DIGITAL HEALTH REPORT
SUMMER 2019
WSGR Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

Avoid Potential Pitfalls When Incorporating Third-Party Software into Wearable Products

By Robert Parr

The global market for wearable devices continues to expand rapidly. Digital health companies that manufacture and sell their own wearable health products ("manufacturers") are contributing to this ever-growing industry. Commercializing these products raises a variety of important legal issues that every digital health company should be aware of, including issues regarding privacy, data security, United States Food and Drug Administration regulation, and product liability. We will unpack some of those issues in upcoming installments of this newsletter. Here, we start with the topic of incorporating third-party commercial software (i.e., software that is usually licensed for a fee) and open source

IN THIS ISSUE

software (i.e., software that generally can be used, modified, and shared for free) into wearable products. Below we provide tips on avoiding some of the common potential pitfalls associated with incorporating third-party software into wearable products.

Commercial Software. Commercial software licensors often grant licensees limited rights, impose restrictions on how the licensed software can be used (e.g., prohibit reproduction, modification, and distribution), and reserve all rights not expressly included in the license agreement. Manufacturers who plan to incorporate commercial software into their wearable products must ensure their commercial licenses clearly give them the rights to do so—these rights should include an express right to reproduce and distribute the licensed software to end-users as part of a larger product, and, if necessary, a right to modify the licensed code for integration purposes. Using commercial software in a manner that is not authorized by the licensor could lead to infringement claims and liability for monetary damages, so manufacturers should obtain all rights they need to use licensed software in clearly worded agreements.

Manufacturers also should avoid giving licensors unfavorable rights that are triggered when the manufacturer sells equity or assigns the license agreement

(Continued on page 2)

Avoid Potential Pitfalls . . . *(continued from page 1)*

as part of an asset sale, such as rights to terminate the license agreement or to pre-approve the equity or asset sale. If the licensed software would be material to the manufacturer's product and difficult to replace without significant expense or disruption, which could be the case with software embedded in wearable products in particular, then these kinds of terms can delay and, in extreme cases, even "kill," potential investment and acquisition deals. Manufacturers should also seek to include in license agreements for commercial software the right to sell-off inventory that includes the licensed software following license agreement termination to ensure they would not have to remove the licensed software from that inventory once the license agreement expires.

Given that wearables with a health-related application may collect sensitive end-user data, manufacturers should also seek (i) appropriate software maintenance and support commitments from commercial software licensors to ensure the licensed software remains secure and up-to-date, and (ii) robust remedies against commercial software licensors for third party claims arising from security breaches attributable to viruses or security vulnerabilities in the licensed software. This is a particularly important issue for manufacturers who sell health-related wearables because the U.S. Federal Trade Commission closely scrutinizes security breaches involving end-user data collected by these products.

Open Source Software. Unlike commercial software, most open source software does not come with warranties or support commitments. Manufacturers therefore should take steps to (i) confirm any code licensed under open source terms does not contain viruses or other contaminants, and (ii) update the code as necessary to ensure it remains secure to avoid potential security breaches arising from open source software components.

Other risks associated with using open source software have to do with the terms under which open source software is licensed. Some of the most popular open source licenses in circulation today are so-called "copyleft" licenses. These licenses generally allow licensees to use, reproduce, modify, and distribute the open source software, but all distributions of the original open source software and all modifications to that software must be provided in source code form and under the terms of the copyleft open source license. Under some widely-used copyleft licenses, proprietary software that is integrated with the open source software in certain ways and then "distributed" is deemed subject to the terms of the copyleft open source license and must be made available in source code form.

Software that is embedded in wearable product hardware or incorporated into companion software applications that end-users download and run locally is considered "distributed" under commonly used open source licenses, including standard "copyleft" licenses. Accordingly, manufacturers should be very careful not to integrate any of their proprietary code with open source software subject to copyleft terms in a manner that would require them to make that proprietary code available in source code form and under the copyleft license terms when that code is "distributed" as incorporated into product hardware or companion software applications. If proprietary code is used in a manner that requires that code to be open sourced, company competitors could access and exploit that proprietary code developed at the company's expense, which may decrease the company's enterprise value in the eyes of potential investors and acquirers.

Failures to comply with open source software requirements can lead to legal claims for copyright infringement, cause licensees to have to re-engineer their proprietary software, cause reputational harm, and may delay or defeat altogether potential investment or acquisition opportunities because this issue is often scrutinized very closely during the due diligence process. To avoid inadvertent copyleft issues and to help comply with open source obligations more generally, a digital health company that plans to or currently does use open source software in its wearable products (or in any other products or manner, for that matter) should implement a written open source policy that governs open source ingestion and use that is customized to the company's particular business model and needs. Among other things, this policy should require the company to maintain an inventory of all open source software components used in all product hardware and software, the license terms that govern those components and require the inventory to be updated regularly.

