Congress of the United States
U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and Technology
Washington, D.C.

Hearing on:

Health Information Technologies: Harnessing Wireless Innovation

March 19, 2013

Testimony of:

Benjamin M. Chodor
Chief Executive Officer
Happtique, Inc.
New York, New York

Testimony of Benjamin M. Chodor, Chief Executive Officer
Happtique, Inc.
Committee on Energy and Commerce Subcommittee on Communications and Technology
March 19, 2013

Summary

Happtique is a mobile health solutions company whose mission is to integrate mobile health into patient care and daily life. Happtique was founded in 2010 and is owned and operated by GNYHA Ventures, Inc., the business arm of the Greater New York Hospital Association (GNYHA). GNYHA represents nearly 250 hospitals and long term care facilities in New York, New Jersey, Connecticut, and Rhode Island, and provides a wide range of membership services to these health care organizations including health information technology.

Happtique believes that the FDA, among the many interested federal agencies, is in the best position to regulate health apps because of its deep expertise on issues of patient safety. Its risk based approach strikes an appropriate balance or guarding against consumer harm, while not chilling technological innovation, and because it is the most prepared to do so. Happtique urges the FDA to release its final guidance on mobile medical apps as soon as possible.

As a complement to the FDA regulatory framework, Happtique has created a certification program with industry stakeholders to offer clinicians and patients a way to identify technically and substantively valid apps. With the cooperation of recognized industry partners, the Happtique Health App Certification Program will provide a valuable tool for the review of health apps.

Happtique does not believe the medical device excise tax should apply to any phones, tablets or mobile health apps. Any application of the tax to these products would be beyond what Congress intended and would serve to slow innovation by placing burdensome costs on app developers in a new and growing market.

Good morning. Chairman Upton and Members of the Subcommittee, my name is Ben Chodor and I am the Chief Executive Officer of Happtique, Inc. It is a distinct honor for me to be here today, and I want to thank you for the opportunity to testify on the very important topic of mobile health technology and applications.

I'd like to begin by telling you about Happtique. Happtique is a mobile health solutions company whose mission is to integrate mobile health into patient care and daily life. Happtique was founded in 2010 and is owned and operated by GNYHA Ventures, Inc., the business arm of the Greater New York Hospital Association (GNYHA). GNYHA represents nearly 250 hospitals and long term care facilities in New York, New Jersey, Connecticut, and Rhode Island, and provides a wide range of membership services to these health care organizations including advocacy; education; emergency preparedness and response; and leadership on key initiatives in such critical areas as health care quality improvement, patient safety, population health management, workforce development and training, and health information technology. GNYHA's businesses, which are national in scope and operated under the umbrella of GNYHA Ventures, Inc., provide group purchasing, consulting, and other valuable products and services to health care organizations across the entire continuum of care with the goal of helping these organizations succeed in delivering high quality health care services in an efficient and cost-effective manner. Today, these businesses serve more than 25,000 customers across the U.S. and are responsible for more than $10 billion in commerce annually.

Happtique, which is the newest member of the GNYHA Ventures' family of companies, was established in direct response to GNYHA members' need for assistance in developing comprehensive mobile health strategies and utilizing mobile health technologies to support their clinicians, facilitate patient engagement, and improve their operations. Happtique's principal offerings include:

- Individually branded, secure, multi-platform application stores for hospitals, continuing care facilities, and physician practices for staff and patient use;
- mRx™, patent-pending technology that enables physicians to "prescribe" apps to their patients;

- a unique system developed by a nationally known medical librarian and a team of physicians and nurses for classifying apps into more than 300 clinically-meaningful categories. This classification system is designed to make the discovery of apps easier and more intuitive to clinicians and consumers; and
- a voluntary certification program for health apps.

I would be happy to discuss any of Happtique's offerings in detail, but in light of the focus of this hearing on the regulation of mobile health technology and applications, I would like to devote the balance of my testimony to a discussion of our certification program and issues related to the mobile health app market and regulation thereof.

Mobile health technology offers unprecedented potential to connect patients and providers—and is coming of age at the perfect time in the history of the American healthcare system. As Americans, we are all cognizant that the costs associated with healthcare management and prevention need to be prioritized. Happtique believes that, in order to move away from individual encounters in the healthcare system toward patient-centered care, greater focus should be placed on connectivity and care management across the continuum. However, before we can fully embrace the necessity for realignment of how healthcare ought to be delivered, we need to recognize that patient engagement is paramount. Fortunately, we have the technological capabilities today (e.g., smartphones, tablets, peripheral devices) that can serve as the ideal vehicles to connect patients and providers remotely and in real time.

Highlights of Market Statistics:

- 87% of adults own a cell phone (Mobile, Pew Internet, January 2013)
- 1 out of 3 cell phone owners has used their phone to look for health information online (Mobile Health 2012, Pew Internet, November 2012)
- 1 out of 5 smartphone owners has at least one health app (Mobile Health 2012, Pew Internet, November 2012)
- 87% of physicians use a smartphone or a tablet in their practice (Screen to Script: The Doctors Digital Path to Treatment, thinkwithgoogle.com, June 2012)

- 78% of consumers believe in the benefits of mHealth (mHealth US end-user research: Beliefs, barriers, success factors and recommendations, GSMA, 2012)
- $200 million in sales for healthcare apps (Frost & Sullivan, 2011)
- 600 million health apps were downloaded in 2012 (Pyramid)

More than 40,000 health apps exist on the market to assist healthcare professionals deliver and improve patient care, in addition to allowing consumers to become educated and manage their own health and wellness. What's driving this proliferation? Unlike other aspects of the healthcare marketplace, there is little to no barrier to entry into the health app market—so basically anyone with an idea and programming skills can build a mobile health app. While this has exposed the healthcare industry to an influx of technologically sophisticated and innovative developers who are eager to make positive transformations, it has simultaneously made the industry vulnerable to a new breed of inventors who are novice to its regulatory landscape. Thus, the easy entry into mHealth offers incredible opportunity for innovation in healthcare; however, the open market comes with certain concerns, namely, "how credible are the apps I am (or my patients are) using?"

