


# Privacy and Security Issues Surrounding the Protection of Data Generated by Continuous Glucose Monitors

Journal of Diabetes Science and Technology  
2017, Vol. 11(2) 216–219  
© 2017 Diabetes Technology Society  
Reprints and permissions:  
sagepub.com/journalsPermissions.nav  
DOI: 10.1177/1932296816681585  
journals.sagepub.com/home/dst  


**Katherine E. Britton, JD<sup>1</sup>**  
**and Jennifer D. Britton-Colonnese, MSN, FNP-BC, CDE, CDTC<sup>1</sup>**

## Abstract

Being able to track, analyze, and use data from continuous glucose monitors (CGMs) and through platforms and apps that communicate with CGMs helps achieve better outcomes and can advance the understanding of diabetes. The risks to patients' expectation of privacy are great, and their ability to control how their information is collected, stored, and used is virtually nonexistent. Patients' physical security is also at risk if adequate cybersecurity measures are not taken. Currently, data privacy and security protections are not robust enough to address the privacy and security risks and stymies the current and future benefits of CGM and the platforms and apps that communicate with them.

## Keywords

continuous glucose monitor, data privacy, data security, protected health information, personally identifiable information, HIPAA

Recent advances in technology revolutionize how patients and health care professionals (HCPs) understand and manage diabetes. Continuous glucose monitors (CGMs) and the platforms and applications (apps) that communicate with CGMs improve patient outcomes. CGMs generate a substantial amount of data by collecting interstitial glucose readings every 5 minutes, which lags behind but is an indicator of the patient's blood glucose (BG). These data are sensitive in nature and while the state and federal privacy and security laws would apply if the data were held by an HCP, the same data are not protected when in the hands of a CGM manufacturer. Who owns these and other data, how they are used, and how they are kept secure are open questions.

CGM, while obtained by a prescription, is a commercial product that is very different from those HCPs generally recommend. The current data privacy and security landscape contains regulatory gaps where adequate protections may not exist. This creates challenges in balancing increasing risks to privacy and security while encouraging patients to reap the benefits that CGMs present.

Privacy and security protections exist to encourage users in sharing their sensitive health data. A lack of trust may deter users from using CGMs, HCPs from prescribing them, and prevents patients and society from reaping the benefits. Classifying the data collected by CGMs as sensitive health data and not simply "personal information" and implementing privacy and security standards appropriate to sensitive information would go a long way in engendering trust.

## CGM Benefits

CGMs keep patients safe from harm from low blood sugars, known as hypoglycemia, by alerting them when their glucose has fallen below a threshold that the HCP has determined as unsafe. This alert can result in a patient confirming their low BG via glucometer, treating their hypoglycemia, and avoiding harm. CGM alerts are particularly important when a patient experiences a dangerous condition called hypoglycemia unawareness, where the patient's body is no longer able to experience the protective signs and symptoms of a low blood sugar, such as shakiness or sweating, which signals to a patient that they need to act to bring up their BG level. CGM technology can stymie harm from hypoglycemia.

Particularly for an insulin-dependent person with diabetes, CGMs can help enhance diabetes care. CGMs integrated with pump therapy tighten BG control. A clinical trial that showed that patients who used CGMs had an average blood sugar level reduction of 2 points.<sup>1</sup>

CGM data can be used and analyzed with the help of apps and platforms. For example, an insulin pump and CGM using various networking technology can send data to a

---

<sup>1</sup>Boston University Medical Center, Boston, MA, USA

## Corresponding Author:

Katherine E. Britton, JD, 1800 Main Street, 1802 Dallas, TX 75201, USA.  
Email: [Kebritton1@gmail.com](mailto:Kebritton1@gmail.com)

smartphone or computer using an app that links the pump and CGM sensor to the user's smartphone or computer. Users can see their information without removing the pump and allow HCPs to view their information. These data can be aggregated and analyzed to reveal trends, which can further our understanding of diabetes.