Conclusion

This article highlights some common challenges and potential pitfalls that may arise when using third-party software in wearable products. Manufacturers should keep in mind that use of third-party software can present other concerns that are beyond the scope of this article, so it is important to engage counsel to help ensure those risks are adequately evaluated and addressed.

An Overview of the FDA's Digital Health Software Precertification Program: What You Need to Know

By David Hoffmeister and Charles Andres

The U.S. Food and Drug Administration, or FDA, regulates, as a medical device, software that is intended or labeled for healthcare purposes. The FDA divides the regulation of software into the following three categories:

1) Software which meets the definition of a medical device under the Food, Drug, and Cosmetic Act. Such software is referred to as *software as a medical device* (SaMD);

2) Software that is integral to a medical device, also known as *software in a medical device* (SiMD); and

3) S*oftware used in the manufacture of a medical device*.

This article focuses on the FDA's Digital Health Software Precertification program, or Pre-Cert program, and its evolving, forward-looking regulation of SaMD; and on an ongoing Pre-Cert Pilot program that is an important step along the path to implementing the Pre-Cert program.

The FDA defines SaMD as "software intended to be used for one or more medical purposes without being part of a hardware medical device." Examples of SaMD include:

1) Software that allows a smartphone to view images obtained from a magnetic resonance imaging (MRI) medical device for diagnostic purposes; and

2) Computer-Aided Detection (CAD) software that is applied to a medical image, like an x-ray, to help detect breast cancer.

For comparison, some examples of software that would not qualify as SaMD include:

1) Software intended to be used as a component in hardware to perform the hardware's medical use, even if sold separately from the hardware;

2) Software that relies on data from a medical device, but does not have a medical purpose, e.g., software that encrypts data for transmission from a medical device; and

3) Software that enables clinical communication and workflow including patient registration, scheduling visits, voice calling, and video calling.

The DHIAP

In its Digital Health Innovation Action Plan, or DHIAP, the FDA outlined a potential new approach to assuring Americans have access to high-quality, safe and effective, digital health products. The FDA recognizes that digital health technologies, or DHTs, can provide new options for early disease diagnosis, management of chronic diseases, and that DHTs rely on software. Software can assist in diagnosis, determining treatment options, storing and sharing health records, and managing clinical practice workflow.

A key element of the DHIAP is the FDA's reimagining its approach to regulating digital medical devices by developing, as part of the reimagining, the Pre-Cert program. The FDA envisions the Pre-Cert program could "replace the need for a premarket submission of certain products and allow for decreased submission content and/or faster review of the marketing submission for other products." An early step in the FDA's implementing its vision is the roll-out of the Pre-Cert Pilot program.

The Software Pre-Cert Pilot Program for SaMD Products

The FDA intends its Pre-Cert Pilot program will help "inform the development of a future regulatory model" that will "provide more streamlined and efficient regulatory oversight of software-based medical devices . . ." Under the new Pre-Cert Pilot program, the FDA intends to first look at the software developer or digital health technology developer, rather than looking at the product.

In the Pre-Cert Pilot program, the FDA's Center for Devices and Radiological Health, or CDRH, *can pre-certify eligible digital health developers* who "demonstrate a culture of quality and organizational excellence" based on specifically enumerated objective criteria. Once pre-certified, the digital health developers could then "qualify to be able to market their lower risk devices without additional FDA review" and market their higher risk devices "with a more streamlined premarket review" that could "include reduced submission content, faster review of that content by CDRH staff, or both."

The FDA cautions that software products from precertified companies would be required to "continue to meet the same safety and effectiveness standard that the agency expects for products that have followed the traditional path to market."

(Continued on page 4)

An Overview of the FDA's Digital Health Software . . . *(continued from page 3)*

How the Pre-Cert Program Is Envisioned to Work

Per its 2019 Test Plan, the FDA's proposed components of a future Pre-Cert program are part of a Total Product Lifecycle Approach, or TPLA. The TPLA includes an *Excellence Appraisal* component, a *Review Determination* component, a *Streamlined Review* component (if required), and a *Real-World Performance* component.

Excellence Appraisal (Meeting Precertification Criteria and Getting Pre-Certified)

In the Excellence Appraisal component, a company must demonstrate a Culture of Quality & Organizational Excellence. Five principles must be met: patient safety, product quality, clinical responsibility, cybersecurity responsibility, and proactive culture. And the FDA is considering two levels of precertification based on: 1) how a company meets the Excellence Appraisal component principles, and 2) whether the company has demonstrated a track record in delivering safe and effective software components.

