

DIGITAL HEALTH REPORT

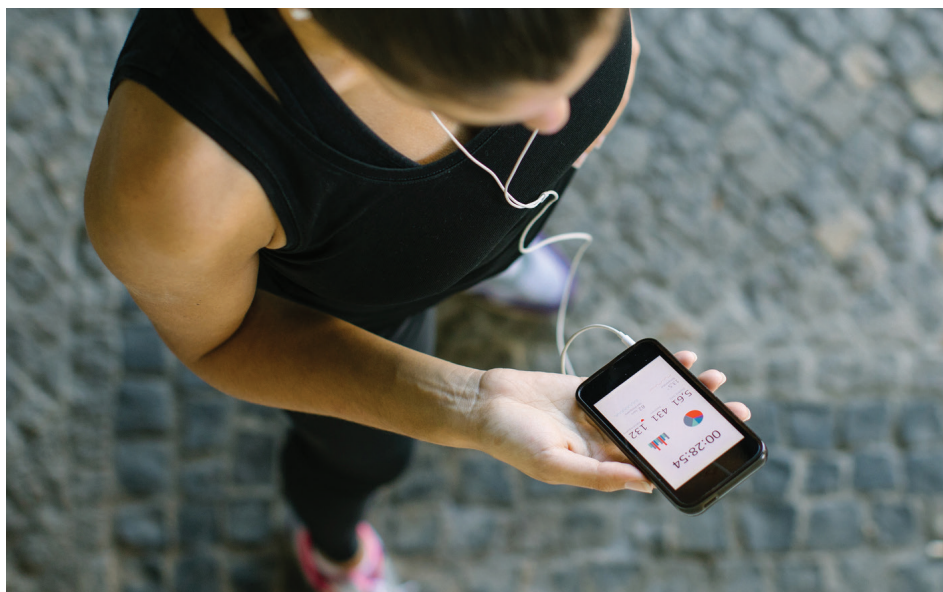
WINTER 2019

W&G Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

The Software Stands Alone: Understanding Software as a Medical Device (SaMD)

By Haley Bavasi and Jacqueline Kwok

Digital health entrepreneurs often come forward with a seemingly straightforward question: “*Is what I’m doing regulated by the FDA?*” Whether developing a medical app to track biometric data through a smartphone, leveraging accelerometers in wearables to evaluate joint health, or training complex algorithms to help health care providers make better treatment decisions, the possibilities—and questions—are vast. While every situation is different, this article briefly outlines a framework for thinking about your product or service and its intersection with the United States Food and Drug Administration (FDA) regulations. In it, we present a brief introduction to the FDA’s regulation of devices generally in order to set the stage for a deeper dive into a particular kind of regulated device—Software as a Medical Device, or SaMD. In particular, we will discuss what is and,



based on new FDA guidance, what is *not* regulated as SaMD.

Introduction to FDA-Regulated Devices

To identify the boundaries of SaMD, it is helpful to have a working understanding of how the FDA regulates medical devices overall. In general, a medical “device” is an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is i) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, ii)

or intended to effect the structure or any function of the body. What makes a device unique from a drug, for example, is that a device does not achieve its purpose through a chemical action in the body.¹ Examples of devices range from a simple tongue depressor to cutting-edge laser surgical devices. The definition of device also encompasses certain software. To avoid confusion, there are two types of software the FDA classifies as a device which are *not* the topic of this article: software that is integral to a medical device (e.g., it drives or controls a hardware device), and software that is used in the manufacture or maintenance of a medical device. We are focused on a third category: Software as a Medical

IN THIS ISSUE

The Software Stands Alone: Understanding Software as a Medical Device (SaMD) Pages 1-3

Two Prongs Making Digital Health Patents Right? Pages 3-6

HIPAA for Digital Health Entrepreneurs: Second Installment Pages 7-8

¹ 21 U.S. Code § 321(h).

The Software Stands Alone . . . (continued from page 1)

Device (SaMD), which is defined by the FDA through incorporation of the International Medical Device Regulator's Forum's (IMDRF) definition as software **intended to be used for one or more medical purposes, that perform the purposes independently of a hardware medical device.** SaMD is unique in that it achieves its purpose without being tethered to a particular device, i.e., it operates "independently" of a hardware device. In fact, SaMD is deployed on a diverse array of platforms (e.g., personal computers, smart phones, network servers) easily accessed and distributed (e.g., through the internet or cloud) on general-purpose (non-medical) hardware (e.g., a smartphone or wearable device). Second, the software must have a "medical purpose," as opposed to the abundance of software used in healthcare (administrative, financial software), that is not itself medical in nature. "Medical purpose" aligns with the definition of a "device" above, including in vitro diagnostics. The evolving nature of defining what SaMD *is* appears limited only by the creativity of those developing it. Because of this ever-changing landscape, it is particularly important to highlight recent FDA guidance that defines software functions which are actually *excluded* from the definition of a device. As discussed below, this delineation is part of an effort to streamline the development of software products that balance a low risk of harm with high degree of potential benefit.

