iOn HEALING™ Mobile App
HIPAA Position Paper December 2021

The iOn HEALING™ Mobile App from 3M Medical Solutions (3M) offers a suite of tools designed to improve customer support, streamline business processes, and facilitate more efficient and effective communication between clinicians and 3M representatives. The iOn HEALING™ Mobile App features the following main functions that may involve the exchange of Protected Health Information (PHI):

- Connect & Consult: Allows clinicians to connect directly with their 3M representative to share wound information and discuss potential treatment options for their own clinical purposes. This function uses two initials to identify the patient and may include de-identified photos. A conversation between a clinician and a medical device manufacturer, in support of patient care, is allowed per HHS FAQ 490 (see later reference) for treatment, payment or operations of the Covered Entity.

- Place Orders: Allows clinicians to place orders for V.A.C.® Therapy and V.A.C.® Dressings and Supplies with 3M, which is acting as a Covered Entity and provider of therapy to the patient.

- Manage Outcomes: Allows clinicians to share their patient's wound healing information with 3M, which is acting as a Covered Entity in documenting medical necessity for medical equipment reimbursement purposes.

The iOn HEALING™ App is designed to be HIPAA - and HITECH-compliant and helps control risks associated with the sharing of PHI by providing the following security features:

- Registration process required for new users to create an account
- Access secured via enforcement of complex passwords on a per-use basis
- Data in motion is transferred via secure 256-bit encryption
- Data is stored under 256-bit encryption on secure servers
- PHI is not stored on the mobile device itself
- Users are automatically logged out after 30 minutes of inactivity

HIPAA and HITECH Act

HIPAA allows for the exchange of PHI among Covered Entities for the purposes of treatment, payment, and healthcare operations. Specifically, the HIPAA Privacy Rule permits a health care provider to disclose PHI for its own treatment purposes or for the treatment purposes of another health care provider. The patient's authorization is not required for treatment-related disclosures of PHI if it meets this purpose. The exchange of PHI among clinicians and 3M representatives through the mobile application in connection with the Connect & Consult function is directly related to the treatment of the patient and, thus, is permitted under HIPAA. Typically, the clinician will disclose PHI for treatment purposes to determine the appropriateness of certain products for the patient's wound and to subsequently order the correct product. When PHI is disclosed to 3M through the Place Orders and Manage Outcomes functions, both the health care provider and 3M are considered to be Covered Entities. 3M will use the shared PHI to facilitate its own treatment and payment functions as it delivers medical equipment services to the patient.

The Department of Health and Human Services ("HHS") has developed FAQ 490[1] regarding the permissible disclosure of PHI to a medical device company representative, which is excerpted in part below:

> Question:
>
> When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative?
>
> Answer:
>
> In general, and as explained below, the Privacy Rule permits a covered health care provider (covered provider), without the individual's written authorization, to disclose protected health information to a medical device company representative (medical device company) for the covered provider's own treatment, payment, or health care operation purposes (45 CFR 164.506(c)(1)), or for the treatment or payment purposes of a medical device company that is also a health care provider (45 CFR 164.506(c)(2), (3)). Additionally, the public health

[1] Available at https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html.

> provisions of the Privacy Rule permit a covered provider to make disclosures, without an authorization, to a medical device company or other person that is subject to the jurisdiction of the Food and Drug Administration (FDA) for activities related to the quality, safety, or effectiveness of an FDA- regulated product or activity for which the person has responsibility. See 45 CFR 164.512 (b)(1)(iii) and the frequently asked questions on public health disclosures for more information.
>
> In certain situations, a covered health care provider may disclose protected health information to a medical device company without an individual's written authorization only if the medical device company is a health care provider as defined by the Rule. A medical device company meets the Privacy Rule's definition of "health care provider" if it furnishes, bills, or is paid for "health care" in the normal course of business. "Health care" under the Rule means care, services or supplies related to the health of an individual. Thus, a device manufacturer is a health care provider under the Privacy Rule if it needs protected health information to counsel a surgeon on or determine the appropriate size or type of prosthesis for the surgeon to use during a patient's surgery, or otherwise assists the doctor in adjusting a device for a particular patient. Similarly, when a device company needs protected health information to provide support and guidance to a patient, or to a doctor with respect to a particular patient, regarding the proper use or insertion of the device, it is providing "health care" and, therefore, is a health care provider when engaged in these services. See 65 FR 82569. By contrast, a medical device company is not providing "health care" if it simply sells its appropriately labeled products to another entity for that entity to use or dispense to individuals.

This FAQ confirms that 3M is a health care provider because it provides support and guidance to both patients and clinicians with respect to 3M products. The FAQ also confirms that the HIPAA Privacy Rule permits clinicians to disclose PHI to 3M without the patient's written authorization.

HIPAA and HITECH provide national minimum standards to protect an individual's PHI. HIPAA originally was created to streamline healthcare processes and reduce costs by standardizing certain common healthcare transactions while protecting the

security and privacy of individuals' PHI. The HITECH Act expanded on the privacy and security requirements of HIPAA by further describing necessary controls for electronic health records. 3M has designed its information systems and applications to be compliant with HIPAA and HITECH privacy and security standards, including reasonable administrative, technical, and physical safeguards. Nevertheless, each user of the iOn HEALING™ Mobile App is solely responsible for its individual compliance with all applicable laws, including HIPAA and HITECH, and any applicable policies and procedures of its employer.

The End User License Agreement for the iOn HEALING™ Mobile App contains additional information related to the security of PHI. Any questions related to privacy controls may be forwarded to HCBGDataCompliance@mmm.com.

Disclaimer

This document is not intended to constitute legal advice. You are advised to seek the advice of legal counsel regarding compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and other laws that may be applicable to you and your business. 3M and its affiliated entities make no representations or warranties that your use of 3M services will assure compliance with applicable laws including, but not limited to, HIPAA and HITECH.