Of course, this raises the issue of who should monitor the mobile health industry. The mHealth community is in need of both direction and a level of expectation to foster innovation while assuring safety and effectiveness. Happtique believes that the industry would benefit from a balanced, risk-based approach where regulation and oversight is borne by various appropriate groups and that is clearly conveyed to all stakeholders.

Recognizing the exponential growth and adoption of health apps by healthcare professionals and consumers, the FDA released Draft Guidance in July 2011. The Draft Guidance describes plans to provide oversight with respect to the safety and effectiveness for a subset of mobile apps – mobile medical applications ("mobile medical apps"). These consist of mobile apps that have either already been classified as medical devices themselves or "affect the performance or functionality of a currently regulated medical devices."

The FDA chose to define a "mobile medical app" in the Draft Guidance as:

> *A mobile app that meets the definition of "device" in section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), and either:*

- *is used as an accessory to a regulated medical device; or*
- *transforms a mobile platform into a regulated medical device.*

Examples of "mobile medical apps" that the FDA plans to provide regulatory oversight for include:

- Mobile apps that are an extension of one or more medical device(s) by connecting to such device(s) for purposes of controlling the device(s) or displaying, storing, analyzing, or transmitting patient-specific medical device data;
- Mobile apps that transform the mobile platform into a medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices; and
- Mobile apps that allow the user to input patient-specific information and – using formulae or processing algorithms – output a patient-specific result, diagnosis, or treatment recommendation to be used in clinical practice or to assist in making clinical decisions.

The FDA also provided the following categories of types of mobile medical apps and their associated classifications:

- Displaying, storing or transmitting patient-specific medical device data in its original format
- Controlling the intended use, function, modes, or energy source of the connected medical device
- Transforming or making the mobile platform into a regulated medical device
- Creating alarms, recommendations or creating new information (data) by analyzing or interpreting medical device data

See Appendix A of the Draft Guidance for examples of each of the above mobile medical app categories/types.

Regulatory Requirements:

In Appendix C of the Draft Guidance, the FDA also provides a "high level description of some select regulatory requirements for medical devices, including mobile medical apps" (e.g., Establishment Registration and Medical Device Listing, Labeling requirements, Premarket submission for approval or clearance, Quality System regulation, Medical Device Reporting, Reporting Corrections and Removals).

Happtique echoes the concerns of the FDA with respect to technologies that pose significant risk and may fall under their surveillance. That said, we don't believe that the FDA should regulate mhealth products that are not considered to be medical devices. The FDA provided clarity in the Draft Guidance as to which mobile apps they do not anticipate classifying as mobile medical apps for purposes of regulation. Happtique agrees with the exclusions, as several significant topics that were excluded from the Draft Guidance are of great importance to the industry.

The following are examples of mobile apps NOT considered "mobile medical apps" by the FDA for purposes of the Draft Guidance:

- Mobile apps that are electronic "copies" of medical textbooks, teaching aids or reference materials, or are solely used to provide clinicians with training or reinforce training previously received
- Mobile apps that are solely used to log, record, track, evaluate, or make decisions or suggestions related to developing or maintaining general health and wellness
- Mobile apps that only automate general office operations with functionalities that include billing, inventory, appointments, or insurance transactions
- Mobile apps that are generic aids that assist users but are not commercially marketed for a specific medical indication
- Mobile apps that perform the functionality of an electronic health record system or personal health record system

Topics that were excluded from Draft Guidance (or to be addressed in a separate piece) include:

- wireless safety considerations
- classification and submission requirements related to clinical decision support software
- application of quality systems to software
- mobile medical apps that are intended to analyze, process, or interpret medical device data (electronically collected or manually entered) from more than one medical device

Due to clarity provided in the Draft Guidance, including these exclusions, Happtique, along with other industry stakeholders, anticipates only a small subset of the health app market (we estimate about 20%) would fall subject to regulatory oversight by the FDA in the event that any final guidance issued by FDA strongly resembles its Draft Guidance. In such event, much of the current health app market would appropriately not be subjected to heighted regulation or supervision. The majority of health apps would only be subject to regulation and oversight by other government agencies such as the Federal Communications Commission (FCC) and Federal Trade Commission (FTC). The size and expressed concern regarding the expected segment of the health app market not subject to heightened scrutiny by the FDA or other government agencies served as the genesis for Happtique to develop our Health App Certification Program (HACP).

Happtique's Health App Certification Program is a voluntary program borne out of the expressed need by many health care organizations and clinicians for a way to identify technically and substantively valid apps. As previously mentioned, there are currently as many as 40,000 health apps across multiple platforms on the market, with thousands more being added each year. While some app developers have submitted their applications to the FDA and received approval as medical devices, there is no reliable way for app users to readily distinguish credible apps from all others; thus, Happtique saw the need for an objective app assessment and validation process.

As you are aware, much in our health care delivery system is regulated by private sector organizations. For example, The Joint Commission accredits hospitals and other health care organizations and the various medical specialty societies provide physician board certification in their specialties. As a company whose origins are deeply rooted in health care; that is platform, device, and application neutral; has an in-depth understanding of existing regulatory requirements pertaining to medical devices, privacy and security requirements as defined under the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), children's online privacy requirements, and other health care-related laws and regulations; and has close ties to many key stakeholders in the health care industry, including hospitals, continuing care facilities, payers, and clinicians, we felt that there was a critical role and need for a private sector-based app certification program and that we were well suited to undertake this role.

Our efforts to develop a voluntary certification program began over a year ago with the formation of a distinguished Blue Ribbon Panel comprised of recognized leaders in mobile health, health care technology, health care certification and accreditation programs, and patient advocacy. Attached to my written testimony is a list of the members of this Panel, which I am pleased to submit for the record (Attachment A). Under the direction of this Panel, we have developed what we believe are a very rigorous set of standards and associated performance requirements. The standards encompass four areas: Operability, Privacy, Security, and Content. In total, there are nearly 150 standards and performance requirements; of these, 13 individual standards and more than 60 performance requirements focus specifically on privacy and security alone.