FDA Report on Excluded (Non-Regulated) Software Functions

The recent changes to the definition of "device" originate in the 21st Century Cures Act (the Cures Act),² which focused, among other things, on ways to bring

medical products to market more quickly. One way in which it sought to do this was to amend the definition of "device" under the Food, Drug and Cosmetic Act (the FD&C Act) to exclude certain software functions, and direct the FDA to issue a follow-up report and guidance. Since the Cures Act, the FDA has published two draft guidances³ (collectively, the FDA Guidance) and a more recent report⁴ (the FDA Report) discussing in more detail the software functions excluded from the definition of a "device" and therefore from more stringent FDA regulatory review, as well as impacts to patient health and best practices.

Summary of FDA Guidance Related to Non-Device Software Functions

Section 3060(a) of the Cures Act amends Section 520(o)(1) of the FD&C Act to exclude the following software functions from the definition of a device:

1. Administrative support of a health care facility;
2. Maintaining or encouraging a healthy lifestyle and unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition;
3. Serving as electronic patient records when not intended to interpret or analyze patient records;
4. Transferring, storing, converting formats, or displaying data; or
5. Providing certain types of clinical decision support to a health care provider, unless interpreting or analyzing a clinical test or other device data.

As directed by the Cures Act, the FDA collected information on the above software functions to further analyze the following questions: a) How do these

functions impact patient safety?, b) What are the benefits and risks to health posed by these functions?, and c) What are best practices to promote safety, education, and competency? The FDA Report found for each of these software functions, the risk to patient safety is relatively low compared to the potential benefits to consumers, and identified steps to promote safe and informed use. Parameters for each of these excluded functions are outlined briefly below; however, we encourage developers to review the FDA Guidance for more examples and additional detail.⁵

1. Administrative support of a health care facility: The definition of device excludes a software function intended for administrative support of a health care facility, including: processing and maintenance of financial records, claims or billing information, scheduling appointments, business analytics, information about patient populations, admissions, practice and inventory management, analysis of historical claims data to predict future utilization or cost-effectiveness, determination of health benefit eligibility, population health management, and laboratory workflow. Historically, these have already been considered these to be non-device functions, but the FDA's Guidance adds additional clarity for developers.

2. Maintaining or encouraging a healthy lifestyle: Software functions that promote a healthy lifestyle and are unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition are excluded from the definition of "device." The FDA has previously provided guidance on what it means to promote a "healthy lifestyle,"⁶ categorizing these "general wellness" products into two categories of

² 21st Century Cures Act. H.R. 34, 114th Congress. 2016. <https://www.gpo.gov/fdsys/pkg/BILLS-114hr34enr/pdf/BILLS-114hr34enr.pdf>.

³ Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act Guidance: <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM587820.pdf>; Clinical and Patient Decision Support Software Guidance: <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM587819.pdf>.

⁴ Report on Non-Device Software Functions: Impact to Health and Best Practices—December 2018: <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM628128.pdf>.

⁵ General Wellness: Policy for Low Risk Devices: <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm429674.pdf>.

⁶ Clinical and Patient Decision Support Software – December 2017: <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm587819.pdf>.

intended use: a) an intended use related to maintaining or encouraging a general state of health or a healthy activity, or b) an intended use that relates to the role of a healthy lifestyle by helping to reduce the risk or impact of certain chronic diseases or conditions, where it is well understood and accepted that healthy lifestyle choices may play an important role in health outcomes for the disease or conditions. If your software function relates to b), it is *not* to be excluded from the definition of “device,” because the function relates to the mitigation or prevention of a disease or condition. *However*, the FDA Guidance makes clear that the FDA will continue not to enforce applicable requirements for this type of general wellness software where it presents a low risk to the safety of users. Making this concept more concrete, the FDA Guidance outlines a number of examples of what it considers healthy lifestyle claims (i.e., not related to the diagnosis, cure, mitigation, prevention or treatment of a disease or condition), including weight management, physical fitness, relaxation or stress management, mental acuity, self-esteem, sleep management, or sexual function. Furthermore, it will amend the Mobile Medical App guidance such that apps that had been classified as “mobile apps for which FDA intends to exercise enforcement discretion” will not be “examples of mobile apps that are NOT medical devices”—offering much clearer-cut guidance for developers.

