

February 12, 2019

Roger Severino  
Director, Office for Civil Rights  
U.S. Department of Health and Human Services  
Hubert H. Humphrey Building  
Room 509F  
200 Independence Avenue, SW  
Washington D.C. 20201

***BY ELECTRONIC SUBMISSION***

**Re: Consumer Technology Association Public Comments in Response to Request for Information on Modifying HIPAA Rules to Improve Coordinated Care – RIN 0945-AA00**

Dear Director Severino:

The Consumer Technology Association (CTA™) appreciates the opportunity to submit comments in response to the U.S. Department of Health and Human Services Office for Civil Rights (OCR) Request for Information (RFI) to assist OCR in identifying provisions of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations that impact the ability to improve coordinated care.<sup>1</sup> OCR published the RFI in the Federal Register on December 14, 2018.

CTA is the trade association representing the \$398 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world’s best-known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world’s gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA’s industry services.

Consumer technology has evolved significantly since the HIPAA privacy and security regulations were first enacted. Consumers now expect to be able to use their smartphones and other devices to readily access sensitive financial fitness, and other information. New technologies allow

---

<sup>1</sup> 83 Fed. Reg. 64302 (December 14, 2018) [hereinafter RFI].

consumers to be engaged in their health care like never before. The consumer should be at the center of care coordination efforts. But the health care sector has not kept pace with these changes. Sometimes this is because of valid issues with HIPAA. More often it is because of misconceptions with HIPAA or obstacles created by other laws. We recommend that OCR use this rulemaking as an opportunity to further clarify an individual's right to receive health information through the consumer technology of their choice, and to eliminate perceived HIPAA-barriers to exchanging health information.

Health data and privacy and security are continually evolving concepts that require a dialogue among technology stakeholders, healthcare providers, patients and regulators. As patient preferences and comfort with technology evolve, so too will company products and services. Innovative technologies like artificial intelligence (AI) and machine learning continue to transform healthcare and the ways that healthcare providers and patients use data to improve care coordination, diagnostic accuracy, and quality of care. Patients increasingly want to be active participants in their own care and want to be able to monitor their health and wellness, and share their data with healthcare providers, applications, caregivers and family members.

CTA believes that collaboration among the healthcare sector, technology stakeholders, consumers, and OCR can help drive better patient care and facilitate better coordination across the healthcare continuum. The collection and sharing of health information is critical to improving the quality and safety of health care and advancing healthcare innovation that can improve the health and wellbeing of patients. That said, CTA recognizes the increased privacy and security threats targeting the healthcare sector as well as patients' concerns regarding the privacy and security of their Protected Health Information (PHI) and other sensitive health and wellness data.

Since its enactment in 1996, HIPAA has played an essential role in supporting the federal government's efforts to improve healthcare quality by facilitating the portability health information, building the privacy and security framework for research initiatives, ensuring awareness about data breaches, and responding to health emergency preparedness. More recent laws and regulations such as the Patient Safety and Quality Improvement Act (PSQIA) of 2005, the Health Information Technology for Economic and Clinical Health (HITECH) Act and the 21<sup>st</sup> Century Cures Act (Cures Act) have promoted interoperability, prohibited information blocking, and enhanced the usability, accessibility, privacy, and security of healthcare data.

Given the increasingly critical role technology plays in healthcare, CTA supports OCR's commitment reflected in the RFI to remove unnecessary regulatory obstacles and reduce regulatory burdens that inhibit care coordination and value-based care. CTA encourages OCR to update HIPAA to allow patients to use PHI in combination with modern technology while not sacrificing data integrity, accuracy and the completeness of a patient's health data.

We appreciate the importance and responsibility of preserving the confidentiality of health information as well as the challenges that OCR faces in potentially updating regulations to achieve a proper balance between the rights and responsibilities associated with promoting efficient coordinated care. CTA offers the following responses to the questions posted for public comment.

