mdpc | medical device privacy consortium

June 1, 2013

VIA EMAIL TO IOT@FTC.GOV

Karen Jagielski
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue N.W.
Room H-113 (Annex B)
Washington, DC 20580

Re: Solicitation of Input on Privacy and Security Implications of the Internet of Things

Dear Ms. Jagielski:

These comments are submitted on behalf of the Medical Device Privacy Consortium, a group of leading companies addressing health privacy issues affecting the medical device industry (the "MDPC").[1] Members of the MDPC manufacture a diverse range of products, from molecular diagnostics to medical imaging equipment to implantable devices, for example. The MDPC appreciates this opportunity to provide input on the privacy and security issues posed by the growing connectivity of consumer devices ("The Internet of Things"), in advance of the public workshop to be held on this issue in November.

Over the last century, medical science has transformed human health. At the start of the 20th Century, the average life expectancy in developed countries was slightly over 45 years. Today, life expectancy exceeds 75 years. Diseases that once would have led to a near-term death can now be managed through drugs and devices. For example, the development of insulin resulted in a tripling of the life expectancy of diabetics. But these advances also have resulted in an increasing prevalence of chronic diseases and conditions – for conditions that once would have been acute can now be controlled, and because people are living longer, conditions like heart disease are more likely to occur.

As health care needs change, the traditional paradigm for delivery of health care has to adapt as well. An ageing population increasingly seeks treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility. In parallel, patients are increasingly reaching out to similarly situated patients through online support communities. These changes not only improve individual lives,

[1] For further information concerning the MDPC, please visit our website at www.deviceprivacy.org.

they benefit society by allowing resources to be more efficiently allocated. When a patient can effectively manage his or her condition at home, the costs of a trip to the doctor or hospital stay can be avoided.

With this backdrop in mind, this paper will describe some of the ways the medical device industry has tried to respond to patient demands. The topics to be addressed include (i) remote monitoring of patient health and safety; (ii) remote management and servicing of medical devices; and (iii) connectivity of medical devices to personal health records and online/mobile applications. For each topic, we will discuss the privacy and security issues that arise.

We focus in this paper on prescription medical devices. As the FTC considers privacy and security issues associated with the connectivity of a range of consumer devices, it is important to understand the regulatory framework that already applies to prescription medical devices. Prescription medical devices are subject to a complex web of Food and Drug Administration (FDA) regulations, and any further regulatory initiatives in this area should be led by the FDA. The definition of a medical device under the Federal Food Drug & Cosmetic Act is broad and includes any instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other article intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease, or intended to affect the structure or function of the human body. Prescription medical devices can include, *inter alia*, implantable/on-body devices, peripheral/supporting devices, capital equipment, and IT systems.

1. Remote Monitoring of Patient Health and Safety

Remote patient monitoring technologies can be effective in managing chronic disease and post-acute care. They can also be used to alert caregivers to situations requiring immediate attention. Many medical devices on the market today come with remote communication abilities embedded or available as optional attachments. For example, many implanted cardiac devices (pacemakers, cardioverter defibrillators, etc.) allow for data to be transmitted to the manufacturer and then made accessible to the patient's health care provider through a web interface. Some devices passively collect this data before transmitting it to the manufacturer (e.g., a wireless peripheral in the patient's home automatically receives information from the device) while others require some action by the patient (e.g., holding a wand near the body to upload information from the implanted device to a peripheral). The data may then be transmitted over an analog phone line, GSM network, or via an ISP.

Some remote patient monitoring technologies can be connected to multiple peripheral devices (e.g., blood pressure cuff, scale, glucose monitor, pulse oximeter, pedometer, etc.). The connections between the communicator and the peripheral devices may be wired or wireless. Any number of wireless transmission protocols or technologies may be used (e.g., Bluetooth™, Zigbee™, WiFi™, WiMax™, RFID, etc.).

As indicated, typically a web interface enables the patient's health care provider to view, print, and/or download information transmitted to the manufacturer from the remote patient monitoring technology. The health care provider may be able to configure periodic reports to be automatically transmitted. In addition, acute events may trigger an alert to the health care provider via email, fax, text message, or phone. Patients may be able to access some or all of the data related to them via patient-directed web sites.