3. Electronic patient records: Software functions that are intended to serve as electronic patient records are not devices. More specifically, a software function that transfers, stores, converts formatting, or displays electronic patient records are not devices if the records a) are created, stored, transferred, or reviewed by health care professionals (or individuals working under them), b) the records are certified by the Office of the National Coordinator for Health Information Technology (ONC),

and c) the software is not intended to interpret or analyze patient records, including imaging data, for the purpose of diagnosis, cure, mitigation, prevention, or treatment of a disease or condition.

4. Transferring, storing, converting, or displaying data: Software that is used to transfer, store, convert the format of, or display clinical laboratory test or other device data and results is not considered a device, *unless* such function is intended to interpret or analyze clinical laboratory test or other device data, results, and findings. Note that software functions that analyze or interpret medical device data *in addition to* transferring, storing, converting formats, or displaying clinical lab test or other device data remains subject to FDA oversight.

5. Providing certain clinical decision support⁷: Finally, software may also be excluded from SaMD if it satisfies all four of the following elements: 1) it is not intended to acquire, process, or analyze a medical image/signal from an in vitro diagnostic device or a pattern/signal from a signal acquisition system; 2) it is intended to display, analyze, or print medical information about a patient or other (e.g., general) medical information; 3) it is intended to support or provide recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and 4) *it enables such health care professional to independently review the basis for such recommendation, so the health care professional does not primarily rely on the software recommendation* in making a clinical diagnosis or treatment decision. The fourth element is the most critical; the point is that while software that is not a medical device may *assist* a health care professional to reach a treatment recommendation, the software must enable the health care professional to *separately come up with such treatment recommendation*, without relying primarily

on the software itself. Software may provide such independent basis for review by clearly explaining: a) the purpose of the software function; b) the intended user (e.g., vascular surgeon); c) the information input in the software to generate such recommendation (e.g., patient age and gender); and d) the software’s rationale behind such recommendation. For example, software that helps health care professionals diagnose diabetes in patients by taking information (e.g., lab test results, patient parameters) input by the health care provider and making suggestions based on whether such input information matches established, readily available external guidelines may be excluded from SaMD. Conversely, software that manipulates or analyzes data from a patient’s CT scan and provides a 3D reconstruction with software-imposed markers to help the health care provider visualize where to place catheters in a surgery, would probably not be excluded from SaMD because the health care provider is not able to independently verify (i.e., apart from the software’s own algorithm) how the software generated this recommendation.

Going Forward

The relative complexity of medical device software coupled with increased connectedness, diversity of operating platforms, and rapid development cycles are just some of the unique features of SaMD versus traditional medical devices that present new challenges and call for evolving FDA (and international) guidance. As an entrepreneur in the digital health space, you can leverage the evolving clarity from the FDA to focus on products that clearly will not be regulated as a device, or dive in knowing that your software product will be regulated, and be educated about the FDA approval process.

⁷ Clinical and Patient Decision Support Software—December 2017: <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm587819.pdf>.

Two Prongs Making Digital Health Patents Right?

New USPTO Guidance for Analyzing Section 101 Patent-Eligible Subject Matter

By Peter S. Kang

February 2019

When determining whether to allow a patent application claiming inventions in the digital health space, the United States Patent and Trademark Office (USPTO) will review this application from various perspectives, including whether the claimed invention is directed to subject matter that is patent eligible under 35 U.S.C. § 101 (Section 101). While the issue of Section 101 patent eligibility is a threshold question that is considered across all technologies, the Section 101 question has particular relevance to digital health technology, which typically implicates software, data processing, and computers—implications that frequently give rise to Section 101 questions during patent prosecution and even patent litigation.

In January 2019, the USPTO issued a guidance (the January 2019 guidance), providing an updated framework for analyzing the question of patent eligibility under Section 101.¹ Effective immediately, the January 2019 guidance may have broad implications across all industries with U.S. patents and patent applications related to digital health, software, diagnostics, and life science technologies.