**General Comments:**

***The Need for Clarification-Protected Health Information (PHI)***

OCR has historically interpreted the definition of “protected health information” very broadly, treating it as any information of individuals, even publicly-available demographic information, if it is tied to a covered entity. As a result, the mere fact that someone has received care from a covered entity, without any information about the nature of the care or the individual’s condition, is treated the same as highly-sensitive diagnostic information. This creates significant liability for the handling of non-sensitive information. OCR has provided guidance that an appointment reminder generally can be sent via postcard in the mail, acknowledging that privacy of less sensitive information should be balanced with consumer convenience and costs. Yet entities are afraid to touch information that merely identifies that someone was once a patient of a provider, because such information comes with significant HIPAA compliance obligations and potential liability.

We recommend that OCR revise its interpretation of the definition of “protected health information,” limiting it to information that specifically identifies physical or mental condition, course of treatment, diagnosis, medical history, or details regarding payment of health care. The regulation should state that information that merely identifies that someone was a patient or plan member of a covered entity, where such information does not touch on a specific diagnosis, is not protected health information. This is more in line with other laws, including the definition of “medical information” in California’s very strict Confidentiality of Medical Information Act, it is a permissible interpretation of the HIPAA statute, it is more consistent with consumer expectations, and it will better allow care coordination by removing burden on sharing information that only identifies someone as a patient or plan member.

***The Need for Clarification-Business Associate***

The definition of *business associate* often creates confusion among covered entities and non-healthcare third parties. Covered entities often require third parties that are not acting on the covered entity’s behalf and, therefore, are not actually business associates—such as an app developer providing an app on the consumer’s behalf—to sign a BAA before the covered entity with exchange an individual’s information. This creates a variety of problems: it delays the exchange of information while the parties argue over the BAA; it requires the third parties to enter into a

contract, the BAA, that was not designed for their relationship; and it requires the third party to stand up a HIPAA compliance program, even though HIPAA was not designed to reach such third parties. Because BAAs are not applicable in many relationships between covered entities and third parties, further clarity from OCR is needed.

OCR has issued helpful guidance clarifying who is and is not a business associate, such as the *Health App Use Scenarios & HIPAA* at <https://hipaagsportal.hhs.gov>. We recommend that OCR include specific examples in the definition of “business associate,” such as that entities do not become business associates of each other when: (1) each organization is providing care coordination on its own behalf with respect to a common individual; and (2) when an entity is providing services to an individual, such as a personal health record, at the individual’s direction.

#### *The Need for Easier Access/Release of PHI*

With the increased adoption of technology by consumers in every facet of their lives, patients are similarly demanding the adoption of technology in the healthcare context. Patients want to play a more active role in making decisions about their health and want to be able to take advantage of technology tools that put them in control of their information and in the center of their care. In this respect, technology providers that provide patients with greater ability to access, store, organize, and share their health information should be treated as integral members of the care coordination team. Applications developed by technology third parties with significant experience in developing consumer engagement tools can provide a more user-friendly experience than has traditionally been the case. Unfortunately, even though HIPAA provides an individual with a right to have their protected health information sent to a third party of their choosing in their preferred form and format, most covered entities and business associate remain unwilling to do so.

To empower patients to best use consumer technology to manage their health information and care, we recommend three changes: (1) further clarifying the right of access to require disclosure to the individual’s choice of software application; (2) revising the definition of “treatment” to include care coordination involving software applications; and (3) revising the right to disclose to the individual to explicitly include disclosures to the individual’s choice of software application.

First, the right of access at 45 C.F.R. § 164.524 should be amended to more explicitly require covered entities to share information with a patient’s choice of technology providers. For example, we recommend that OCR consider the following change:

45 C.F.R. § 164.524(c)(2). *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable

hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) Upon an individual's request, the covered entity must transmit the information in a designated record set to a personal health record or other software application of the individual's choice, if the covered entity is able to do so without the purchase of additional technology. A covered entity may not refuse to transmit the designated record set to the individual's choice of software application based on the covered entity's concerns about the privacy or security of the individual's choice of software application. A covered entity is not liable nor have breach notification obligations under this subchapter for the acts or omissions of the entity that maintains or provides the software application. A covered entity may not delay transmission of the designated record set to the individual's choice of software application by requiring a business associate agreement or other contract or agreement.