In developing the standards, we consulted with key public and private sector organizations, including the FDA, FTC, FCC, Office of the National Coordinator for Health Information Technology (ONC), American Medical Association (AMA) Association of American Medical Colleges (AAMC), Mobile Marketing Association (MMA), GSM Association (GSMA), mobile Healthcare Information and Management Systems Society (mHIMSS), and Association for Competitive Technology (ACT).

In July, 2012, we published the standards in draft form for public comment and received 115 comments from app developers/vendors, hospitals and health systems, trade organizations, information technology organizations, and other entities and individuals. After a thorough analysis of the comments, we made a number of revisions to the standards, and last month published the final set of standards and performance requirements, which we will use to evaluate apps once the certification program is underway. It should be noted that, while our standards are not officially endorsed by any Federal agency, they are explicitly designed to complement the existing regulations and guidelines of the FDA, FTC, FCC, and ONC, and it is our intent to modify them, as necessary, to ensure that they remain in lockstep with any new guidance or rules pertaining to mobile health applications that these agencies may issue in the future. As importantly, however, for the first time, they provide a solid basis for evaluating the thousands of apps that are not currently subject to any public agency regulation or oversight. Attached to my written testimony is a copy of HACP's final Standards and Performance Requirements, which I am also pleased to submit for the record (Attachment B).

HACP is a voluntary certification program that will be available to any publisher or developer of medical, health, and fitness apps intended for sale and/or use in the U.S. and that run on iOS, Android, Blackberry, or Windows smartphones and tablets. Web-based applications (so-called "Web apps"), other mobile health products, and mobile apps intended for sale or use outside the U.S. are not presently included in our certification program, but may be added in the future.

To conduct the certification process, we are engaging key organizations as certification program partners. Intertek, an internationally-recognized leader in the provision of testing, inspection, certification and auditing services to a wide range of industries and in the mobile application space, will test each app submitted for certification for its compliance with our Operability, Privacy, and Security—or so-called "Technical"—standards. Apps that pass the technical assessment will then be reviewed to validate their content. Content reviewers will have credentials relevant and appropriate for the content being reviewed. So, for example, cardiologists will review cardiology apps, nurses will review nursing apps, dieticians will review diet and nutrition apps, certified personal trainers will review fitness apps, and so forth. Presently, we are pleased that the AAMC and CGFNS International have agreed to serve as program partners for the purposes of reviewing medical/patient education apps and nursing apps, respectively, and we expect to finalize agreements shortly with numerous other partner organizations that will provide content experts in the many other clinical specialties and disciplines that we need to conduct this program. Apps that pass both the technical testing and content review will be awarded the Happtique Certification Seal. Certification will be valid for a two-year period and is specifically associated with the version of the app that was submitted for evaluation.

We are currently finalizing numerous other operational details associated with this program, including submission requirements, re-certification requirements, procedures for assuring compliance with our standards between certification reviews, and so forth. We are also forming an Advisory Board that will provide ongoing oversight of the operation of the program. Like any certification or accreditation program, we expect to continuously monitor the standards performance requirements and update them, as necessary. We are currently beta testing all of our systems and processes with a number of apps and expect to formally launch HACP this spring.

We are very excited about our certification program and believe it will play an extremely valuable role and make an important contribution in the mobile health arena by giving health care professionals, consumers, and patients the confidence they deserve to have in the apps they are using or recommending.

Mr. Chairman and members of the Subcommittee, I would now like to make a few remarks about questions regarding the medical device tax and how it relates to mobile health apps.

The Patient Protection and Affordable Care Act (PPACA) imposes an excise tax of 2.3% on certain medical devices in order to generate revenue to help offset the spending created by the law. In general, under the PPACA, a taxable medical device is a device that is listed by the FDA under Section 510(j) of the Federal Food, Drug, and Cosmetic Act and 21 CFR Part 807. There are specific medical devices that are exempt from the PPACA's excise tax, such as eyeglasses, contact lenses, and hearing aids. There is also an exemption, commonly called the retail exemption, for any device of a type that is generally purchased by the general public at retail for individual use.

The final regulations issued by the Internal Revenue Service provide for a "facts and circumstances" approach to determine whether a type of device meets the retail exemption. The regulations enumerate several factors that are relevant, with the determination being based on the overall balance of factors relevant to a particular type of device. A device will be considered exempt if it is regularly available for purchase and use by individual consumers who are not medical professionals, and if the design of the device demonstrates that it is not primarily intended for use in a medical institution or office or by a medical professional. One of several factors relevant is whether consumers who are not medical professionals can purchase the device in person, over the telephone, or over the Internet, through retail businesses such as drug stores, supermarkets, or medical supply stores and retailers that primarily sell devices.

Since the passage of PPACA, and increasingly over the last several months, the medical device excise tax has come under broad attack from industry groups, commentators, and legislators. While Happtique does not have a position on the existence of the medical device excise tax as a general matter, we are opposed to its imposition on the sale of smartphones, tablet devices, and apps used by any type of individual in any setting or circumstance.

We do not believe that it was the intent of Congress to impose an excise tax on iPhones, iPads, Android phones or tablets, or Blackberries. A fair reading of the final regulations implementing the tax should lead one to conclude that the retail exemption applies to all smartphones and tablets that are on the market today. A physician's use of an iPhone app to treat or diagnose a patient that has been regulated by the FDA as a mobile medical app does not change the nature of the iPhone from a consumer device sold to the general public at retail to a medical device subject to the medical device excise tax. As far as we can ascertain, nobody in the Congress, the Congressional Budget Office, or the investor community thought that the PPACA was imposing a 2.3% tax on Apple or RIM. We think that the retail exemption should apply in all circumstances to all smartphones and tablets that are sold the general public, but if for some reason there is confusion, doubt, or the IRS reaches a different conclusion, then changes should be made to the statute as appropriate, to the effectuate such a result.