Background: Step 2A of the Section 101 Analysis

At a high level, the original Section 101 framework required, *inter alia*, determining whether a patent claim is “directed to” a judicial exception, i.e., Step 2A. Judicial exceptions included abstract ideas, laws of nature, or natural phenomena. If the claims were directed to a judicial exception under the original Step 2A test,

the claims were preliminarily determined to not be patent-eligible unless an “inventive concept” could be found in Step 2B.

As part of the original Step 2A test, USPTO examiners (examiners) were instructed to analyze the patent claim as a whole and compare their finding with court decisions determining whether the patent claim was or was not directed to a judicial exception. As a guide, the examiners relied on the USPTO’s “Eligibility Quick Reference Sheets” (USPTO reference sheets). Last updated in July 2018, the USPTO reference sheets listed more than 100 examples of subject matter directed to a judicial exception (abstract ideas) and just eight examples of subject matter not directed to an abstract idea. The USPTO reference sheets and its examples of abstract ideas and non-judicial exceptions continued to grow and evolve as more and more court decisions interpreting Section 101 came forth.

The New Framework: Prong-One and Prong-Two Under Step 2A

Realizing that relying on an ever growing USPTO reference sheets was impractical and that the current Step 2A framework could yield inconsistent conclusions among the examiners as to whether a claim was directed to a judicial exception, the January 2019 guidance offers a new Prong-One and Prong-Two approach for Step 2A.

Step 2A—Prong One

Under Prong One, the examiners are instructed to determine whether the claim recites a judicial exception. This prong is largely similar to procedures in prior guidance except in the case of determining if a claim recites an abstract

idea. Now, the examiners are expressly instructed to disregard the USPTO reference sheets and stop analogizing the claims to the 100+ previous examples of abstract ideas. Instead, the examiners are to determine whether the claim limitations recite the following three “abstract idea” subject matter groupings: 1) mathematical concepts; 2) certain methods of organizing human activity; and 3) mental processes.² If the claims do not recite any of these groups, then the claims should not be treated as reciting an abstract idea except in rare circumstances and be found to be patent eligible.³

Step 2A—Prong Two

If a claim is found to recite a judicial exception under Step 2A—Prong One, then the examiners are instructed to proceed to Step 2A—Prong Two. Under Prong Two, the examiners are to analyze whether the recited judicial exception “is integrated into a practical application of that exception.” If integration into a practical application of that exception exists, the examiners are instructed to find that the claims are not directed to a judicial exception and that the claims are patent eligible. Specifically, the examiners evaluate “integration into a practical application by 1) identifying whether there are any additional elements recited in the claim beyond the judicial exception(s); and 2) evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application. A non-exhaustive list of exemplary additional elements integrating an exception into a practical application includes:

- An additional element reflecting an improvement in the functioning of a computer, or an improvement to other

¹ See 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50 (Jan. 7, 2019).

² “Mathematical concepts” is defined as “mathematical relationships, mathematical formulas or equations, mathematical calculations.” See Fed. Reg. Vol. 84, No. 4 at 52 (Jan. 7, 2019). “Certain methods of organizing human activity” is defined as “fundamental economic principles or practices (including hedging, insurance, mitigating risk); commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or sales activities or behaviors; business relations); managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions.” See *id.* “Mental processes” is defined as “concepts performed in the human mind (including an observation, evaluation, judgment, opinion).” See *id.*

³ Only in rare circumstances should a claim that does not recite one of the three subject matter groups qualify as a “tentative abstract idea.” In such cases, the examiner should go through the rest of the other Section 101 analysis steps. If still found to be a tentative abstract idea, the application is to be brought to the Technology Center Director and the Section 101 rejection must be approved by the Technology Center Director.

technology or technical field;⁴

- An additional element applying or using a judicial exception to effect a particular treatment or prophylaxis for a disease or medical condition;⁵
- An additional element implementing a judicial exception with, or using a judicial exception in conjunction with a particular machine or manufacture that is integral to the claim;⁶ or
- An additional element effecting a transformation or reduction of a particular article to a different state or thing.⁷

Step 2B: Largely Unchanged Since *Berkheimer*

The January 2019 guidance kept the Step 2B framework largely unchanged since the USPTO April 2018 *Berkheimer* Memo and accompanying training materials.⁸ Per the January 2019 guidance, a patent claim can still be found patent eligible even if the claim fails Prongs One and Two of Step 2A if the claim recites “additional elements [that] provide[] ‘significantly more’ than the recited exception (e.g., because the additional elements were unconventional in combination).”⁹ The examiners are instructed to evaluate “the additional elements individually and in combination under Step 2B to determine whether they provide an inventive concept.”¹⁰

