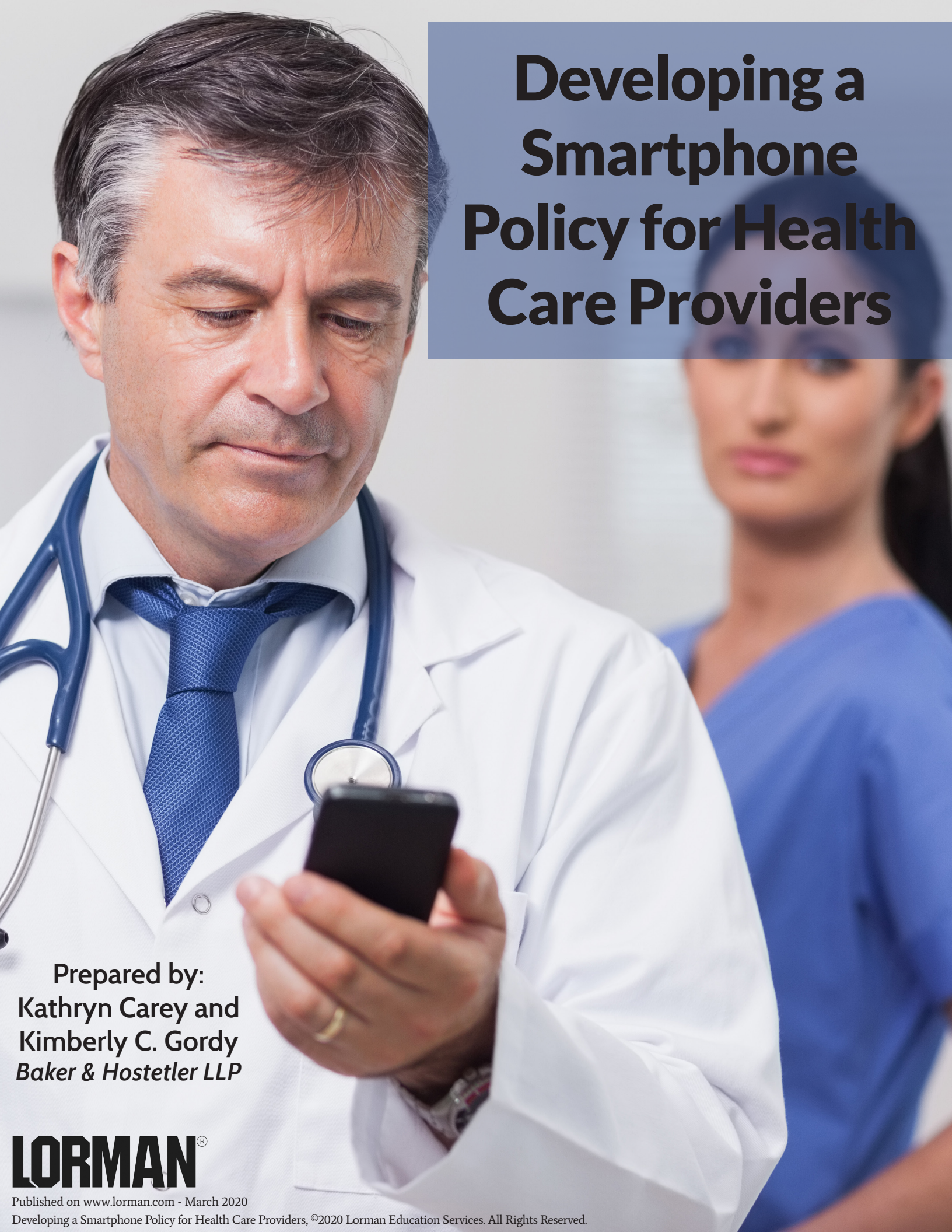

Developing a Smartphone Policy for Health Care Providers

Prepared by:
Kathryn Carey and
Kimberly C. Gordy
Baker & Hostetler LLP

LORMAN®

Published on www.lorman.com - March 2020

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 110+ live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 3,800 courses available
- ☑ **Videos** - More than 1,900 available
- ☑ **Slide Decks** - More than 3,000 available
- ☑ **White Papers** - More than 1,900 available
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Developing a Smartphone Policy for Health Care Providers

HIPAA – The Health Insurance Portability and Accountability Act of 1996

HIPAA sets forth national standards for electronic health care transactions and established federal privacy protections for health information.

President Obama signed the HITECH Act, as part of the American Recovery and Reinvestment Act, which furthered HIPAA in addressing privacy and security of health information and introduced the Breach Notification Rule. It also gave the Office for Civil Rights greater enforcement powers.

Privacy Rule Implications

Privacy Rule establishes national standards to protect individuals' medical records and other personal information. It requires appropriate safeguards to protect the privacy of personal health information (PHI).

Nothing in the Privacy Rule specifically addresses smartphones, but there are provisions we need to be aware of.

Security Rule Implication

The Security Rule establishes security standards for protecting certain PHI held or transmitted in electronic form. It works with the Privacy Rule by addressing the technical and non-technical safeguards must put in place to secure electronic PHI.

Addressable v. Required

Encryption is an addressable item under HIPAA. "Addressable" items have to be implemented unless:

There is an alternative measure that accomplishes the same purpose or it can be demonstrated that the secured measure is not necessary to protect PHI.

Texting & Healthcare

There are many risks to having smartphones in the healthcare environment (lost devices; stolen devices; etc.) but also many benefits (increased patient satisfaction; better communication between providers and patients).