With respect to mobile health apps, while we believe the FDA is the best suited and most appropriate agency to regulate those apps that fall under their purview for the reasons stated above, we believe that mobile apps, regardless of their intended use, or classification as medical devices or accessories to medical devices under the FDA's existing regulatory framework, should be exempt from the medical device excise tax. We recognize that due to the nature of some apps, the facts and circumstance test and the factors enumerated by the regulations may in some cases lead to the conclusion that the retail exemption does not apply, despite the fact that the app is sold in the App Store. We do not believe it was the intent of Congressto tax any apps sold in the Apple App Store or Google Play. If apps were intended to be taxed, the statute would have expressly stated so, and the tax would have been referred to as the medical device and software tax. Further, the imposition, or even the threat of imposing the medical device excise tax on app will stifle innovation for app developers and publishers, which is a market that was not the intended target of the tax.

In closing, may I again thank the Chairman and members of the Subcommittee for the opportunity to participate in this hearing. I would be happy to answer any questions you might have.

Attachment A

Happtique Health App Certification Program
Blue Ribbon Panel

- David Lee Scher, M.D., Panel Chair – former practicing cardiologist and mHealth authority
- Franklin Schaffer, EdD, RN, FAAN – Chief Executive Officer, CGFNS International
- Shuvo Roy, Ph.D. – Director, Biomedical Microdevices Laboratory and Associate Professor, Department of Bioengineering and Therapeutic Sciences, School of Pharmacy, University of California, San Franciso
- Dave deBronkart (“ePatient Dave”) – well-known spokesman for patient engagement

Attachment B

Happtique™

Your Prescription for Mobile Health

HEALTH APP CERTIFICATION PROGRAM

CERTIFICATION STANDARDS

February 27, 2013

happtique.com @happtique

TABLE OF CONTENTS

App Operability (OP) Standards[1]

Standard OP1

The app installs, launches, and runs consistently[2] on the target device(s) and target operating system(s) for that app.

Performance Requirements for Standard OP1

- OP1.01 The app downloads and installs on the target device(s) and target operating system(s).
- OP1.02 The app consistently launches and runs on the target device(s) that it is installed upon.

Standard OP2

If applicable, the app connects consistently to any and all peripheral or accessory devices (e.g., NFC, Bluetooth), third party mobile application or software, regulated or unregulated, required for operation and/or marketed for use in conjunction with such app.

Performance Requirements for Standard OP2

- OP2.01 The app connects to the peripheral device(s) and operates consistently.
- OP2.02 The app has a mechanism to notify the user in the event that the app fails to connect to any and all peripheral or accessory devices.
- OP2.03 The app connects consistently to any and all third party mobile applications, software, and online user accounts, but such connection shall only occur after: (i) notifying user; (ii) requesting permission; and (iii) receiving consent from the user.
- OP2.04 The app has a mechanism to notify user of any and all updates applicable or necessary for app to connect to any such device, application, software or online user accounts.

Standard OP3

If the app requires that it be connected to a network, the app is able to connect and operates consistently on the intended domestic and global carriers or Local Area Network (LAN).[3]

Performance Requirements for Standard OP3

- OP3.01 The app connects to the network via wireless technology (e.g., CDMA2000 and GSM).
- OP3.02 The app connects to the LAN via well-established standards (e.g., 802.11, 802.15, 802.16).

[1] These standards are based, in part, on materials from the National Alliance for Health Information Technology, the Mobile Marketing Association's "Mobile Application Privacy Policy Framework" (December, 2011), and GSM Association's "Privacy Design Guidelines for Mobile Application Development" (February, 2012).

[2] To be defined in conjunction with vendors performing Technical Standards testing.

[3] Due to the number of mobile operators (approx. 800), two U.S. operators and WiFi will be used as a proxy for this test.

Standard OP4

If the app connects to the network, the IP addresses and URIs are known or can be determined.

Performance Requirements for Standard OP4

- OP4.01 The list of IP addresses and/or URIs that the app connects to are documented, and the owners of those addresses and domain names are either disclosed or are capable of being determined from testing.
- OP4.02 The app does not connect to any hidden IP addresses that are used behind the firewall of a router or gateway, without user's knowledge, control, or consent.

Standard OP5

A method for contacting the App Publisher and technical support (if different than the App Publisher) is provided.

Performance Requirements for Standard OP5

- OP5.01 The App Publisher's contact information—including but not limited to, mailing address, email address for support and general inquiries, web address and/or DNS address—is provided within the app, or the app provides a link to a webpage that contains the same information.
- OP5.02 The app provides a method for users to submit feedback to the App Publisher for purposes of improving the user experience, including without limitation, any technical issues, bugs, and errors detected by users.

Standard OP6[4]

The app shall be designed to operate in a manner that supports a usable and useful end-user experience.

Performance Requirements for Standard OP6

- OP6.01 App Publisher has a documented process to review, escalate and incorporate, on a timely basis, modifications needed to address suspected errors and other technical issues.
- OP6.02 In designing and maintaining the app, the App Publisher has a documented process for addressing:
  - User feedback regarding efficiency (the speed with which users can complete their tasks), effectiveness (the accuracy and completeness with which users can complete tasks), and satisfaction (the user's satisfaction with how well the app operates); and

[4] This Standard is derived from the mHIMSS report, "Selecting A Mobile App: Evaluating the Usability of Medical Applications" (see http://www.mhimss.org/resource/selecting-mobile-app-evaluating-usability-medical-applications).

    - Reasonable requests by users regarding features and functionality not supported by the app (e.g., support in additional languages, audiology assistance, visual impairment support, and other requests specific to the demographic of the app's intended audience).

Standard OP7

Electronic health record (EHR) systems optimized for mobile devices are apps for certified EHRs (EHRs that have been certified by a Federally-designated Authorized Testing and Certification Body). Certified EHRs may consist of complete EHRs or EHR modules.

Performance Requirements for Standard OP7

- OP7.01 The app operates in accordance with the documented functionality provided by the Certified EHR.
- OP7.02 Documentation is provided regarding any relevant EHR certification received.

Standard OP8

An app that is intended to connect to an Electronic Health Record (EHR) or Personal Health Record (PHR) enables users to send and retrieve patient information between a mobile device and the EHR/PHR, and does so in a secure manner.