Security of data generated or transmitted by remote patient monitoring technologies is a priority. Manufacturers' web sites typically employ firewalls and encryption to protect patient data. Users must register and are provided, or prompted to create, access credentials (username, password, etc.). With respect to the medical devices themselves, security requirements based on the risks must be incorporated into device design. For devices that employ wireless communication, the wireless signal could be subject to interception of data, and there is the potential for external interference (intentional or otherwise) which could impact device performance. For manufacturers, these security risks must be managed while keeping in mind design limitations. For example, implanted medical devices may require emergency access modes that bypass a subset of security features.

The MDPC recently launched a new working group on medical device product security. The MDPC's product security working group aims to advance industry dialogue and information sharing on how to protect medical devices from security threats and address related privacy concerns. The working group intends to monitor, analyze, and influence global standards and guidelines on medical device product security and develop practical tools that can be used to enhance product security. Further, the working group intends to liaise with other medical device industry stakeholders to gather and share intelligence regarding industry-wide efforts related to product security.

At the regulatory level, both FDA medical device regulations and regulations promulgated by the HHS Office for Civil Rights (OCR) under the Health Insurance Portability and Accountability Act (HIPAA) can be relevant to remote patient monitoring privacy and security. As part of the FDA's premarket approval (PMA) process for Class III medical devices, the FDA considers various risks, which can include information security risks. Recommendations concerning the FDA's consideration of information security risks were recently the subject of a report by the US Government Accountability Office.[2] When patches are necessary to update the software on a medical device in response to a security vulnerability, the patch must undergo thorough assessment and testing before it can be released. As FDA explains in its guidance for industry on software validation:

> When changes are made to a software system, either during initial development or during post release maintenance, sufficient

[2] GAO, "FDA Should Expand Its Consideration of Information Security for Certain Types of Devices," GAO-12-816 (Aug 2012).

> regression analysis and testing should be conducted to demonstrate that portions of the software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correctness of the implemented change(s).
>
> The specific validation effort necessary for each software change is determined by the type of change, the development products affected, and the impact of those products on the operation of the software. Careful and complete documentation of the design structure and interrelationships of various modules, interfaces, etc., can limit the validation effort needed when a change is made. The level of effort needed to fully validate a change is also dependent upon the degree to which validation of the original software was documented and archived.[3]

In addition to validation of the patch itself, in limited circumstances (e.g., where the patch could make the device less safe or effective), changes to medical device software can require FDA clearance or approval. Because there is a complex regulatory structure already covering prescription medical devices, the MDPC believes that any further regulatory initiatives relating to such devices should be led by the FDA.

Remote patient monitoring services can trigger a HIPAA business associate relationship between the service provider and the covered health care provider. Under changes to the HIPAA regulations that became effective in March 2013, HIPAA business associates must comply with the Security Rule and many provisions of the Privacy Rule in their performance of the covered function or service.

2. Remote Management and Servicing of Medical Devices

Remote service is the delivery of hardware and/or software system support, maintenance, and troubleshooting from a location beyond the healthcare delivery organization's site. Remote servicing capability has become common for most IT-based medical equipment. Remote servicing allows an equipment service provider to more efficiently:

- Monitor system performance and be alerted to out-of-parameter performance issues. This enables early detection of potential hardware and/or software problems that could jeopardize the correct operation or continued availability of the device. It also enables monitoring and diagnosing the cause of sporadic technical problems that are difficult to replicate in on-site service visits.

[3] FDA, General Principles of Software Validation (Jan 11, 2002) at Section 5.2.7.

- Provide immediate support in the event of a system failure. Remote service connections provide the most time efficient way for service technicians to assess the severity of the problem and determine possible solutions. This can be particularly critical when a failure occurs during a medical procedure and the healthcare provider requires immediate assistance.
- Perform routine maintenance such as upgrading of software components and implementation of patches. The rapid deployment of such maintenance can be critical to ensuring that a device is protected against malware and other cyber-security threats.
- Provide information and "over-the-shoulder" support on proper use of a device. Traditionally, such training and support either required the on-site presence of a medical device representative or had to be conducted over the phone with attendant limitations of a voice-only connection. Remote service tools can allow service provider staff to more effectively provide support information and advice when on-site visits are costly or impractical.