Second, where the individual does not go through the formal process of requesting access, we recommend clarifying the Privacy Rule to explicitly include consumer technology in care coordination. For example, we recommend revising the definition of "treatment" at 45 C.F.R. § 164.501 as follows: "*Treatment* means the provision, coordination, or management of healthcare and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, the transmission of protected health information to a to a personal health record or other software application of the individual's choice, . . . ."

Third, we recommend that OCR amend the permission to share protected health information with the individual to include the individual's choice of technology. For example, we recommend revising 45 C.F.R. § 164.506(a)(1)(i) as follows: "A covered entity is permitted to use or disclose protected health information as follows: (i) To the individual, including to a personal health record or other software application when the covered entity has a good faith belief the individual has chosen such application to assist in managing the individual's care or payment; . . . ."

Disclosures to an individual's choice of software application should never require a formal authorization. First, it is based on the individual's choice, as evidenced by the individual choosing

the software application. Second, such authorizations create significant obstacles to the exchange of information. Covered entities often do not want to review a third party's authorization for compliance with HIPAA, instead insisting on the use of their own authorization form. A technology provider, however, cannot operationalize obtaining and completing each covered entity's unique authorization form.

#### Standardized Privacy Controls- The Security Rule

CTA recommends that the HIPAA Security Rule align with and provide standardized privacy/security controls to incentivize various entities including medical device manufactures, researchers, and service providers to act in compliance. Industry standard frameworks such as NIST 800-53 or ISO27001 should be specified by OCR to help standardized security and privacy controls and to provide standardized interoperability between health providers, facilities, systems and patients.

#### Specific Questions:

Question 3: *Should covered entities be required to provide copies of PHI maintained in an electronic record more rapidly than records maintained in other media when responding to an individual's request for access? (The Privacy Rule does not currently distinguish, for timeliness requirements, between providing PHI maintained in electronic media and PHI maintained in other media). If so, what timeframes would be appropriate?*

CTA believes that information maintained in an electronic record should be available more rapidly. However, CTA also believes that OCR must provide enough time for covered entities to provide the ePHI in a meaningful and organized format. Requiring a response time that is too short will lead covered entities to dump large amounts of data into useless files that will make it difficult for patients to effectively use. We recommend that HHS, through other regulatory vehicles, such as EHR certification standards, should continue to promote the availability of more protected health information to the consumer in real time and in interoperable, standard formats, expanding beyond the Common Clinical Data Set that is currently made available through certified EHR technology.

Question 4: *What burdens would a shortened timeframe for responding to access requests place on covered entities? OCR requests specific examples and cost estimates, where available.*

While CTA agrees that while OCR should implement a shortened timeframe to produce ePHI, OCR should not place unnecessary regulatory burdens on covered entities. CTA believes that individuals should have expedited access to ePHI, but more importantly the ePHI should be complete and accurate. Implementing a real-time access standard may be difficult as EHR systems vary in terms of the platform used and the information contained within the specific EHR. Additionally, although

there have been improvements for standardization, many covered entities have not adopted the standardized platform.

CTA also believes there is a disconnect in HIPAA between a patient's right to access a Designated Record Set and the type of data elements that are maintained by EHR systems. EHR systems are set up to deliver access to a limited standard set of data elements known as the Common Clinical Data Set (CCDS). However, HIPAA gives individuals the right to access all their information contained in the Designated Record Set. If the OCR implements a shorter timeframe to respond to requests, without building in time to obtain all the information contained in the fuller Designated Record Set, there is a likelihood that individuals would only receive what is in the CCDS—meaning patients would be receiving incomplete information. Given that not all the information in the Designated Record Set is readily available in a patient portal, many organizations will need additional time to compile the information appropriately.

