

## Report on Patient Privacy Volume 21, Number 3, March 11, 2021 Select Provisions of Subcontractor Agreement (Sample)

---

Below are the sample clauses that might be different or should be specifically considered when a HIPAA business associate (BA) is imposing obligations on subcontractors who may also access a covered entity's (CE's) protected health information when performing services for the BA.<sup>[1]</sup>

### **ARTICLE X: SECURITY INCIDENTS**

- A. Reporting. Subcontractor will report to BA any confirmed or suspected Security Incident involving CE Confidential Information immediately upon discovery, both orally and in writing, but in no event more than twenty-four (24) hours after Subcontractor reasonably believes a Security Incident has or may have occurred. Subcontractor's report will identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Confidential Information accessed, used or disclosed, (iii) the person(s) who accessed, used, disclosed and/or received Confidential Information (if known), (iv) what Subcontractor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action Subcontractor has taken or will take to prevent future unauthorized access, use or disclosure. Subcontractor will provide such other information, including a written report, as requested by the BA or CE. In the event of a suspected Security Incident, Subcontractor will keep BA informed regularly of the progress of its investigation until the uncertainty is resolved. To the extent that Subcontractor cannot assemble the required information within the required timeframe, Subcontractor will provide to The BA (or CE if requested) the information in Subcontractor's possession, supplement as additional information becomes available, and in any event supply all required information to BA (or CE if requested) within five (5) days of the date on which Subcontractor became aware of the actual or potential Security Incident.
- B. Coordination of Security Incident Response Activities: Subcontractor will fully cooperate with BA's and CE's investigation of any Security Incident involving BA, CE and/or the Services, including without limitation making witnesses and documents available immediately upon BA's or CE's reporting of the Security Incident. Subcontractor's full cooperation will include but not be limited to Subcontractor:
1. Immediately preserving any potential forensic evidence relating to the Security Incident, and remediating the Security Incident as quickly as circumstances permit
  2. Promptly (within 2 business days) designating a contact person to whom BA or CE will direct inquiries, and who will communicate Subcontractor responses to BA or CE inquiries;
  3. As rapidly as circumstances permit, applying appropriate resources to remedy the Security Incident condition, investigate, document, restore BA service(s) as directed by BA, and undertake appropriate response activities;
  4. Providing status reports to BA on Security Incident response activities, either on a daily basis or a frequency approved by BA;
  5. Coordinating all media, law enforcement, or other notifications related to the Security Incident with BA and CE in advance of such notification(s), unless expressly prohibited by law; and

6. Ensuring that knowledgeable Subcontractor staff is available on short notice, if needed, to participate in CE or BA-initiated meetings and/or conference calls regarding the Security Incident.
- C. Grounds for Termination. Any Security Incident shall be grounds for immediate termination of the Agreement in whole or in part by BA, without penalty and without the provision of further opportunity to cure.

This document is only available to subscribers. Please log in or purchase access.

[Purchase](#) [Login](#)