Nevertheless, it is important to recognize that remote servicing can also raise questions on the part of healthcare delivery organizations, patients, and government regulators as to how personal data accessed in the course of servicing is used and what safeguards exist to ensure that the data is protected from unauthorized access, use, and disclosure. Common concerns include that:

- Miscommunication between the service provider and the healthcare delivery organization could lead to access to the wrong device or network. Such administrative errors might occur more easily in remote servicing simply because conversations are not held face-to-face, and service provider staff are not physically shown the device to be serviced. This highlights the importance of standard operating procedures to verify that the device to be accessed is, in fact, the intended device.
- Information accessed or stored at the remote servicing center could be subject to unauthorized access or disclosure. This highlights the importance for the healthcare delivery organisation and remote service provider to agree on appropriate security policies and procedures.
- Device connections to the internet or local networks could expose these devices to malware or hacking attempts. This highlights the need for device security patches to be applied in a timely manner and for healthcare delivery organisations to have in place appropriate network intrusion detection and prevention technologies.

These are legitimate concerns, and both healthcare delivery organisations and service providers benefit from a frank and open dialogue on what privacy and security concerns exist and how these can be addressed.[4]

[4] Some medical device manufacturers use a standard reporting form to convey information to their customers about device security. The Manufacturer Disclosure Statement for Medical Device Security (MDS^2) is endorsed by the American College of Clinical Engineering (ACCE), ECRI (formerly the Emergency Care Research Institute), the

(Continued)

The benefits of remote servicing (and, conversely, the risks associated with inadequate maintenance) also, however, need to be clearly understood. Maintenance and support of today's highly sophisticated medical devices require a degree of specialized knowledge and training that can be costly for healthcare delivery organization IT Departments to maintain in-house. If healthcare facilities could not outsource the servicing of medical devices, they would either need to greatly expand the size of their IT staff in order to maintain all of the devices in a typical healthcare facility setting or maintenance would suffer. Thus, without the ability of service providers to remotely service devices, (i) there is a greater likelihood of device failures due to insufficient maintenance; (ii) there are likely to be longer equipment downtimes as on-site support visits will need to be scheduled when problems arise; (iii) service providers will have reduced ability to oversee the timely implementation of upgrades and patches, some of which may be critical to data security; and (iv) healthcare costs will increase as tasks that could be completed remotely will instead require on-site visits. Patient care unnecessarily suffers when important medical devices fail and become unavailable if such problems could have been mitigated or averted through remote servicing.

Like remote patient monitoring services, remote servicing typically can trigger a HIPAA business associate relationship between the service provider and the covered health care provider. Where such a relationship exists, a business associate agreement is required, and the service provider is subject to HIPAA regulations.

3. Connectivity of Medical Devices to PHRs and Online/Mobile Apps

As the connectivity of medical devices increases, so too does the availability of applications that enable patients to interpret medical device data and keep track of their health. Such applications are sometimes offered by the manufacturer of the equipment and other times by third parties. Such applications can empower patients to play a more active role in their own health care and help to reinforce behaviors that will lead to selected health goals. On the other hand, some medical device data require interpretation by a qualified clinician, and there is a risk in such cases of misdiagnosis or missed warning signals if health care professionals are not appropriately involved in interpreting device data.

As with remote patient monitoring and remote servicing of devices, security in this context is important. The FTC's Health Breach Notification Rule applies to vendors of applications intended for use by individuals in managing, sharing, and controlling their identifiable health information drawn from multiple sources (a "personal health record" or "PHR"), as well as entities that access information in a PHR or send information to a PHR. The Rule requires notification to affected individuals and the Commission whenever a breach of unsecured

(Continued)
National Electrical Manufacturers Association (NEMA), and the Healthcare Information and Management Systems Society (HIMSS).

identifiable health information occurs. The Rule creates a strong incentive for manufacturers of medical devices that connect to PHRs to build security into the design of their products.

_____

We appreciate your consideration of our comments. Please do not hesitate to contact us with any questions.

Sincerely,

Peter Blenkinsop
MDPC Secretariat and Legal Counsel

DC01/ 3152666.2