An Example of the January 2019 Guidance Applied to Digital Health Subject Matter

In addition to the January 2019 guidance, the USPTO has also published several examples of how hypothetical claims may be analyzed under the new Section

101 framework.¹¹ Notably, Example 42 describes a “Method for Transmission of Notifications When Medical Records Are Updated.”¹² In a hypothetical Background section, Example 42 states how “[p]atients with chronic or undiagnosed illnesses often must visit several different medical providers for diagnosis and

Hypothetical Claim 1	Hypothetical Claim 2
<p>A method comprising:</p> <ol style="list-style-type: none"> storing information in a standardized format about a patient’s condition in a plurality of network-based non-transitory storage devices having a collection of medical records stored thereon; providing remote access to users over a network so any one of the users can update the information about the patient’s condition in the collection of medical records in real time through a graphical user interface, wherein the one of the users provides the updated information in a non-standardized format dependent on the hardware and software platform used by the one of the users; converting, by a content server, the non-standardized updated information into the standardized format, storing the standardized updated information about the patient’s condition in the collection of medical records in the standardized format; automatically generating a message containing the updated information about the patient’s condition by the content server whenever updated information has been stored; and transmitting the message to all of the users over the computer network in real time, so that each user has immediate access to up-to-date patient information. 	<p>A method comprising:</p> <ol style="list-style-type: none"> storing information about a patient’s condition in a plurality of network-based non-transitory storage devices having a collection of medical records stored thereon; providing access, by a content server, to users so that any one of the users can update the information about the patient’s condition in the collection of medical records; and storing the updated information about the patient’s condition in the collection of medical records in the plurality of network-based non-transitory storage devices.

⁴ For example, a modification of internet hyperlink protocol to dynamically produce a dual source hybrid web page. See MPEP 2106.05(a) for more information concerning improvements in the functioning of a computer or to any other technology or technical field, including a discussion of the exemplar provided herein, which is based on *DDR Holdings*, 773 F.3d at 1258–59. See also USPTO *Finjan* Memorandum (discussing *Finjan* and *Core Wireless*).

⁵ For example, an immunization step that integrates an abstract idea into a specific process of immunizing that lowers the risk that immunized patients will later develop chronic immune mediated diseases. See, e.g., *Classen Immunotherapies, Inc. v. Biogen IDEC*, 659 F.3d 1057, 1066–68 (Fed. Cir. 2011). See also *Vanda Pharm. Inc. v. West-Ward Pharm. Int’l Ltd.*, 887 F.3d 1117, 1135 (Fed. Cir. 2018) (holding claims to the practical application of the natural relationships between iloperidone, CY-P2D6 metabolism, and QTc prolongation to treat schizophrenia, not merely the recognition of those relationships, to be patent eligible at *Mayo/Alice* step 1 (USPTO Step 2A)), and USPTO *Vanda* Memorandum (discussing *Vanda*).

⁶ For example, a Fourdrinier machine (which is understood in the art to have a specific structure comprising a headbox, a paper-making wire, and a series of rolls) that is arranged in a particular way that uses gravity to optimize the speed of the machine while maintaining quality of the formed paper web. See MPEP 2106.05(b) for more information concerning use of a judicial exception with, or in conjunction with, a particular machine or manufacture, including a discussion of the exemplar provided herein, which is based on *Eibel Process Co. v. Minnesota & Ontario Paper Co.*, 261 U.S. 45, 64–65 (1923).

⁷ For example, a process that transforms raw, uncured synthetic rubber into precision-molded synthetic rubber products by using a mathematical formula to control operation of the mold. See MPEP 2106.05(c) for more information concerning transformation or reduction of a particular article to a different state or thing, including a discussion of the exemplar provided herein, which is based on *Diehr*, 450 U.S. at 184.

⁸ Robert W. Bahr, Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (*Berkheimer v. HP, Inc.*) (Apr. 19, 2018), available at <https://www.uspto.gov/sites/default/files/documents/memo-berkheimer-20180419.PDF>; see also Training: Well-Understood, Routine, Conventional Activity (posted May 7, 2018), available at <https://www.uspto.gov/sites/default/files/documents/berkheimer-training-20180427.pptx>.

For a fuller explication of the USPTO April 2018 *Berkheimer* Memo, please refer to: Peter S. Kang, Get Your Facts Right: *Berkheimer*’s Impact on the Second *Alice*/ *Mayo* Step of the Patent Eligibility Analysis, WILSON SONSINI GOODRICH & ROSATI DIGITAL HEALTH REPORT, Fall 2018, available at <https://www.wsgr.com/publications/PDFSearch/digital-health-report/Fall18/digital-health-report.htm>.

