the level of trust patients expect in modern healthcare delivery models.

Digital credentials may free up state licensing staff or medical staff professionals from the daunting collection and review of paper-based documents and allow their efforts to focus on staff management, ongoing compliance and enforcement efforts, and improved quality standards.

By beginning now, the FSMB is an early mover; however, it will adopt and maintain an evolutionary approach. Its first step will be to update its systems to "unbundle" credentials to their base elements to allow them to be delivered individually. For the FSMB, this step is required in order to adjust its workflow and deliver products to meet future needs. These changes are made with a clear understanding that the mechanism to deliver these documents will change over time. *It is expected that the first incarnation of these documents will be delivered using digital certificates.*

For organizations considering adopting a new model, it is worth considering the following maxims that have been identified through recent FSMB projects and collaborations in the credentialing space:

1. Don't implement technologies because they are shiny and new, but because they meet requirements. Blind adoption of blockchain solutions fall into this category, particularly permissioned blockchains.
2. Empire-building will not be successful. Successfully enabling the portability of credentials requires actors participating in a networked ecosystem; it does not require the building of new, fee-based, centralized databases. Attempts at creating new centralized credential databases have been attempted in recent years, but have not been successful in part because they go against the main tenant of empowering self-ownership of credentials.
3. Data standards are key to automation and must be pursued. The creation of the VGMET form for medical training was a pivotal step forward for GME data. This standard, endorsed by key national bodies (ACGME, AHA, NAMSS, OPDA) enables source institutions to utilize technology to issue a durable, reusable credential document. This is the first step in removing redundancies, and such a standard should be sought for all document types.
4. Standards for tools should be sought as well. Success will require multiple tools, implemented by multiple solution providers. Wallet applications and portfolio systems are examples. Having to maintain a tool - app or otherwise - to support a single document is not a tenable solution. Organizations should work together to create prevailing standards that support documents issued from multiple sources, and vendors should offer tools that provide portability across platforms.

The digital transformation in credentialing is still in its early days, and the FSMB looks forward to working with our constituents, including state medical boards, other users of its verified documents, and the educational institutions who so often act as source information providers and who are also looking at new models of delivering and consuming credentials. If the potential of digital credentials to provide an enhanced trust framework for the needs of today and tomorrow is to succeed, the conceptual and exploratory work must be systemically aligned and never lose focus on the role credentials have in protecting the public against harm.

GLOSSARY

Asymmetric Cryptography: The use of public and private keys to encrypt and decrypt data. The keys are a set of large numerical strings that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Blockchain: A type of distributed ledger in which modifications to the ledger are appended as "blocks" of transactions, ordered sequentially in time. Once a block has been appended to the series of previous blocks, it is cryptographically signed, replicated across nodes running the database protocol, and can no longer be altered by any database user. In other words, a blockchain can be thought of as an append-only, immutable database of transactions. Blockchains were originally used to maintain records of ownership of digital currency, thereby preventing its replication (and devaluation). This allowed digital currency to come into wide use for the first time with the Bitcoin protocol. However, the same technology primitives can be employed to verify the integrity of and track ownership of any digital asset, including a medical credential.

Certificate Authority (CA): A third-party service which certifies ownership of public keys by issuing Digital Certificates.

Decentralized Identifiers (DIDs): A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network.

Digital Signature: A means of creating an electronic signature that is unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data in a manner such that if the data is changed, the signature is invalidated.

Distributed Ledgers (DLT): A database that is consensually shared and synchronized across multiple sites, institutions or geographies. The participants at each node of the network can access the recordings shared across that network and can own an identical copy of it. Further, any changes or additions made to the ledger are reflected and copied to all participants. A blockchain is a type of distributed ledger.

JavaScript Object Notation (JSON): A lightweight data-interchange format based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, such as C, C++, C#, Java, JavaScript, Perl, and Python.

JSON Web Signature (JWS): A compact signature format intended for space constrained environments such as HTTP Authorization headers and URI query parameters. It represents signed content using JSON data structures. The JWS signature mechanisms are independent of the type of content being signed, allowing arbitrary content to be signed.