In the end, there are two options to texting in the workplace: De-Identification and Texting Apps.

- Covered Entities vs. Business Associates under HIPAA – HIPAA applies to Covered Entities and Business Associates. Web developers may be considered Business Associates and are required to comply with HIPAA.
- A Business Associate is someone who creates, maintains, receives, transmits PHI on behalf of a covered entity.
- If you are only offering services directly to – and collecting information for/on behalf of consumers and not a provider, health plan or health care clearinghouse, you are not likely subject to HIPAA.

De-identification of PHI

- True de-identification of PHI based on OCR Guidance
- Would initials be enough to prevent re-identification? MRN?
- It's not de-identified PHI but it could, potentially, be low probability under the 4-factor risk assessment.

- Policies can direct staff to de-identify data when sending it over text message or email from a smartphone.
- The challenge to this approach is enforcement with your staff.
- Regulators will want to see extensive training on de-identifying or alternative ways to reference patients i.e. MRN (assuming it cannot be used outside of the facility).

Regulators and Policies – Smartphones in Healthcare

Guidance from the Experts

- Health & Human Services Office for Civil Rights – OCR enforcement has previously addressed lost laptops (CardioNet Settlement in April 2017). As smartphones continue to evolve, they become more and more like hand held computers, with an immense amount of data.
- National Cybersecurity Center of Excellence – In 2015, issued Mobile Device Security: Cloud and Hybrid Builds, to provide guidance on mobile device management solutions.
- In February 2016, the OCR issued a crosswalk to provide guidance to organizations on how to apply

Asset Management

Risk Analysis and Risk Management Plans

Training is an important piece, regardless of whatever approach you take to smartphones in the workplace. OCR expects to see extensive training with staff on proper use of smartphones.

Data Security

Protective Technology

Policies and training need to recognize that smartphones can be used beyond just texting.

- Smartphones have the capabilities of filming video and recording sound in the healthcare setting. This needs to be addressed.

Mobile Apps

"App" is short for "application." It references any software that can be installed onto a device. Although most common on mobile devices, apps can be installed on tablets and computers.

Benefits: An app store provides a one-stop shop. By purchasing through an app store, the download and installation are instantaneous.

Patients are likely to have increased compliance and improved communication with providers

Employees, especially the younger generations, are more likely to meet deadlines and provide accurate documentation of events if it can be done on a mobile device

Downsides: The app store can discontinue or remove the software at any time. There can be a lack of transparency regarding the app developer and their experience with HIPAA matters.

HIPAA applies to some, but not all apps:

Apps that provide patient management services that involve creating, receiving, maintaining, and transmitting PHI on behalf of the provider create a Covered Entity/Business Associate Relationship. This type of app is subject to the HIPAA Rules.

Direct-to-Consumer Apps: Patient/Consumer apps that allow patients to input their own information and share the information with their healthcare provider are not always subject to HIPAA. The app is transmitting data on behalf of the consumer to and from the provider; therefore the App and the Provider do not need a BAA.

Crafting a Smartphone Policy

Banning smartphones in the workplace won't eliminate smartphones in the workplace. It will mean that employees will sneak their smartphones.

Benefits of creating a policy: Employees are permitted to have smartphones and the practice is able to implement security standards and guidelines.

Policy Content

A policy should state when smartphone use is permitted - this considers the nature, pace, and needs of practice.

Call should be permitted during breaks or lunch hour.

Consider extending this to "at anytime provided there is no disruption to patient care or interference with job duties or performance." This language is better suited for salaried employees who take breaks or lunch at unscheduled intervals.

Employees should be able to keep smartphones on their person.

Employees should have access to personal content during breaks. However, the WIFI use and access to certain websites (Facebook, Gmail) is an employer decision. Employees may use their personal data or go offsite if these websites are not permitted.

A policy should activities that are prohibited under all circumstances

Photography or livestreaming of patients and staff should be prohibited under all circumstances

If the nature of the practice necessitates photos, the photo should be taken within a secure app or platform so it is not stored in personal cloud-based storage

There is no reason for livestreaming outside of the telemedicine context.

Any access to pornography, discriminatory, or other inappropriate content is prohibited

Employers may want to extend policy language to prohibit posting on social media during the workday.

Employers may include language that puts employees on notice that posting of discriminatory content or hate speech may result in loss of employment, even if posting is on personal account and outside of work hours.

Bandwidth and WIFI do not support streaming or downloading: although a practice-based decision, this is generally a good recommendation to avoid downloading from websites that may be harmful.

A policy should require technical safeguards

Smartphones should require multifactor authentication to reach work related content

The policy should specify which workforce roles receive remote access

The policy should include password management and regular passcode resets

Auto-logging should be enabled on email

Consider disallowing removable devices

Technical safeguards are important because:

10% of all incidents result from lost or stolen devices

30% of incidents result from phishing

A smartphone policy should align with your social media policy

It's becoming a trend for workplaces to request employee social media account access. Before requiring employees to turn over social media account information, verify there are no applicable state laws or union agreements

Set additional guidelines regarding "friending" of patients, and educate employees on ways to decline sharing personal information with patients

Smartphone policies for patient-use

Provide guidelines to patients on smartphone use, including signage requesting phones be put away

Offer filming or photography services (ex. Labor and Deliver)

Include information on filming policies on website

Implement a "guest WIFI" network to control steaming capacity