Medtronic's CGM (Medtronic Diabetes, Northridge, CA) along with IBM Watson Health's cognitive mobile app, Sugar.IQ with Watson (IBM Watson Health, Cambridge, MA) will use cognitive computing to provide patients and HCPs with insights such as uncovering important patterns and trends to predict hypoglycemia, to help users understand how their behavior affects their BG and other real-time and personalized insights to understand and manage diabetes.<sup>2</sup> As the app uncovers behaviors associated with glucose patterns, it will deliver personalized messages in real time to help users track food in a diary or therapy-related actions and events that can help users understand how specific actions and habits affect their BG.

## Privacy and Security Risks

There are privacy issues since CGM manufacturers and their corresponding apps and platforms store patients' health data and allow those data to be shared and analyzed. There are few specific guidelines as to how these issues should be addressed and little oversight in ensuring that adequate protections are in place. Companies are not required to provide users with notice of how their information is used, but many do so in their privacy policies. Specific opt-outs, meaningful choice, and control over data are nonexistent.

People with diabetes are faced with accepting how a CGM manufacturer and its concomitant platforms and apps gather, use, and share all kinds of their data, which may include "derived information" or forego using the product and its associated benefits. According to Dexcom's (San Diego, CA) privacy policy, Dexcom can gather information including IP address and other information regarding the user's computer, Internet service, the browser used, and the user's activities while using Dexcom Products and Services. Dexcom's privacy policy, for example, explains that the way it deidentifies personal information is by "removing information that could not identify the user" without specifically identifying how.<sup>3</sup> Dexcom, along with most privacy policies, disclose that so long as the data are not "personally identifiable" and meet a nebulous business need, the data can be used for any purpose. Privacy policies often disclose that they are subject to change without notice. What users or their HCPs expect of how data are safeguarded, what duties are theirs to perform, and what privacy risks exist may be a second or nonexistent thought and may be inconsistent with reality.

There ought to be stronger protection in the collection, storage, and distribution of sensitive data that a patient may not wish to be revealed as even deidentified information can

be reidentified and the amount and types of collectable information are overbroad.

The Future of Privacy Forum, a nonprofit organization that advances principled data practices in support of emerging technologies, recommends as a best practice that wearables and wellness apps provide users with enhanced notices that are clear, prominent, and conveniently located outside of a traditional privacy policy that specifies among other things the type of data collected, how they are collected, stored, used, secured, and disclosed, specific deidentification commitments, and users' options regarding access, correction, or deletion of covered their data.<sup>4</sup> This advice is voluntary on behalf of the company, but if they make certain promises including on how data will be gathered, used, and disclosed and not keep their promises, they could face enforcement by state and federal consumer protection agencies and breach of contract lawsuits that would deter them from going beyond their regulatory obligations.

In addition to privacy, security risks should be addressed. Security involves making sure that data are not disclosed inadvertently and in making sure that the physical device is not compromised. Depending on the level of encryption, transmitting data encrypted reduces the risk that personal information would fall into the wrong hands. Should a CGM or insulin pump have inadequate security, it can be hacked and result in patient harm. In late September 2016, a security flaw was discovered for an insulin pump and CGM, which could be remotely programmed over a specific unencrypted radio frequency.<sup>5</sup> If a malefactor identified that frequency, the individual could program and command the pump to supply insulin to an unsuspecting patient victim.

HCPs have a duty to "do no harm" and should make patients aware of technologies, products, and services that will improve their outcomes. In the current regulatory landscape, HCPs are in a difficult position where without adequate privacy and security protections, it is difficult to unconditionally recommend CGM. HCPs are counselors and specialists in science and medicine, not technologists or legal experts. As such, it is difficult for HCPs to recommend products without understanding and communicating the full ramifications to a patient's privacy and security when the full risks are inadequately addressed.

