Vendor Payment Disputes and Access to Stored Patient Data

Dental practices will feel the impacts of the COVID-19 pandemic on many levels and for quite some time. This resource is intended to provide guidance in the event you experience disputes with vendors or experience difficulties accessing stored patient data.

What happens if my software company stops accepting new PHI because we're in a payment dispute? Or what if something else happens that might threaten access to our PHI?

Much is unknown about the potential impacts of the COVID-19 pandemic. Possible scenarios include: a business associate unable to fulfill the terms of its agreement with the dental practice; a business associate able to maintain existing PHI as required but unable to accept any new PHI; or threats to PHI, including cyberattackers, such as ransomware attackers who try to capitalize on the pandemic by tricking people into clicking on harmful links or attachments in phishing emails.

Dental practices can help protect the availability of PHI in these types of situations by paying attention to these HIPAA Security Rule requirements:

- **Risk Analysis.** Update the practice's HIPAA Security Risk Analysis by adding any risks that were newly identified as a result of the COVID-19 pandemic. Remember that any risk analysis must include threats to the availability of PHI, as well as to the confidentiality and integrity of PHI.
- **Contingency Plan.** Review the practice's HIPAA Security contingency plan policies and procedures. Determine whether anything should be modified in response to new information identified through the risk analysis. For example, a practice may decide to update its contingency plan to include policies and procedures for implementing a paper-based recordkeeping in emergency situations.
- **Data back-up.** HIPAA requires a covered dental practice to establish and implement procedures to create and maintain retrievable exact copies of electronic PHI. Properly encrypting the backup can help ensure confidentiality and would likely be required by HIPAA. Restoring PHI from backup – for example, in the event of a ransomware attack – might help a dental practice recover from a cyberattack or loss of service.

Can my software company cut off access to our patient information if our payment is late or if we have a payment dispute?

A business associate, such as a software vendor, may not block or terminate a covered dental practice's access to the protected health information (PHI) that the business associate maintains for or on behalf of the dental practice because of a payment dispute.

Nevertheless, under the Health Insurance Portability and Accountability Act (HIPAA), dental practices are responsible for ensuring the availability of their own PHI. For example, a dental practice that signs a business associate agreement that prevents the dental practice from ensuring the availability of their PHI is not in compliance with HIPAA.

- From HHS: May a business associate of a HIPAA covered entity block or terminate access by the covered entity to the protected health information (PHI) maintained by the business associate for or on behalf of the covered entity?