⁹ 84 Fed. Reg. at 56.

¹⁰ *Id.*

¹¹ Subject Matter Eligibility Examples: Abstract Ideas, available at https://www.uspto.gov/sites/default/files/documents/101_examples_37to42_20190107.pdf.

¹² *Id.* at 17.

Two Prongs Making Digital Health Patents Right? *(continued from page 5)*

treatment” and the difficulty “for medical providers to share updated information about a patient’s condition with other health care providers using current patient management systems” due to challenges associated with records being “stored locally on a computer in a non-standard format selected by whichever hardware or software platform is in use in the medical provider’s local office.”¹³ The hypothetical solution is offered in the form of a “network-based patient management method that collects, converts, and consolidates patient information from various physicians and health-care providers into a standardized format, stores it in network-based storage devices, and generates messages notifying health care providers or patients whenever that information is updated.”¹⁴

Specifically, Example 42 illustrates the hypothetical claimed subject matter in two claim forms:¹⁵

Finally, Example 42 analyzes how each hypothetical claim would be analyzed under the new Section 101 framework and concludes that 1) Hypothetical Claim 1 would be found patent eligible for satisfying Step 2A—Prong Two (integration into a practical application); but 2) Hypothetical Claim 2 would be found patent ineligible.¹⁶

Conclusion

In sum, the January 2019 guidance offers simpler and narrower categories for what should qualify as an abstract idea, which should have a positive impact

on the patent eligibility of digital health software-related patent applications as they are prosecuted at the USPTO. The January 2019 guidance further offers a clearer structure on how to evaluate the “integration into a practical application” prong, which should offer more consistency of the patent eligibility analysis across examiners in all industries implicated by Section 101 issues, including digital health, software, diagnostics, and life sciences. The accompanying USPTO examples of hypothetical claims should also serve as a helpful tool for digital health companies to consider as they evaluate the merits of seeking patent protection around their intellectual property.

Hypothetical Claim 1 Analysis	Jan. 2019 Section 101 Framework Steps	Hypothetical Claim 2 Analysis
Yes. The claim recites a series of steps and, therefore, is a process.	Step 1: Statutory Category	Yes. The claim recites a series of steps and, therefore, is a process.
Yes. The claim as a whole recites a method of organizing human activity. The claimed invention is a method that allows for users to access patients’ medical records and receive updated patient information in real time from other users which is a method of managing interactions between people. Thus, the claim recites an abstract idea.	Step 2A—Prong 1: Judicial Exception Recited?	Yes. The claim as a whole recites a method of organizing human interactions. The claimed invention is a method that allows for users to access and update patients’ medical records and store the updated information which is a method of managing interactions between people. The mere nominal recitation of a generic content server and generic network-based storage devices does not take the claim out of the methods of organizing human interactions grouping. Thus, the claim recites an abstract idea.
Yes. The claim recites a combination of additional elements including storing information, providing remote access over a network, converting updated information that was input by a user in a non-standardized form to a standardized format, automatically generating a message whenever updated information is stored, and transmitting the message to all of the users. The claim as a whole integrates the method of organizing human activity into a practical application. Specifically, the additional elements recite a specific improvement over prior art systems by allowing remote users to share information in real time in a standardized format regardless of the format in which the information was input by the user. Thus, the claim is eligible because it is not directed to the recited judicial exception (abstract idea).	Step 2A—Prong 2: Integrated into a Practical Application?	No. The claim as a whole merely describes how to generally “apply” the concept of storing and updating patient information in a computer environment. The claimed computer components are recited at a high level of generality and are merely invoked as tools to perform an existing medical records update process. Simply implementing the abstract idea on a generic computer is not a practical application of the abstract idea.
NA	Step 2B: Inventive Concept?	No. As noted previously, the claim as a whole merely describes how to generally “apply” the concept of updating medical records in a computer environment. Thus, even when viewed as a whole, nothing in the claim adds significantly more (i.e., an inventive concept) to the abstract idea. The claim is ineligible .

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.* at 18, 19.

¹⁶ *Id.* at 18-20.

HIPAA for Digital Health Entrepreneurs: Second Installment

By Haley Bavasi

Welcome to the second installment of our series on Health Insurance Portability and Accountability Act of 1996 (HIPAA) for digital health entrepreneurs. If you missed the first, then a brief re-introduction is in order: This series is specifically tailored to HIPAA topics that impact our digital health clients, particularly for those wading into health privacy for the first time. The first installment laid some basic groundwork outlining the law; in this article, we will dig deeper into a particular topic—business associates.