## HIPAA

The Department of Health and Human Services (HHS) recognizes the need for stricter data privacy protection requirements and identified regulatory gaps for Congress to fill for entities, whose products and services, including CGM are not covered by HIPAA.<sup>6</sup>

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security rules protect protected health information (PHI), which is generally a patient's health information or treatment as covered by the Act and collected by covered entities, such as HCPs, insurers and certain

business associates. Where a patient's health information is deidentified, it is not considered PHI and is not covered by HIPAA. HIPAA is aggressively enforced by HHS and provides some of the strongest data privacy and security protections for patients. HIPAA's Privacy Rule requires covered entities or business associates that maintain or transmit PHI on behalf of a covered entity to provide appropriate safeguards to protect covered information. In addition, the Privacy Rule sets limits and conditions on how such information may be used and disclosed without customer authorization. The Privacy Rule gives patients rights over their information, such as the right to examine and obtain a copy of their health records as well as to direct the covered entity to transmit their health information to a person or entity of their choosing, such as via a mobile health app. Other than providing their customers with these printed rights voluntarily in a privacy policy, CGM manufacturers are not legally obligated to give users the rights that they would have under HIPAA's privacy rule even though HIPAA covers similarly sensitive health information.

HIPAA's Privacy Rule provides 2 standards for deidentification of what would otherwise be PHI if tied to an identifiable patient. These are (1) the Safe Harbor Standard and (2) the Statistical Standard. The Safe Harbor Standard requires the deidentification of 18 specific data elements that could uniquely identify an individual. While many CGM manufacturers disclose in their privacy policies that they may deidentify certain information, they are not legally obligated to meet HIPAA's Safe Harbor standard for deidentifying data. Many CGM manufacturers disclose in their privacy policies that they may use deidentified information differently than personally identifiable information. Without transparency on the deidentifying methods, there is no indication that the deidentifying methods used are effective.

The HIPAA Security Rule specifies a series of administrative, physical, and technological safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of electronic PHI. The HIPAA Breach Notification Rule requires covered entities to notify consumers, the HHS Secretary, and the media following a breach of unsecured PHI and requires business associates to notify the HIPAA covered entity in the event of a breach.

There has been little regulation over data that HIPAA would otherwise protect if held by a covered entity. HHS made clear that it does recognize a need for legislation to fill the regulatory gap where HIPAA does not apply and the privacy and security risks are not adequately addressed.

The Federal Trade Commission (FTC) and state enforcement agencies might have regulatory authority over entities handling patients' health information. The Food and Drug Administration (FDA) provides cybersecurity guidance to such companies. Privacy policies may disclose that the company follows requirements under "applicable law," however it is not clear which laws, if any, are being followed. Where certain laws apply, they may not be adequately enforced.

## **FTC**

Where an entity lets users manage their medications or lets them upload readings from a CGM, the FTC's Health Breach Notification Rule applies. This rule requires affected consumers, the FTC, and the media following a breach of unsecured personal health information be notified of the breach. Entities that provide service to a personal health records provider or related entity must notify those entities following a breach.

Section 5 of the FTC Act prohibits deceptive or unfair acts or practices. The entity must reasonably protect customers' privacy and ensure that statements such as those in a privacy policy are truthful, substantiated, and not misleading. The FTC has been aggressive in the privacy and security space and advocates for incorporating privacy and security principles in every state of the product's life cycle and advocates for notice, choice, access, accuracy, data minimization, security, and accountability.

## **FDA**

If an app is intended to be used in diagnosing disease or other conditions, or used to cure, mitigate, treat or prevent disease, the Food and Drug Administration (FDA) has authority to enforce the Federal Food, Drug, and Cosmetic Act (FD&C Act). The primary concern of the FDA is over safety of devices, and accuracy of data provided. Even where the FD&C Act applies, the FDA will not enforce compliance with the Act's regulatory requirements in cases where there is a "minimal risk" posed to the user. The FDA may not enforce the Act against certain platforms or products that only help users self-manage their disease without providing specific treatment suggestions or those that provide simple tools to organize, log, track, or trend their events or measurements, such as BG, insulin intake, and diet and share this information with their HCP as part of a disease-management plan.