Performance Requirements for Standard OP8:

- OP8.01 The EHR and/or PHR systems with which the app connects (e.g., Allscripts, Epic, Microsoft HealthVault, etc.) are specifically enumerated and documentation of the interoperability with each specified EHR and PHR is provided.
- OP8.02 The details and description of the data fields that the app saves, sends to, and/or receives from each specified EHR/PHR systems regarding patient information (e.g., medical history, diagnoses, treatment plan, medications, laboratory results, radiology images, etc.) is provided.
- OP8.03 The app maintains (*at rest*) and transmits (*in motion)* patient information in a secure, HIPAA-compliant manner, as applicable (see Standards S2, S3, and S4).

Standard OP9

The App Publisher certifies that the app constitutes a medical device as defined by the U.S. Food and Drug Administration (FDA), has ascertained its correct classification, and either certifies that the app complies with all applicable FDA regulatory requirements[5] or certifies that it is not a medical device.

Performance Requirements for Standard OP9

- OP9.01 The App Publisher has ascertained that the app, including any and all peripheral devices required or intended for operation and/or marketed for

[5] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm

use in conjunction with such peripheral devices, is a Class I, II or III medical device[6].

- OP9.02 The App Publisher provides documentation demonstrating that the app complies with all applicable FDA requirements, including but not limited to: Establishment registration; Medical Device Listing; Premarket Notification 510(k)[7], unless exempt, or Premarket Approval (PMA)[8]; Investigational Device Exemption (IDE) for clinical studies; Quality System (QS) regulation; Labeling requirements; and Medical Device Reporting (MDR).
- OP9.03 The App's Publisher has a mechanism to immediately notify all users and Happtique about an FDA-approved app that is recalled, the subject of an FDA advisory, or similar status that calls the app's safety and/or effectiveness into question.
- OP9.04 If the app does not constitute a medical device as defined by the FDA, the App Publisher certifies that the app is not a medical device by written attestation on the HACP App Submission Form.

[6] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/default.htm

[7] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/default.htm

[8] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/default.htm

App Privacy (P) Standards[9]

Standard P1

The type(s) of data that the app obtains, and how and by whom that information is used, is disclosed to the user in a Privacy Policy.

Performance Requirements for Standard P1

- P1.01 Prior to downloading, installing, or activating an app, the identity of any entities that will have access to, collect and/or use of the user's personal information, including a company or individual name, country of origin, and related contact information is disclosed to the user.
- P1.02 App Publisher discloses any and all ownership, rights or licenses to any data collected in connection with the app and its usage, including the use of any data for commercial purposes.
- P1.03 The app has a section (tab, button or equivalent) or active link to its Privacy Policy, and owner represents that commercially reasonable efforts are used to notify users of any material changes to its Privacy Policy.
- P1.04 If registration is required to use all or some of the app's features, the user is provided with an explanation as to the uses of the registration information.
- P1.05 User is provided (or has access to) a clear list of all data points collected and/or accessed by the app, including by App Publisher and any and all third parties such as in-app advertisers, pertaining to the usage of the app, including but not limited to browsing history, device (e.g., unique identifiers), operating system, and IP addresses. How and from where such data points are collected is disclosed.
- P1.06 User is provided (or has access to) a clear list of all data points collected and/or accessed by the app pertaining to the specific user, including user-generated data and data that are collected automatically about the user through other means or technologies of the app. This includes data points collected for the purpose of any third-party sharing. How and from where such data points are collected is disclosed.
- P1.07 App Publisher obtains affirmative express consent before using user data in a materially different manner than was previously disclosed when collecting the data or collecting new data, including for the purpose of third-party sharing.
- P1.08 App Publisher obtains affirmative express consent before collecting personal data, in particular information about children, financial and health information, Social Security numbers, and location data.
- P1.09 The Privacy Policy informs users how they can get a copy of their personal information that was collected by the app. The Privacy Policy also informs users how they can correct and update information supplied by, or collected about them, held by or on behalf of the owner, or shared with

[9] In general, these Privacy Standards are intended to be consistent with the principles set forth in "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Federal Trade Commission, March, 2012.

third parties, including the identity of such third parties, particularly in compliance with the HIPAA Privacy Rule[10], if applicable, and any other laws, rules, or regulations to the extent applicable.

- P1.10 If not otherwise provided by default, the app allows users to control the collection and use of their in-app browsing data by supporting an online Do Not Track mechanism, if applicable.
- P1.11 If not otherwise provided by default, the app allows users to control their receipt of commercial messages from the App Publisher and third parties through an "opt out" option, "do not contact," or substantially similar feature.
- P1.12 Each major component of the Privacy Policy is affirmatively agreed to by the user. Such components include, but are not limited to, entities that will have access to, collect and/or use of the user's personal information; all ownership, rights or licenses to any data collected and its usage; list of all data points collected; and so forth.
- P1.13 Except when expressly disclaimed by App Publisher and the user provides an affirmative consent, App Publisher does not share any user data with third parties, unless App Publisher: (i) has an agreement with such third party that addresses safeguarding any and all such user data; and (ii) takes the necessary measures to anonymize/de-identify all user data. The App Publisher has documented this within the Privacy Policy.

Standard P2

If data are collected, the user is informed about how long the data are retained.

Performance Requirements for Standard P2

- P2.01 The Privacy Policy discloses the retention policy regarding user information. Such statement includes policies with respect to data retention under any third-party data sharing arrangement.
- P2.02 Retention and deletion time periods, which are based on clearly defined business needs or legal obligations, are set. If business needs are defined as "in perpetuity," this is disclosed.

Standard P3

The app user is informed if the app accesses local resources (e.g., device address book, mobile and/or LAN network interface, GPS and other location-based services, contacts, camera, photos, SMS or MMS messaging, and Bluetooth) or resources from and/or for social networking platforms, provided with an explanation by any appropriate means (e.g., the "About" section) as to how and why such resources are used, and prior consent is obtained to access such resources.