If you have begun to explore HIPAA on your own, you may have noticed that much (although certainly not all) of what is freely available on the internet is geared toward advising “covered entities.” As discussed briefly in the last article, covered entities are defined by HIPAA as **health care providers** (who transmit any health information in electronic form in connection with certain health care transactions), **health plans**, and **health care clearinghouses**.¹ It makes sense that the spotlight tends to focus on covered entities, because HIPAA applies to nearly every organization that directly provides, insures, or bills for health care in an industry worth trillions. The cost of compliance (and non-compliance) for these entities isn’t trivial.

Our digital health entrepreneurs, however, generally do *not* fit the definition of a covered entity, but instead are focused on services to customers in the health care economy. Given this, the most common question we get is whether a particular digital health product or service implicates HIPAA. In other words, “Am I a business associate?” Here are three scenarios which often prompt this question:

- 1) **“New Territory”**: You are developing a new product or service, adding a feature, or moving into the health care vertical for the first time, and want advice about whether your plans will require you to comply with HIPAA.
- 2) **“BAA Pusher”**: You have launched a product or service and have been successfully marketing it to customers; you are pretty sure you are not regulated by HIPAA, but all of a sudden a potential

customer is pushing you to sign a business associate agreement (**BAA**). You want to know whether you can take the position that you are not providing business associate services, and thus avoid the BAA, without losing the deal.

3) **“You’re not a business associate even if you want to be”**: Maybe you are comfortable with signing a BAA, and have had your HIPAA house in order for some time. You want to enter into a partnership or collaboration with a covered entity, e.g., a hospital or clinic to beta test your platform and solicit feedback from providers. The problem is that you *aren’t actually offering any “services” to the covered entity*. Even where you may wish to receive, and the covered entity may be willing to give, access to protected health information (**PHI**), the key takeaway is that a business associate agreement is not a sufficient legal basis if no business associate services are being rendered. More discussion is on this point below.

Under any of these scenarios, the answer to “does this make me subject to HIPAA” can be a complex one; however, this article will give you an initial framework to think about the implications of your product or service in the context of HIPAA.

What Are Business Associate Services?

Here is the bottom line first: Not all services provided to a customer in the health care space will render you a business associate. If your product or service is **only marketed to individual users**, or your customer is **involved in health care, but is not a covered entity**, then, as a general rule, HIPAA is not implicated. That said, many of our clients launch their product as direct-to-consumer first (e.g., a wellness tracker in the App Store), but have plans to expand its functionality to connect both individual and provider customers in the future, which may involve HIPAA compliance. The key is to be future-oriented about your product arc and where it may eventually intersect with HIPAA, while knowing where you stand today. The rest of this section focuses solely on the scenario where you target your product or service to a *covered entity* customer, which gives rise to implications under HIPAA.

A **“business associate”** is any person (broadly defined to include a natural person or organization) who, on behalf of a covered entity:

- 1) **Creates, maintains, receives, or transmits PHI for a function or activity that is regulated by HIPAA, or**
- 2) Provides **legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services** to or for such covered entity, **and the provision of such service involves the disclosure of PHI.**²

Why does the law separate these into two separate baskets of services? Looking closely at the language, (2) expressly defines certain services that aren’t inherently business associate services, but *will* be if PHI is exchanged. On the other hand, (1) is a bit more nebulous—the service must relate to a “function or activity regulated by HIPAA.” While the regulations provide certain examples, the list is not exhaustive. Because of this, it may be relatively straightforward to determine whether your product or service falls within the ambit of a business associate, and other times it can be more complex.

We suggest, therefore, that instead of beginning by thinking about the nature of the services, start with the lower-hanging fruit working through this analysis:

- 1) Is my target customer a “covered entity”?
- 2) If yes, will I create, maintain, receive, or transmit PHI, or will my product or services otherwise involve the disclosure of PHI?
- 3) If still yes, then does the service itself fit within the definition of a business associate?

If you make it past the first two questions answering “yes” and on the third answer “no,” you should pause, as this may indicate an issue. Your covered entity customer must have a legal basis for sharing PHI with you. If there is no business associate service being rendered, then another legal basis must exist. Generally

¹ See definition of “covered entity” at 45 C.F.R. 160.103.