For an app that uses an attachment to mobile platforms to measure BG levels, however, the FDA considers it a "mobile medical app" and does intend to apply its regulatory oversight. For example, an app that uses a mobile platform for medical device functions such as an attachment of a BG strip reader to a mobile platform to function as a glucose meter is a mobile medical app. Such an app will undergo FDA review and be evaluated according to the same regulatory standards and risk-based approach that the FDA applies to other medical devices. The FDA classifies medical devices into 3 categories based on the risk the devices pose to consumers, intended use, and indications for use. A glucose test system used to test BG over the counter will be evaluated for safety and effectiveness through a premarket submission process before it will be allowed to be sold to the public.

On January 22, 2016, the FDA issued draft guidance for industry and FDA staff on post market management of

cybersecurity in medical devices.<sup>7</sup> This guidance contains nonbinding recommendations and was intended to address the cybersecurity concerns present in networked medical devices that may be vulnerable to cybersecurity threats. The FDA emphasized that security vulnerabilities present risks to the safety and effectiveness of medical devices. Addressing those risks requires building security into every stage of the product's life cycle and performing continual maintenance to ensure an adequate degree of protection against such exploits to proactively addressing the cybersecurity risks. Specifically, manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.

## Conclusion

With the current regulatory landscape surrounding CGM, patient's health data and security may be compromised in ways that full ramifications are unknown. The regulatory landscape is such that the same information protected by HIPAA is not protected because data generated by CGM is not held by a covered entity. Similar robust privacy and security protections as HIPAA provides should apply where sensitive health information is collected, stored, and used. A CGM is a consumer product on the market that requires HCP advice, interpretation, and a prescription. Both patients and HCPs must be aware of the not-so-obvious risks with CGM and similar technologies that open the door for privacy violations. Until tighter privacy and security protections are established, it will be for patients to make the best decisions for themselves to the level of risk for privacy and security risk that they are able to tolerate.

## Abbreviations

apps, applications; BG, blood glucose; CGM, continuous glucose monitor; FDA, Food and Drug Administration; FD&C Act, Federal Food, Drug, and Cosmetic Act; FTC, Federal Trade Commission; HCP, health care professional; HHS, Department of Health and Human Services; HIPAA, Health Insurance Portability and Accountability Act of 1996; PHI, protected health information.

## Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## References

1. FTC Staff Report. Internet of things: privacy & security in a connected world 20. 2015. Available at: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.
2. Bruls A. First live experience of Sugar.IQ with Watson for people with diabetes. September 26, 2016. Medtronic Integrated Care Blog. Available at: <http://www.medtronicdiabetes.com/blog/first-live-experience-of-sugar-iq-with-watson-for-people-with-diabetes/>. Accessed October 15, 2016.
3. Dexcom Privacy Policy. September 26, 2016. Available at: <https://www.dexcom.com/dexcom-privacy-policy-sep-16>. Accessed October 15, 2016.
4. Future of Privacy Forum. Best practices for consumer wearables and wellness apps and devices. August 17, 2016. Available at: <https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf>.
5. JJ Warns Insulin Pump Vulnerable to Cyber Hacking OneTouch Ping uses unencrypted radio signal. *Wall Street Journal*. October 4, 2016. Available at: <http://www.wsj.com/articles/j-j-warns-insulin-pump-vulnerable-to-cyber-hacking-1475610989>.
6. HHS Report. Examining oversight of the privacy & security of health data collected by entities not regulated by HIPAA. 2016. Available at: [https://www.healthit.gov/sites/default/files/non-covered\\_entities\\_report\\_june\\_17\\_2016.pdf](https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf).
7. FDA Draft guidance for industry and Food and Drug Administration staff. Postmarket management of cybersecurity in medical devices. Available at: <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>.