Personally-Identifiable Information (PII): Information meant to identify a specific individual, which often includes data such as a name, Social Security number, driver's license number, financial accounts, email addresses, login credentials and passwords, addresses, phone numbers, and birth date.

Primary Source Verification: Verification of an individual's reported credentials and qualifications conducted through communication with the organization or governmental entity that issued the document or credential, or through a designated equivalent source. Methods for conducting primary source verification include direct correspondence with the issuing source, such as through a documented telephone conversation or by facsimile, email, or other electronic means.

Public Key Infrastructure (PKI): The set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public keys. Portable Network Graphic (PNG) Format. The PNG format was created in response to limitations with the GIF format, primarily to increase color support and to provide an image format without a patent license. PNG files are commonly used to store graphics for web images.

Secure Socket Layer (SSL): A security protocol that enables secure communications between two machines. An SSL certificate is a small data file leveraging this security protocol to serve two functions. One is that SSL certificates serve as credentials to authenticate the legitimacy of a website. Second, when SSL is installed on a web server, it enables the padlock to appear in the web browser and activates the HTTPS protocol to secure the connection between the web server to a browser.

Scalable Vector Graphics (SVG) Format: A graphics file that uses a two-dimensional vector graphic format created by the World Wide Web Consortium (W3C). It describes images using a text format that is based on XML and was developed as a standard format for displaying vector graphics on the web.

Transport Layer Security (TLS) certificate: An updated version of SSL that provides advanced encryption options including Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA), or Digital Signature Algorithm (DSA).

END NOTES

[1]See Open Identity Exchange, TRUST FRAMEWORKS FOR IDENTITY SYSTEMS (June 2017), https://www.openidentityexchange.org/wp-content/uploads/2017/06/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf
[2]E.g. RCW18.71.050.
[3]42 C.F.R. § 482.
[4]See e.g., Garland Community Hospital v. Rose, 156 S.W.3d 541 (Tex. 2004) (When a plaintiff's credentialing complaint centers on the quality of the doctor's treatment the hospital's alleged acts or omissions in credentialing are inextricably intertwined with the patient's medical treatment and the hospital's provision of health care).
[6]Federation of State Medical Boards, REPORT OF THE SPECIAL COMMITTEE ON UNIFORM STANDARDS AND PROCEDURES (1998).
[7]Federation of State Medical Boards, REPORT OF THE SPECIAL COMMITTEE ON LICENSE PORTABILITY (2002), https://www.fsmb.org/siteassets/advocacy/policies/grpol-license-portability.pdf
[8]Federation of State Medical Boards, REPORT ON PHYSICIAN WELLNESS AND BURNOUT (2018), http://www.fsmb.org/siteassets/advocacy/policies/policy-on-wellness-and-burnout.pdf
[8]State enactments of UETA supersede the provision of ESIGN Section 7001. Conducting certain transactions through electronic means (such as family law or probate) may be prohibited. However, the minor differences between the two statutes, as well as the minor prohibitions, are irrelevant for the purposes of the analysis in this paper, as the substantive effect of both statutes allow for credentialing transactions to be recognized as lawful if conducted in a digital format.
[9]Turner, Dawn M. 2016. "Advanced Electronic Signatures for eIDAS." Cryptomathic. 21st April. https://www.cryptomathic.com/news-events/blog/advanced-electronic-signatures.
[10]American Institutes for Research, THE POTENTIAL AND VALUE OF USING DIGITAL BADGES FOR ADULT LEARNERS (2013), https://lincs.ed.gov/publications/pdf/AIR_Digital_Badge_Report_508.pdf
[11]http://www.bu.edu/busmplus/accme/
[12]https://www.aota.org/Education-Careers/Continuing-Education/digital-badge.aspx
[13]Michael Casey and Paul J. Vigna, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING, 13 (2018).
[14]We use two major thematic criteria to determine whether a record format is self-sovereign: 1) Demonstrable recipient ownership of the credential; and 2) Vendor-independent use and verification of the credential. Another way of describing a self-sovereign credential is that it is "self-attesting." See Christopher Allen, "The Path to Self-Sovereign Identity," for additional details: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[15]Uniform Law Commission, Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal ESIGN Act, Blockchain Technology, and "Smart Contracts" (2019) ("UETA already adequately encompasses blockchain and smart contracts, and changes to specifically address these technologies are not only unnecessary but also detrimental."); Digital Chamber of Commerce, Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable, https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf

Sources and Additional References

Allen, Christopher. "The Path to Self-Sovereign Identity." Life with Alacrity. April 25, 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Association of Corporate Counsel. "Contracts 2.0: Making and Enforcing Contracts Online." September 2012. https://www.venable.com/files/Publication/2ca2d13e-6b3a-486c-b644-028552542e12/Presentation/PublicationAttachment/68ba86d1-6009-4875-bd51-0dd146b361d5/Making_and%20Enforcing_Contracts_Online.pdf

Casey, Michael and Paul J. Vigna, The Truth Machine: The Blockchain and the Future of Everything. New York: St. Martin's Press, 2018.

Chamber of Digital Commerce. 2018. "'Smart Contracts' Legal Primer: Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable." January. https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf.

Cornell Law School, Legal Information Institute. "Adhesion Contract (Contract of Adhesion)." https://www.law.cornell.edu/wex/adhesion_contract_%28contract_of_adhesion%29

Council of the European Union. 2014. Regulation (EU) "No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC." https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014R0910

DocuSign. "Electronic signature laws by state." https://www.docusign.com/esignature/electronic-signature-laws-state

DocuSign. "US electronic signature laws and history." https://www.docusign.com/learn/us-electronic-signature-laws-and-history

DocuSign. "The eIDAS Regulation: A primer." https://www.docusign.com/learn/eidas-regulation-primer

Duffy, Kim. "W3C Credentials Community Group Charter." W3C. 19th October, 2017. https://www.w3.org/community/credentials/charter/

European Commission. "EU Trusted Lists." https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers.

European Parliament. 1999. "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

European Parliament. 2018. "Distributed ledger technologies and blockchains: building trust with disintermediation." http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN&ring=B8-2018-0397

Sources and Additional References

Kimpel, Scott and Chris Adcock. 2018. “The State of Smart Contract Legislation.” 5th September. https://www.blockchainlegalresource.com/2018/09/state-smart-contract-legislation/?utm source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

Mendelsohn, Stephen A. 2012. “U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures.” National Law Review. 2nd January. https://www.natlawreview.com/article/us-department-education-amends-its-ferpa-regulations-to-allow-certain-additional-student-dis

Merkle, Ralph. 1990. “A Certified Digital Signature.” In Advances in Cryptology — CRYPTO’ 89 Proceedings. Lecture Notes in Computer Science. Edited by G. Brassard. Vol. 435, pp. 218-138. New York: Springer. https://link.springer.com/chapter/10.1007/0-387-34805-0_21

Learning Machine Technologies. “Distributed, Trustless Timestamps: How adding the blockchain creates advantages over traditional PKI techniques.” Medium. 21st February, 2017. https://medium.com/learning-machine-blog/trusted-timestamps-bbeb3d29cc0

National Conference of Commissioners on Uniform State Laws. 1999. “Uniform Electronic Transactions Act.” https://www.uniformlaws.org

New York Times Editorial Board. “How Silicon Valley Puts the ‘Con’ in Consent.” New York Times. 2nd February, 2019. https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html

Renieris, Elizabeth M. “Liability under GDPR and the Self-Sovereign Identity Model.” SSI Meetup. May 21, 2018. https://ssimeetup.org/liability-gdpr-self-sovereign-identity-model-elizabeth-renieris-webinar-4/

Renieris, Elizabeth M. “"Sensitive" says who?” hackylawyER. 19th January, 2019.