*Question 6: Do health care providers currently face barriers or delays when attempting to obtain PHI from covered entities for treatment purposes? For example, do covered entities ever affirmatively refuse or otherwise fail to share PHI for treatment purposes, require the requesting provider to fill out paperwork not required by the HIPAA Rules to complete the disclosure (e.g., a form representing that the requester is a covered health care provider and is treating the individual about whom the request is made, etc.), or unreasonably delay sharing PHI for treatment purposes? Please provide examples of any common scenarios that may illustrate the problem.*

CTA's experience is that it is common for health care providers to impose obligations beyond HIPAA's scope that create obstacles and delays that limit covered entities' abilities to obtain PHI from other covered entities for treatment purposes. For example, CTA members have observed covered entities requiring unnecessary non-disclosure agreements when disclosing PHI for treatment purposes. Members have also observed healthcare providers' requests for payor claims data unnecessarily delayed for various reasons by payors. This is particularly problematic when the healthcare provider's business associate is the entity that makes the request. Usually, after the request from the business associate is denied, the payor will notify the provider and explain the information can only be shared with the business associate if they execute a non-disclosure agreement that is not required by HIPAA, notwithstanding the fact that the business associate is already subject to a BAA with the health care provider on whose behalf it is making the request. Such an additional non-disclosure agreement is unnecessary and significantly impedes care coordination. We note, however, that this may be an issue better addressed through HHS' rulemaking on information blocking, where HHS can specify that an entity may not condition disclosure of health information on completion of a contract or form when the recipient is already subject to HIPAA as a covered entity or pursuant to a BAA.

Question 7(c): *Should business associates be subject to the disclosure requirement? Why or why not?*

CTA requests that OCR consider revisions to HIPAA to clarify the disclosure obligations and liability for business associates. Business associates often do not have a direct relationship with the patient. The patient's healthcare provider has the direct relationship, familiarity and trust of the patient. Requiring business associates to be subject to additional disclosure requirements directly to the patient would place significant additional regulatory burdens on business associates to implement new procedures and processes for managing and sharing PHI with the patients.

Question 9: *Currently, HIPAA covered entities are permitted, but not required, to disclose PHI to a health care provider who is not covered by HIPAA (i.e., a health care provider that does not engage in electronic billing or other covered electronic transactions) for treatment and payment purposes of either the covered entity or the non-covered health care provider. Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in Questions 7 and 8? Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester? Do the risks associated with disclosing PHI to health care providers not subject to HIPAA's privacy and security protections outweigh the benefit of sharing PHI among all an individual's health care providers?*

CTA believes that it is critical to enable the sharing of information between covered entities and non-healthcare third parties, especially regarding issues concerning mental health and substance use disorders. Many non-healthcare third parties are integral in facilitating treatment and recovery for those suffering from mental health and substance use issues. As such, CTA urges OCR or another appropriate federal agency to provide additional guidance (in partnership with the private sector) regarding the appropriate privacy and security standards when a covered entity shares PHI with an entity that is not covered by HIPAA in the context of treatment for mental health and substance use disorders.

Question 12: *What timeliness requirement should be imposed on covered entities to disclose PHI that another covered entity requests for TPO purposes, or a non-covered health care provider requests for treatment or payment purposes? Should all covered entities be subject to the same timeliness requirement? For instance, should covered providers be required to disclose PHI to other covered providers within 30 days of receiving a request? Should covered providers and health plans be required to disclose PHI to each other within 30 days of receiving a request? Is there a more appropriate timeframe in which covered entities should disclose PHI for TPO purposes? Should electronic records and records in other media forms (e.g., paper) be subject to the same timeliness requirement? Should the same timeliness requirements apply to disclosures to non-covered health*



*care providers when PHI is sought for the treatment or payment purposes of such health care providers?*

CTA recognizes the importance of providing third parties with timely access to their PHI but believes that the accuracy and completeness of the PHI is as important as the timeliness of the response. If a covered entity provides inaccurate or incomplete PHI, a patient's health may be put at risk. Timeframes should be determined by the covered entities and the business associates—so long as they are reasonable—as those entities are in the best position to determine the scope of the PHI request and the anticipated time that it takes to accurately and completely disclose the PHI.