Review Determination (Determining the Level of Review Necessary)

The FDA notes that, potentially, pre-certified companies "could market lower-risk devices without a regulatory submission or only a streamlined premarket review based on the company's precertification level and the International Medical Device Regulators Forum, or IMDRF, risk categorization." IMDRF's risk categorization framework for software contains four risk categories (I-IV). Under the IMDRF framework, category I has the lowest impact on public or patient health, and category IV has the highest impact on public or patient health. Thus, and consistent with past precedent, the degree of regulation depends at least in part on the level of risk presented by the software.

The FDA plans to employ the IMDRF framework to help determine the risk categorization of the SaMD product, "incorporating information about the medical purpose of the SaMD and the seriousness of the medical condition that the SaMD is intended to address."

Streamlined Review (When Necessary)

The FDA states it is "exploring using an interactive streamlined review of a SaMD with information the agency has gained from the process to precertify a company. "The FDA also contemplates employing "additional information the company would share about the SaMD's product performance, clinical association between the SaMD and a clinical condition, and safety measures." As described above, for SaMD in a lower risk category, a regulatory submission and review by the agency may be unnecessary.

Real-World Performance (Collecting, Monitoring, and Adjusting)

The FDA is "considering how best to work with a company to collect and interpret real-world information about a SaMD and to evolve the product's safety and effectiveness to address any emerging risks."

Other

The FDA initially selected nine companies to participate in the Pre-Cert Pilot Program, and hired three Entrepreneurs-in-Residence fellows to help support the program. A presentation is available from the February 7, 2019, Digital Health Software Precertification Pilot User Session.

Conclusion

The Pre-Cert Pilot Program is an important early step in the FDA's proposed new and innovative approach to regulating SaMD. Also, the FDA is seeking test cases from software organizations planning to submit a *De Novo* Request or 510(k) submission for SaMD in 2019 or shortly thereafter to meet the goals of the Test Plan. Finally, SaMD companies should continue to monitor regulatory developments in this important area, and consider planning to become pre-certified when this option becomes more widely available.

HIPAA for Digital Health Entrepreneurs: Third Installment

By Haley Bavasi

Welcome to the third installment of our series exploring the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for digital health entrepreneurs. This series focuses on HIPAA topics that impact our digital health clients, particularly for those who may be newly encountering health privacy. The first installment presented some basic HIPAA background and framework, and the second took a deeper dive into business associates, which represent the majority of our clients who provide services to covered entities. While these first installments focused on answering the question, "am I subject to HIPAA?", this article aims to guide you if the answer is "yes."

If your company's activities are regulated by HIPAA, the next question invariably is what do you need to do to become "HIPAA compliant"? How long will that take? How difficult is it? Unfortunately, there is no easy, one-size-fits-all answer, and the Department of Health and Human Services (HHS)—the government agency responsible for enforcing HIPAA—does not offer a way to certify or guarantee than any particular entity is in complete compliance with the law. The good news, however, is that HIPAA is a flexible and scalable standard that does not advocate for a one-size-fits-all approach—in fact, quite the opposite. At the end of the day, once you have an overview of HIPAA's requirements, you will be prepared to evaluate how much work must be done to comply with these standards, which will depend on your organization's size, resources, and nature of your business.

This article will give a brief overview of both the Privacy and Security Rules, which contain certain **Administrative, Technical, and Physical Safeguards** with which covered entities and business associates must comply. These safeguards are separated into "**standards**" (broad requirements), and further parsed into "**implementation specifications**" (steps to implement a particular standard). Because our clients often are interested in the nitty-gritty of what is technically required under the law, we will *summarize* the implementation specifications of both rules, as well as provide some helpful guidance on taking the first steps toward making your organization HIPAA compliant, particularly as required under the Security Rule by performing a Security Risk Analysis.

The HIPAA Privacy Rule

The HIPAA Privacy Rule[1] establishes a set of national standards for the protection of "individually identifiable health information" or "PHI" held or transmitted by a covered entity or its business associate, in any form or media, whether in electronic, paper, or oral form (this is in contrast to the Security Rule, discussed next, which only applies to PHI that is transmitted in *electronic form*). The Privacy Rule primarily addresses 1) the use and disclosure of PHI by organizations subject to HIPAA, and 2) individuals' privacy rights to understand and control how their health information is being used.

PHI can only be used or disclosed (a) as permitted or required by the Privacy Rule,[2] or (b) as authorized by the individual (or the individual's representative). Because there are finite "permitted purposes" under the Privacy Rule, any other purposes

[1] 45 CFR Part 160 and Part 164, Subparts A and E.
[2] Future installments will discuss uses and disclosures of PHI in more detail; *see* 45 C.F.R. § 164.502.

Continued on page 6...

HIPAA for Digital Health Entrepreneurs: Third Installment *(continued from page 5)*

require affirmative, written authorization be obtained from the individual meeting certain specifications. In addition to this basic principle, the Privacy Rule commands that even where there is a permitted purpose, an entity must make reasonable efforts to use, disclose, or request only the "minimum necessary" PHI needed to accomplish the intended purpose.