[10] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

Performance Requirements for Standard P3

- P3.01 If the app uses the mobile network, why the network is being used and a reasonably likely estimate of the average amount of bandwidth consumed per user per month is disclosed to the user.
- P3.02 If the app uses a LAN, why the network is accessed and a likely estimate of the average amount of bandwidth consumed per user per month is disclosed to the user.
- P3.03 If the app or App Publisher uses SMS or MMS messaging, the user is provided with a likely estimate of the average number of messages per month, and a disclosure that data rates will apply.
- P3.04 If the app or App Publisher sends emails, the user is provided with a likely estimate of the number of emails sent per month.
- P3.05 If the app uses Bluetooth, why Bluetooth is being used and which of the Bluetooth profiles are being used is disclosed to the user.
- P3.06 If the app uses the device's camera, why the camera is being used is disclosed to the user.
- P3.07 If the app uses device-available methods to determine location, why the location is being determined is disclosed to the user.
- P3.08 If the app accesses the device's native address book, why the address book is being used is disclosed to the user.
- P3.09 If the app accesses the device's native calendaring or alarm system, why the calendar and/or alarm system is being used is disclosed to the user.
- P3.10 If the app accesses the Public Switched Telephone Network (PSTN), why the PSTN is being accessed is disclosed to the user.
- P3.11 If the app accesses social networking sites, the reason why such sites are being accessed is disclosed to the user.

Standard P4

If the app, on behalf of a Covered Entity or a Business Associate (each as defined by HIPAA and HITECH and the rules thereunder), collects, stores, and/or transmits information that constitutes Protected Health Information (as defined by HIPAA and HITECH and the rules thereunder), it does so in full compliance with HIPAA, HITECH, and all applicable laws, rules and regulations.

Performance Requirements for Standard P4

- P4.01 The user can affirmatively opt in or out (at any time) of information shared with or given access by third parties.
- P4.02 The App Publisher certifies that a Business Associate Agreement (BAA) has been executed pursuant to HIPAA with any and all necessary third parties.
- P4.03 The user has the ability to access or request any of his/her Protected Health Information (PHI) collected, stored and/or transmitted by the app, and has the ability to learn the identity of any person or entity who had or has been granted access to his/her PHI.
- P4.04 The App Publisher uses requisite efforts to limit the use and disclosure of PHI, including ePHI, to the minimum necessary to accomplish the intended purpose (e.g., "need-to-know").

Standard P5

The app has measures in place to protect children in accordance with applicable laws and regulations (e.g., Children's Online Privacy Protection Act[11]).

Performance Requirements for Standard P5

- P5.01 The app provides clear notice of the content that will be made available and its suitability for specific age groups.
- P5.02 The app includes a clear and conspicuous Privacy Policy that addresses use by any child under the age of 13.
- P5.03 The app provides for an age verification process—either automatic or self-reported—to control access to age-restricted content and to minimize the inappropriate collection, use, or disclosure of personal information from a child.
- P5.04 The app does not, without obtaining verifiable parental/legal guardian consent, collect, use, or disclose data from any child under the age of 13.
- P5.05 The app enables a parent/legal guardian who becomes aware that the child has provided information without his/her consent to contact the App Publisher.
- P5.06 The Privacy Policy provides that the App Publisher will delete any child's personal information upon notice, or in the event that the App Publisher becomes aware or has knowledge, that such information was provided without the consent of a parent/legal guardian, including information that was shared with a third party.
- P5.07 Apps that are intended for children must have a location default setting that enables parents/legal guardians to prevent the app from automatically publishing their child's location.

Standard P6

Retroactive or prospective material changes to Privacy Policies require the prior consent of the user.

Performance Requirements for Standard P6

- P6.01 A mechanism is in place to notify users of changes to the Privacy Policy.
- P6.02 A mechanism is provided that enables users to acknowledge and consent to changes to the Privacy Policy.

[11] http://www.ftc.gov/ogc/coppa1.htm

App Security (S) Standards

Standard S1

The app, including without limitation, any advertisement displayed or supported through the app, is free of known malicious code or software such as malware, including, but not limited to, viruses, worms, trojan horses, spyware, adware, rootkits, backdoors, keystroke loggers, and/or botnets.

Performance Requirements for Standard S1

- S1.01 A scan of the app using scanning software does not reveal any known malicious code or software objects.
- S1.02 A scan of any third party code, including advertising networks, incorporated into app for purposes of displaying or supporting advertisements (e.g., banner, interstitial) does not reveal any known malicious code or software.

Standard S2

The App Publisher ensures that the app's security procedures comply at all times with generally recognized best practices and applicable rules and regulations for jurisdiction(s) in which the app is intended to be sold or used and such procedures are explained or made available to users.

Performance Requirements for Standard S2

- S2.01 Administrative, physical, and technical safeguards to protect users' information from unauthorized disclosure or access are provided and employed.
- S2.02 Access to user's information is limited to those authorized employees or contractors who need to know the information in order to operate, maintain, develop, or improve the app.
- S2.03 If the app utilizes unique identifiers, the identifier is linked to the correct user and is not shared with third parties.
- S2.04 Where possible, risk-appropriate authentication methods are used to authenticate users.
- S2.05 A written description of security procedures (in detail sufficient to apprise end users about how their personal information is safeguarded) is provided in a section of the app (tab, button, or equivalent) or through an active link. The security procedures are written in clear, easy-to-understand language and terms and are affirmatively agreed to by the user. Such components include, but are not limited to, how personal information is safeguarded, how unique identifiers are linked to the correct user, and authentication methods used.
- S2.06 The App Publisher has a mechanism in place to review security procedures on an ongoing basis and update security procedures, as necessary, to ensure that they comply at all times with applicable rules and regulations for jurisdiction(s) in which the app is intended to be sold or used.
- S2.07 Cloud-based apps meet Statement on Standards for Attestation Engagements (SSAE) No. 16 requirements and a SSAE No. 16 audit report is provided.

- S2.08 If the app uses SMS or MMS, the user is informed whether messages are encrypted and, if so, the level of encryption.
- S2.09 The App Publisher has a formal and documented secure software development lifecycle (SDLC) process that has been implemented throughout the inception, testing, implementation, deployment, and maintenance of the app.

Standard S3

If the app collects, stores or transmits any personal information, including, but not limited to, usernames and passwords, such information is collected, stored, and transmitted using encryption.

