CARLTON FIELDS

10 Steps for Responding to a Telehealth Data Breach

HEALTH CARE | CYBERSECURITY AND PRIVACY | APRIL 30, 2020

Patricia S. Calhoun

Patricia M. Carreiro

Thus far, telehealth breaches have been exceedingly rare, but as telehealth is increasingly used, telehealth data breaches and similar incidents may become more commonplace. Here are 10 steps for responding to a telehealth data breach or similar incident:

1. **Stop the Leak**

Whatever the data compromise, end it. Shut down the access rights being abused; take down the mistakenly posted records. However, any action taken to stop the leak should be undertaken with an understanding of how that action could affect document preservation.

2. **Perform an Initial Assessment**

Ask: What type of information was exposed? Does it constitute a "breach" under relevant state law definitions and/or HIPAA?

If your incident involves unencrypted protected health information, under HIPAA, it is presumptively a "breach" unless your risk assessment demonstrates a low probability that the protected health information has been compromised or an exception applies.

Make sure your risk assessment considers the nature and extent of the information involved, who the information was used by or disclosed to, whether it was actually acquired or viewed, and the extent of mitigation.

For HIPAA purposes, some things are, by definition, not a "breach":

- Disclosures that do not involve unsecured protected health information (if the information was unusable by unauthorized persons, its exposure is not a "breach");
- Unintentional, good faith acquisition, access, or use by a workforce member or person under the authority of a covered entity or business associate within the scope of their authority;
- Inadvertent disclosure by someone authorized to access the information to another person authorized to access the information; and
- Disclosure to someone for whom there is a good faith belief could not retain the information.

3. **Follow Your Incident Response Plan**

As part of its preparation for a breach or similar incident, an organization should develop and practice with its incident response plan. Then, when a breach or incident occurs, the plan can serve as the organization's playbook with key action items, such as:

- Notifying your privacy and security officer;
- Gathering your incident response team;
- Retaining counsel;
- Notifying your insurance carrier; and
- Putting a litigation hold in place.

4. **Investigate**

Counsel should retain your forensic firm to preserve privilege and gather a full understanding of the breach, including:

- Its cause;
- What information, systems, or devices were, or may have been, disclosed or otherwise affected; and
- How, and when, the compromise was discovered.

5. **Comply with HIPAA and State Breach Notification Requirements**

- Determine whom you will notify (law enforcement, regulators, the media, consumers, etc.). The law provides stringent timing requirements for many of these notices. Work with counsel who has the experience and contacts to get this done efficiently and correctly.
- For business associates, this will require reporting to the covered entity whose information was compromised.

6. **Review and Comply With Relevant Contracts**

Businesses and their data are woven together by contracts, most of which now include provisions regarding cybersecurity and data incidents. Make sure you review implicated contracts and comply with them. For example, business associate agreements may include a provision requiring the business associate to report the incident to the covered entity, to other business associates, or possibly even to individuals affected by the breach.

7. **Mitigate Damages**

Act to reduce the harm to the individuals impacted by the breach and your business. Minimize the damages consumers may suffer and your own reputational harm and lost business (often one of the largest costs of a data breach) by:

- Preparing a communication plan with affected individuals where they can receive helpful information, including contact information for key contacts, like law enforcement, the state identity theft hotline, and the FTC;
- Providing credit monitoring for affected individuals if appropriate given the nature of the breach or incident (this may not make sense in every case);
- Using disciplinary policies as appropriate to address employees whose conduct failed to comply with applicable guidelines; and
- Consider terminating any relationship that caused the breach.

8. **Document Your Efforts, but Be Careful What Evidence You Create**

It is important to document your efforts and response to any data incident: what you learn, when, the decisions you make, and the basis for those decisions. When doing so, however, consider the discoverability of those materials in any future enforcement proceeding, document production, or trial. That means being careful about the evidence you create and doing everything possible to maximize the protection of the attorney-client privilege (see immediate next step).

9. **Preserve Privilege**

Work with counsel to protect privilege at every step of the way. As noted above, counsel should retain the forensic firm and any other vendors needed to investigate and respond to the incident.

10. **Plan for the Next One**

Once you have contained the current incident, it is time to reflect and plan for the next one.

- Look at what worked and did not, and adjust your data incident response plan and other policies accordingly.
- Consider what you can do to strengthen your cybersecurity and privacy practices. Is it time for another employee training? Does your incident response plan need adjustment?
- Once you implement changes, test them.