In order to comply with these and other tenets of the Privacy Rule, an organization must implement certain "Administrative Requirements."[3] For business associates, these will essentially all overlap with the standards required under the Security Rule, e.g., you will need policies and procedures under both rules, but the substance required under each rule is different. In other words, the Privacy Rule requires policies about keeping information confidential, while the Security Rule requires policies about keeping information secure. Here is a summary of these Administrative Requirements:

- **Policies and Procedures** – Develop and implement written privacy policies and procedures consistent with Privacy Rule
- **Privacy Official** – Designate privacy official responsible for developing and implementing privacy policies and procedures
- **Training** – Train all workforce (including employees, volunteers, trainees, and others under direct control of entity) on privacy policies and procedures and apply appropriate sanctions for violations
- **Mitigation Plan** – Develop plan to mitigate any harmful effect caused by use or disclosure of PHI
- **Safeguards** – Maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent use or disclosure of PHI in violation of Privacy Rule (note the Security Rule prescribes certain of these safeguards for PHI in electronic form, discussed below)
- **Complaint Procedures** – Maintain procedures for individuals to complain about compliance with policies and the Privacy Rule, and procedure must be in privacy practices (for covered entities)
- **Non-retaliation** – Refrain from any retaliation against a person for exercising rights under Privacy Rule
- **Documentation** – Maintain all documentation, including privacy policies and procedures, privacy practices notices, disposition of complaints and other actions, activities that the Privacy Rule requires to be documented for six years

While these Administrative Requirements may be relatively specific, they are *not* prescriptive: HHS understands that entities under HIPAA jurisdiction range from sprawling hospital systems to the smallest service provider. Therefore, the Privacy Rule takes a flexible approach, allowing organizations to determine how best to implement these safeguards in a way that is appropriate in regards to size, resources, and nature of the business.

The Security Rule

As a digital health company, the transmission of PHI in electronic form (referred to as "e-PHI") puts you squarely in the crosshairs of regulation by the Security Rule.[4] The Security Rule operationalizes the safeguards contained in the Privacy Rule through certain "reasonable and appropriate" Administrative, Physical, and Technical Safeguards that specifically protect e-PHI (the Security Rule does not apply to PHI maintained in non-electronic forms). A matrix outlining the safeguards, standards, and implementations specifications has been easily formatted by the HHS and is accessible Appendix A to Subpart C of Part 164—Security Standards: Matrix.[5]

The biggest hurdle for any digital health company seeking to become HIPAA compliant will be to meet the implementation specifications required under the Security Rule. Like the Privacy Rule, the Security Rule takes a flexible approach, expressly stating that organizations may use *any security*

[3] 45 C.F.R. § 164.530.
[4] 45 CFR Part 160 and Part 164, Subparts A and C.
[5] Security Standards Matrix available at https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

measures that allow them to comply with the Security Rule, *as long as* the organization considers and documents the following four factors:

1. Its size, complexity, and capabilities,
2. Its technical, hardware, and software infrastructure,
3. The costs of security measures, and
4. The likelihood and possible impact of potential risks to e-PHI.

Further promoting flexibility, the Rule labels some implementation specifications as "required" and others as "addressable." "Addressable" does not mean "optional," but allows an organization to determine whether an implementation specification is reasonable and appropriate (based on the factors above), and if not, adopt an alternative that achieves the purpose of the standard.

So, if you are a very small startup with limited resources handling a limited amount of e-PHI that is not particularly sensitive, what is "reasonable and appropriate" in terms of implementing the standards below will look different than a large, sophisticated operation handling large amounts of highly sensitive e-PHI. You may breathe a sigh of relief knowing that your small startup would not be held to the same standard as, say, the Mayo Clinic. No matter how small the operation, however, it is critical to complete an initial **Security Risk Analysis** and begin addressing any identified gaps before holding your business out as "HIPAA compliant," including signing any business associate agreements (which essentially represents that you comply with the relevant privacy and security requirements under the law).

The Security Risk Analysis (SRA) is a process by which you identify which security measures are reasonable and appropriate for your organization. It in itself is one of the Administrative Safeguards, but is discussed separately because it impacts the implementation of all safeguards contained in the Security Rule. Happily, the HHS and the Office of the National Coordinator for Health Information Technology (ONC) co-developed a free, interactive SRA tool[6] that will guide you through the analysis and produce a report for your organization. So, while it's true the HHS doesn't rubber-stamp any organization as "compliant," using the HHS-developed tool and documenting how your organization addresses identified gaps is a great starting point toward HIPAA compliance that your organization can undertake on its own.

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.

[6] SRA Tool available at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

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

WSGR
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