Question 16: *What considerations should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent with rulemaking by the Office of the National Coordinator for Health Information Technology (ONC) to prohibit “information blocking,” as defined by the 21st Century Cures Act?*<sup>2</sup>

CTA believes that OCR should ensure that any changes to the HIPAA Privacy Rule related to the disclosure of PHI is consistent with any regulations regarding information blocking prohibitions promulgated by ONC. Related regulatory provisions from various federal agencies need to be aligned to ensure better compliance from stakeholders.

Question 17: *Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard? For instance, should population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development be excepted from the minimum necessary requirement? Would these exceptions promote care coordination and/or case management? If so, how? Are there additional exceptions to the minimum necessary standard that OCR should consider?*

CTA believes that OCR should clarify and revise the minimum necessary standard as it unnecessarily impedes effective care coordination. Exceptions to the minimum necessary rule should be implemented that allow for the creation of effective, automated treatment innovation based on machine learning and artificial intelligence. Machine learning and artificial intelligence applications have the potential to identify and apply new insights in health care, but necessarily require large volumes of data to do so. Innovations in this space can be impeded by concerns that a regulator may view that too much information is being analyzed by the algorithms, in potential violation of the minimum necessary standard. Yet, an algorithm analyzing a large data set does not create the same privacy risks as a human analyzing such a data set, as the algorithm will disregard and will not

---

<sup>2</sup> Sec 4004, Public Law 114-255, 130 Stat. 1033 (amending Subtitle C of title XXX of the Public Health Service Act by adding Sec. 3022(a)(3)).

retain any excess data that proves unnecessary. It is only the output, to the extent that the output includes protected health information, which raises any human-related privacy concerns. To alleviate concerns regarding the application of the minimum necessary standard to processing of large data sets, OCR should provide guidance that computer analysis of data, such as machine learning and artificial intelligence, is exempt from the minimum necessary requirements.

*Questions 19: Should OCR expressly permit disclosures of PHI to multi-disciplinary/multi-agency teams tasked with ensuring that individuals in need in a particular jurisdiction can access the full spectrum of available health and social services? Should the permission be limited in some way to prevent unintended adverse consequences for individuals? For example, should covered entities be prevented from disclosing PHI under this permission to a multi-agency team that includes a law enforcement official, given the potential to place individuals at legal risk? Should a permission apply to multi-disciplinary teams that include law enforcement officials only if such teams are established through a drug court program? Should such a multi-disciplinary team be required to enter into a business associate (or similar) agreement with the covered entity? What safeguards are essential to preserving individuals' privacy in this context?*

CTA supports OCR's efforts to improve the efficiency, accuracy, completeness, and timeliness of the exchange of PHI to address issues raised by mental health and substance use disorders. CTA believes that unnecessary regulatory burdens should not impede disclosing PHI to allow patients in substance abuse programs to be better managed and simultaneously allow the health providers to better manage patient's information.

*Questions 23: How can OCR amend the HIPAA Rules to address serious mental illness? For example, are there changes that would facilitate treatment and care coordination for individuals with SMI, or ensure that family members and other caregivers can be involved in an individual's care? What are the perceived barriers to facilitating this treatment and care coordination? Would encouraging more sharing in the context of SMI create concerns similar to any concerns raised in relation to the previous question on the opioid epidemic? If so, how could such concerns be mitigated?*

CTA agrees that there is a need for improvement regarding the collection, use, and disclosure of PHI concerning mental illnesses and addiction. CTA strongly urges OCR to work with the private sector to develop procedures and policies to facilitate better treatment and care coordination. For example, a procedure could be undertaken for individuals suffering from mental illness in which psychiatric advance directives are prepared ensuring family members and caregivers are involved with the individual's care, and certain individuals are authorized to make certain decisions on the patient's behalf.

Question 25: *Could changes to the Privacy Rule help ensure that parents are able to obtain the treatment information of their minor children, especially where the child has substance use disorder (including opioid use disorder) or mental health issues, or are existing permissions adequate? If the Privacy Rule is modified, what limitations on parental access should apply to respect any privacy interests of the minor child?*

CTA supports OCR evaluating whether an exception to the HIPAA Privacy Rule should be permitted to allow a patient's family members to access and share the patient's PHI during a mental health or addiction-related episode.

