ALSTON & BIRD

WWW.ALSTON.COM

Health Care / Cybersecurity Preparedness & Response ADVISORY ■

MARCH 16, 2020

COVID-19 and HIPAA: Privacy, Security, and Breach Response During a Global Pandemic

by Dawnmarie Matlock, Angie Burnette, Kim Peretti, Jon Knight

By now, almost everyone knows of the coronavirus (COVID-19) pandemic. But this type of international crisis is not just a global health issue: it is also a security issue. Scammers and cyber threat actors have always followed the headlines, using the public's heightened fear and desire for information or solutions as leverage to gain access to systems, data, and money. The current pandemic is no different.

The Food and Drug Administration (FDA) and the Federal Trade Commission (FTC) have already seen a significant uptick in the number of complaints relating to phony COVID-19 cures, requests for "donations" from fake charities, and spam or phishing emails claiming to be from government sources with official information relating to the outbreak. And the cyber research and security company Malwarebytes recently discovered a website purporting to be a map showing COVID-19 cases on a global scale. This map was almost identical to the one published by Johns Hopkins University except it contained a hidden code that could steal usernames, passwords, credit card numbers and other data stored in the user's browser. In other words, COVID-19 poses a real security threat.

Just as the doctors, nurses, and other health care providers are not immune from COVID-19, entities and business associates covered by the Health Insurance Portability and Accountability Act (HIPAA) are not immune to this threat to data privacy and security. For example, the U.S. Office for Civil Rights (OCR) emphasized in a recent bulletin that the COVID-19 outbreak does not relieve HIPAA-covered entities and business associates of their obligations under the HIPAA Privacy Rule. There is also no indication that the HIPAA Security Rule has been or will be suspended during this time. Given this state of affairs, HIPAA-covered entities and business associates should consider the following proactive steps.

Keep Practicing Good Cybersecurity Hygiene

This may seem obvious, but it is a principle that cannot be taken for granted during a time of crisis. An environment of fear and distraction means personnel are more likely to forget to use good cybersecurity practice. But warning them now may help with security awareness during an outbreak.

Companies should consider reminding all employees of the following basic security principles:

- Be careful opening attachments and links from distrusted or unknown sources. Phishing or other malicious emails can easily be disguised as alerts about COVID-19.
- Try to only use trusted sources, for example the CDC's official COVID-19 website, for receiving up-to-date information about the outbreak.
- Never respond to emails or phone calls asking for personal or financial information, usernames, or passwords.
- Be careful making donations and reject any request for donations in cash, by gift card, or by wiring money.
- Remind the increased numbers of employees who may be working remotely to use good security for any remote connections, such as VPNs, especially if they are accessing protected health information.

Review and Update Business Continuity and Disaster Recovery Plans

The COVID-19 outbreak is unlikely to directly impact infrastructures holding electronic health records or patient information. However, it is possible that a severe outbreak will impact the availability of personnel assigned to monitor or use those infrastructures. This is an opportunity to review business continuity and disaster recovery plans to ensure they appropriately cover scenarios that might arise if multiple key personnel are ill, absent, or incapacitated. Similarly, if you use managed security service providers or other security vendors for critical parts of your program, you can take this opportunity to verify that those vendors have similar plans and redundancies. And if a decision is made to quickly bring in additional staff or contractors, be sure to use appropriate HIPAA-compliant business associate agreements as needed. Ultimately, this is the perfect opportunity to ensure that all key players have recently reviewed these plans and engaged in tabletop simulations relating to business continuity.

Maintain Good Access Controls to Electronic Health Records and Patient Records

Every few hours it seems that news breaks of some well-known person—a movie star, basketball player, government leader—becoming infected with the coronavirus. Dozens more are anonymous individuals identified as "having tested positive" for the coronavirus. In this climate, it is natural for those with access to electronic health records and patient records to be curious about who may have contracted COVID-19 within their communities. However, any inappropriate access to health records places the HIPAA-covered entity or business associate at risk of violating the HIPAA Privacy and Security Rules. To reduce this risk, consider:

- Reminding employees of the difference between appropriate and inappropriate access.
- Applying extra protections for COVID-19 health records such as a protocol that automatically notifies certain personnel when the health record is accessed.
- Increasing the frequency of reviewing audit logs for inappropriate access.
- Taking appropriate corrective action if inappropriate access occurs, including imposing sanctions as appropriate.

Remain Prepared to Comply with Breach Notification Rules and OCR Investigations

The HIPAA Security Rule remains in full effect and yet many businesses are encouraging (or requiring) employees to work remotely or cancel work travel as part of the response to COVID-19. But suddenly expanding the number of employees working remotely comes with increased cybersecurity and information technology risks. Cybercriminals will have a target-rich environment since more company devices (and company data) will likely be used outside

the protections of the company infrastructure. It will also be easier for devices to be lost, stolen, or compromised, particularly if employees are not familiar with company policies on how to securely work from home. A HIPAA-covered entity or business associate should remain alert to responding to, investigating, and reporting potential breaches, even if key personnel are absent or ill due to COVID-19.

Consider taking the following steps:

- Reviewing incident response plans and revising if needed to include backup personnel if key personnel such as the HIPAA privacy officer and/or the HIPAA security officer are incapacitated or unavailable.
- Having backup personnel review the incident-response process. For example, they may need to know who to contact, such as outside legal counsel and forensic consultants, when analyzing a potential breach. They may also need to be aware of prior HIPAA notice letters sent by the company and where notice templates, if any, are located. And they may need to be familiar with the full breach notification process under HIPAA, including for reporting a breach to the media and the U.S. Department of Health and Human Services.
- Cross-training appropriate personnel in both the HIPAA Privacy and Security Rules so that the organization can respond to an OCR investigation even if individuals are sick or incapacitated. This could include making sure that all key and backup personnel know the location of the core documents and policies traditionally sought as part of an OCR investigation.

You can subscribe to future ***Health Care*** and ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Jonathan Knight
202.239.3270
jon.knight@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333