Performance Requirements for Standard S3

- S3.01 Passwords are stored using a random length, one-way salted hash, SHA-1 or better.
- S3.02 Usernames and passwords are collected and transmitted only when using encryption between the client app and the server.
- S3.03 Other personal information while at rest and/or in motion is encrypted using a generally recognized, industry-accepted encryption method (e.g., FIPS 140-2[12], ISO/IEC) for such information and the encryption level is disclosed.
- S3.04 App contains security safeguards to verify the identity of intended user in the event of forgotten, lost or unknown user name, password and/or passcode ("unique identifiers"), for purposes of reminders, re-linking, or creation of new unique identifiers.

Standard S4

If the app collects, stores and/or transmits information that constitutes PHI as defined by HIPAA, HITECH, and the rules thereunder (e.g., App Publisher constitutes a Business Associate pursuant to HIPAA and HITECH), it uses requisite efforts to maintain and protect the confidentiality, integrity, and availability of individually identifiable health information that is in electronic form (e.g., ePHI).

Performance Requirements for Standard S4

- S4.01 If the app, or through its use, subjects the user or any party to HIPAA or HITECH, the App Publisher has implemented administrative, physical and technical safeguards, and developed policies and procedures, pursuant to the HIPAA Security Rule[13], as applicable. For purposes of the technical safeguards/security controls, only certain certified encryption technologies are permissible for compliance with HIPAA and HITECH.
- S4.02 If the app is, or through its use becomes, subject to HIPAA or HITECH, all PHI collected and/or stored is encrypted at all times and is otherwise protected in accordance with HIPAA and HITECH.

[12] http://csrc.nist.gov/groups/STM/cmvp/standards.html#02

[13] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

- S4.03 If the app is or becomes subject to HIPAA or HITECH, all data transmission to and/or from the app through any network with any server, system, software, application and third party is encrypted at all times.
- S4.04 If applicable, the app or the App Publisher has safeguards in place and/or uses requisite efforts to comply with any and all obligations pursuant to any BAA, including capabilities to assist a covered entity in curing any breach, and address all other requirements of HITECH in the event of a breach.
- S4.05 The App Publisher has the capabilities to enable compliance, and shall comply with any and all applicable notification requirements to its users in the event that users' PHI is or is suspected to be compromised (e.g., Breach Notification Rule pursuant to HIPAA and HITECH including the capability to support and execute notification requirements[14]).

Standard S5

If the app collects, stores and/or transmits personal information, the app offers one or more industry-accepted methods for guarding against identity theft.

Performance Requirements for Standard S5

- S5.01 The app provides a method for securely authenticating the user at a session level (e.g., password, pass phrase, PIN, challenge phrase) and also utilizes additional methods or techniques[15] to further secure the identity of the users whenever the system is initially establishing identity or the system has indications that the identity might have been compromised (e.g., multiple password failures).

Standard S6

The App Publisher has a mechanism to notify end users about apps that are banned or recalled by the App Publisher or any regulatory entity (e.g., FDA, FTC, FCC).

Performance Requirements for Standard S6

- S6.01 In the event that an app is banned or recalled, a mechanism or process is in place to notify all users about the ban or recall and render the app inoperable.
- S6.02 In the event that the app constitutes a medical device (e.g., 510(k)) or is regulated by the FDA in any other capacity, the App Publisher has a policy and a mechanism in place to comply with any and all applicable rules and regulations for purposes of handling all aspects of a product notification or recall, including all corrections and removals.

[14] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

[15] Examples of additional methods or techniques might be the use of certificates signed by recognized certificate authorities, two-factor authentication methods, static knowledge based authentication methods, and/or dynamic knowledge-based authentications.

Standard S7[16]

The app implements reasonable and requisite security measures to safeguard user financial data in accordance with any and all applicable laws, regulations, industry best practices, and standards.

Performance Requirements for Standard S7

- S7.01 Any app that collects, stores and/or transmits user financial data for any purpose, including payment processing, or the app directs to any website for the purpose of collecting and/or processing of financial information, including any third party website, shall comply with any and all applicable Federal and state laws, rules and regulations, and private sector regulatory best practices guidelines and initiatives regarding data security requirements (e.g., Section 5 of the FTC Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Payment Card Institute Data Security Standards, the SANS Institute's security policy templates, and standards and best practices guidelines for the financial services industry provided by BITS, the technology policy division of the Financial Services Roundtable).

[16] FTC Act, Section 5, available at: http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf

PCI Security Standards Council, PCI SSC Data Security Standards Overview, available at: https://www.pcisecuritystandards.org/security_standards/

SANS Institute, Information Security Policy Templates, available at: http://www.sans.org/security-resources/policies/

BITS, Financial Services Roundtable BITS Publications, available at: http://www.bits.org/publications/index.php

App Content (C) Standards[17]

Standard C1

The app is based on one or more credible information sources such as an accepted protocol, published guidelines, evidence-based practice, peer-reviewed journal, etc.

Performance Requirements for Standard C1

- C1.01 If the app is based on content from a recognized source (e.g., guidelines from a public or private entity), documentation (e.g., link to journal article, medical textbook citation) about the information source and copyright compliance is provided.
- C1.02 If the app is based on content other than from a recognized source, documentation about how the content was formulated is provided, including information regarding its relevancy and reliability.

Standard C2

The app's content reflects up-to-date information (as of the date that the app is submitted for certification).

Performance Requirements for Standard C2

- C2.01 Documentation about the source of the app's content and explanation as to why it is deemed to be up-to-date is provided.
- C2.02 The date(s)/source(s) of the app's content is provided through an "About" section (tab, button or equivalent).
- C2.03 The App Publisher has a method or protocol for determining if an app's content requires updating in order to remain up-to-date.
- C2.04 The App Publisher has a method or protocol for updating the app's content when new or changing information warrants. Updates should include a description of and documentation for each change.

Standard C3

For any app that contains content that is derived from a third-party source (e.g., accepted protocol, published guidelines, evidence-based practice, peer-reviewed journal), any significant deviations in an app's content from the original source (e.g., excerpts, abbreviated versions) are indicated and explained. Any such app shall also provide a method or citation to enable the user to locate to the complete content.