Question 27: *How many requests for an accounting of disclosures do covered entities receive annually and from what percentage of total patients? Of these, how many requests specify a particular preferred electronic form or format, and to what extent do covered entities provide the accounting in the requested form or format?*

CTA encourages OCR not to modify the HIPAA Rules to require all disclosures related to treatment, payment, and healthcare operations (TPO) be logged and disclosed to an individual at their request. This requirement is unnecessarily burdensome and extremely challenging to track and report. Moreover, the accounting of disclosure offers limited value to patients and lacks meaningful information. The HITECH Act indicates that HHS should consider the interests of individuals in learning of TPO disclosures and the administrative burden of accounting for such disclosures. CTA's understanding is that individuals have demonstrated minimal interest in receiving an accounting of disclosures, while the administrative burden of expanding accounting requirements would be substantial. Considering how much the burden would outweigh any benefit, CTA believes OCR can comply with the statute by making a formal determination that the burden of expanding the accounting of disclosures to encompass TPO disclosures would unreasonably outweigh any benefit to individuals, in light of evidence that individuals have limited interest in such an accounting.

Question 54: *In addition to the specific topics identified above, OCR welcomes additional recommendations for how the Department could amend the HIPAA Rules to further reduce burden and promote coordinated care.*

*(a) What provisions of the HIPAA Rules may present obstacles to, or place unnecessary burdens on, the ability of covered entities and/business associates to conduct care coordination and/or case management? What provisions of the HIPAA Rules may inhibit the transformation of the health care system to a value-based health care system?*

*(b) What modifications to the HIPAA Rules would facilitate efficient care coordination and/or case management, and/or promote the transformation to value-based health care?*

*(c) OCR also broadly requests information and perspectives from regulated entities and the public about covered entities' and business associates' technical capabilities, individuals' interests, and ways to achieve these goals.*

CTA urges OCR to consider updating current guidelines on de-identification which create regulatory burdens and obstacles to the development of machine learning, artificial intelligence and innovative data applications. The de-identification guidelines from 2012 require the removal of 18 identifiers. The guidelines, however, need to be updated to align with modern healthcare technology to ensure that the de-identification standard continues to support “secondary use of data” to provide advanced research and improve value-based healthcare.

Additionally, CTA seeks more clarity from OCR regarding when a business associate may use a covered entity’s de-identified data set for the business associate’s own purposes. The de-identified data set would not be attributable to anyone and would not impede privacy standards. The de-identified data could be used in creating significant health technology innovation.

On a related point, to further improve value-based healthcare, business associates should be permitted to utilize PHI to create de-identified data for research. If broader access is given to PHI for research and business associates are provided with the ability to use PHI to create de-identified data sets (without regard to whether the BAA expressly permits such a use), then critical research could be performed which could lead to various healthcare advancements. CTA encourages OCR to revise the Privacy Rule to explicitly permit business associates to use PHI to create de-identified data.

CTA also believes that it would be helpful for OCR to provide clarity regarding when machine learning-based de-identification algorithms can be used under the “expert determination” method of de-identification. For example, instead of an expert providing a determination that the risk is very small that an individual can be identified in a single data set, CTA recommends that OCR provide guidance that an expert can determine that the risk of identification is very small if a data set has gone through a particular de-identification algorithm. Such an algorithm can then be broadly used, without the need to obtain an expert determination with respect to each data set. By providing that a machine learning-based algorithm is an accepted method for rendering PHI de-identified, advancements in de-identifying large data sets can be achieved to advance healthcare research.

\* \* \* \* \*

CTA thanks OCR for the opportunity to comment and we welcome the opportunity to discuss these issues in more depth. If you have any questions, please do not hesitate to contact us.

Respectfully submitted,

Consumer Technology Association

Michael Petricone  
Senior Vice President, Government and Regulatory Affairs

René Quashie  
Vice President, Policy and Regulatory Affairs, Digital Health

Kinsey Fabrizio  
Senior Director, Member Engagement, Health and Fitness Technology

1919 South Eads St.  
Arlington, VA 22202