² See definition of “business associate” at 45 C.F.R. 160.103.

HIPAA for Digital Health Entrepreneurs: Second Installment *(continued from page 7)*

speaking, for our clients, that alternative legal basis would be to obtain a HIPAA-compliant authorization from any individual for whom PHI will be disclosed. We often hear that obtaining a HIPAA authorization from individuals is not scalable, because it is individualized and must be coordinated with the covered entity. We tend to agree with this from a business operations perspective; however, if your model relies on you receiving PHI without providing a business associate service, then it might be a signal to rethink the model.

It is worth noting that it is the covered entity's responsibility to ensure there is an adequate legal basis to initially use or disclose PHI. Occasionally our clients ask for a retrospective review of whether a business associate agreement *should* have been entered into with their customers. Even where the answer is yes, the client is likely performing a business associate service, the risk for them is low because the covered entity should be the one to require the BAA be signed. However, as a matter of good business practice, we encourage clients to proactively determine whether they think their services would qualify them as a "business associate", and sign (or decline to sign) BAAs uniformly across customers.

Special Considerations for Cloud Service Providers

Given the proliferation of cloud computing solutions, the agency responsible for enforcing HIPAA—the Department of Health and Human Services, Office of Civil Rights (HHS-OCR)—has taken steps to clarify through guidance when and how cloud service providers (CSPs) are regulated under the law. You can view detailed information on the types of services providers HHS-OCR considers to be CSPs by viewing the National Institute of Standards and Technology guidance on the topic,³ but generally CSPs "offer online access to shared computing resources with varying levels of functionality depending on the users' requirements, ranging from mere data storage to complete software solutions (e.g., an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs."⁴ HHS-OCR is clear that when a covered entity or a business associate engages a CSP to create, receive, maintain or transmit electronic PHI (ePHI) on its behalf, *the CSP is itself a business associate*.

Quite often we are asked whether our client (or its subcontractor) would be considered a business associate if it is not able to access the ePHI because, e.g., the data is encrypted and they don't have the code.

HHS-OCR is clear and emphatic on this point—the CSP is still a business associate *even if it processes and stores only encrypted ePHI and lacks an encryption key for the data*. Lacking an encryption key does *not* exempt a CSP from HIPAA regulation. This point is often confused with the so-called "conduit exception" under HIPAA, whereby service providers who only incidentally handle PHI are not considered business associates. The examples of conduits given by HHS-OCR are the United States Postal Service and some other private couriers; it does not include CSPs whose role is tied to managing ePHI, regardless of whether the CSP itself has direct access.

If you are offering cloud services that relate to ePHI, either directly or through a third-party CSP (e.g., Amazon Web Services), be prepared to execute a BAA with your covered entity customer or with the third-party CSP provider as your subcontractor.

Next Steps

On the way are more real-world examples and analyses of how HIPAA is impacting the digital health industry. Of course, if this has provoked questions about HIPAA, privacy in general, or anything digital health related, please reach out to your WSGR attorney for more information.

³ SP 800-145, The NIST Definition of Cloud Computing, *available at*: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

⁴ HHS-OCR Guidance on HIPAA and Cloud Computing, *available at*: <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>.

The *Digital Health Report* is developed and reviewed by a team of attorneys from the firm's corporate, intellectual property, litigation, and regulatory departments, including the individuals listed below.

Ali Alemozafar
Partner
Patents and Innovations
415-947-2054
aalemozafar@wsgr.com

Haley Bavasi
Associate
Technology Transactions
617-598-7826
hbavasi@wsgr.com

Jake D. Gatof
Associate
Corporate
617-598-7812
jgatof@wsgr.com

Farah Gerdes
Partner
Technology Transactions
617-598-7821
fgerdes@wsgr.com

Charles T. Graves
Partner
IP Litigation
415-947-2109
tgraves@wsgr.com

David Hoffmeister
Partner
Corporate
650-354-4246
dhoffmeister@wsgr.com

Michael Hostetler
Partner
Patents and Innovations
858-350-2306
mhostetler@wsgr.com

Peter Kang
Associate
Intellectual Property
858-350-2362
pkang@wsgr.com

Manja Sachet
Partner
Technology Transactions
206-883-2521
msachet@wsgr.com



Wilson Sonsini Goodrich & Rosati

PROFESSIONAL CORPORATION

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Austin Beijing Boston Brussels Hong Kong London Los Angeles New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC Wilmington, DE

© 2019 Wilson Sonsini Goodrich & Rosati, Professional Corporation. All rights reserved.