Performance Requirements for Standard C3

- C3.01 For any app derived from a third-party source that does not contain the original source's complete content, such app's description or "About"

[17] These standards are based, in part, on materials from the Association of American Medical Colleges (AAMC), including AAMC's MedEdPORTAL Submission Standards and Scholarly Criteria (https://www.mededportal.org/download/262700/data/mepsubmissionstandards.pdf).

section shall indicate the specific portion(s) absent and contain an explanation as to why each portion(s) is not included.

- C3.02 For any app derived from a third-party source that does not contain the original source's complete content, the app provides a link, reference, or other appropriate method to enable the user to locate the complete content.

Standard C4[18]

The app's description and content are truthful, fair, and not misleading.

Performance Requirements for Standard C4

- C4.01 Backup documentation is provided to substantiate any claims made in the description and/or content.
- C4.02 Disclosures are provided, as needed, to prevent deception. Such disclosures shall be presented in a clear and conspicuous manner.
- C4.03 Disclosures are provided, as needed, if the app requires an additional fee(s) (e.g., subscription fee) in order to fully access the app, its associated functionality, and/or content.

Standard C5

An app that contains tools that perform user or patient management functions, including but not limited to, mathematical formulae, calculations, data tracking, reminders, timers, measurements, or other such functions, does so with consistent accuracy and reliability to the degree specified in the app.

Performance Requirements for Standard C5

- C5.01 When operated, the app produces consistent and accurate results that are independently verifiable.

Standard C6

Reference apps (e.g., apps that are used for reference purposes to inform clinical decision-making, etc.) derive their content from one or more authoritative sources.

Performance Requirements for Standard C6

- C6.01 The app's content is based on authoritative sources as recognized by the field or discipline that is the subject of the app.
- C6.02 As appropriate, prior accepted work (e.g., published, peer reviewed) is used to derive the content of the app.
- C6.03 The source(s) and date(s) (e.g., published, last modified) of the app's content are cited.

[18] For further information and guidance, refer to "Dot Com Disclosures: Information about Online Advertising," Federal Trade Commission. (http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf)

Standard C7

Instructional, educational assessment, and other such apps (e.g., apps used in educational settings for physicians, nurses, students, etc.) derive their content from one or more authoritative sources and are based on accepted pedagogy and/or learning strategies or techniques that are appropriate for the intended audience(s).

Performance Requirements for Standard C7

- C7.01 The app's content is based on authoritative sources as recognized by the field or discipline that is the subject of the app (e.g., recognized textbook and/or peer-reviewed journals in an applicable field or discipline).
- C7.02 As appropriate, prior accepted work (e.g., published, peer reviewed) is used to derive the content of the app.
- C7.03 The source(s) and date(s) (e.g., published, last modified date) of the app's content are cited.
- C7.04 The app's learning goals and objectives are clearly stated.
- C7.05 The app uses suitable teaching and/or learning approaches to meet its stated objectives.
- C7.06 A process or method for assessing and documenting improvements in knowledge or skills is provided.

Standard C8

Apps that constitute clinical decision support (CDS) software and apps that integrate or work in conjunction with CDS software, comply with current rules and regulations, if applicable (e.g., for CDS software that is regulated by the FDA), and evidence-based/accepted practice guidelines.

Performance Requirements for Standard C8

- C8.01 Documentation is provided regarding the regulations and any applicable evidence-based/accepted practice guidelines that the app operates in accordance with.
- C8.02 App has a process and mechanism to deliver all applicable updates pursuant to any relevant guidelines when such guidelines are issued or made available.

Standard C9

For a multi-purpose app (e.g., apps that have reference, instructional, or educational assessment content, integrate or work with CDS software, etc.),where each element of the app can be separated for testing, each element of the app meets the requirements of the relevant Content Standard(s) herein.

Performance Requirements for Standard C9

- C9.01 Each separate function and/or content area is defined, documented, and operates in accordance with relevant Content Standards described herein.

Standard C10

An app that contains advertisements clearly identifies the advertising and complies with any and all applicable regulatory requirements, particularly advertisements that involve or relate to products or services that are clinical or related to health.

Performance Requirements for Standard C10

- C10.01 Information in any app that constitutes advertising is denoted by the message "This is an advertisement" or equivalent.
- C10.02 Information in any app that constitutes advertising will at all times comply with all applicable regulatory requirements related to the marketing of any product or service, including, but not limited to those of the FDA, FTC, FCC, and any laws, rules, regulations and policies of other regulatory entities in all jurisdictions that app's owner makes its app available.
- C10.03 App Publisher takes commercially reasonable efforts to clearly and prominently indicate (e.g., in the "About" section) that any advertisement, which may be perceived as health care or medical advice or treatment, is being displayed for the sole purpose of advertising and should not be construed as a substitute for medical or clinical advice.

Standard C11

The content of apps should be written and presented in a manner that is appropriate for the intended audience.

Performance Requirements for Standard C11

- C11.01 The content of an app is designed and written in a way that is appropriate for the target audience (e.g., age, educational background, healthcare professional versus patient or consumer, caregiver, and so forth).

Appendix 1. Acronyms

A number of acronyms are used in this document. The following table provides the full term for each acronym.

Acronym	Full Term
AAMC	Association of American Medical Colleges
BA	Business Associate refers to a person/entity that requires disclosure of ePHI in order to deliver their product/service to or on behalf of a Covered Entity.
BAA	Business Associate Agreement (required in certain circumstances under HIPAA and HITECH [defined below])
CDMA2000	Refers to a family of 3G standards providing high-quality voice and broadband data services over wireless networks
CDS	Clinical Decision Support software
DNS	Domain Name System
EHR	Electronic Health Record (also referred to as EMR – Electronic Medical Record)
FCC	Federal Communications Commission
FDA	U.S. Food and Drug Administration
FTC	Federal Trade Commission
GPS	Global Positioning System (a satellite-based navigation system)
GSM	Global System for Mobile Communications (originally, Groupe Spécial Mobile)
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
LAN	Local Area Network
MMS	Multimedia Messaging Service
NFC	Near Field Communication
PHI	Protected Health Information
PSTN	Public Switched Telephone Network
SMS	Short Message Service
URI	Uniform Resource Identifier