COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 28, Number 18. May 13, 2019 Responding to a Possible Breach: An Incident Plan Checklist

Covered entities are required to have incident response plans ("OCR: Imaging Company Pays $3M to Settle HIPAA Case, Sat on FBI Tip," *RMC* 28, no. 18), says Chris Apgar, president of Apgar & Associates. Contact him at capgar@apgarandassoc.com.

Security Incident Investigation - Covered Entity

A. Incident Details:	
1. Date of Incident	
2. Date of discovery of incident	
3. Date Incident was reported to Business Associate/Covered Entity's Compliance Officer, Privacy Officer, Security Officer or Designee	
4. Status of investigation (e.g., completed, estimated completion date)	
5. Status of Corrective Action (e.g., devising, implementing, completed)	
B. Incident Description	
1. General Description	
2. What data elements were involved and the extent of the data involved in the breach.	[Name] [Birth date] [Etc.]
3. Description/name of the unauthorized person known or reasonably believed to have improperly used or disclosed PHI.	
4. Description of where the PHI is believed to have been improperly transmitted, accessed or utilized.	

5. Cause of Incident or probable cause.	
6. Impact of Incident – potential misuse of data, identity theft, etc.	
7. Interviews conducted and interview documentation	Names: Names: Documentation: See appendices [if applicable]
8. Whether any federal or state laws requiring individual notifications of breaches are triggered.	See Appendix – Risk Assessment [***if entity completing report is a covered entity***]; if unsecure PHI, initially assuming notification required
9. Forensic analysis conducted by:	
10. Results of forensic analysis	
11. Mitigation - steps to reduce any harmful effects known to Covered Entity as a result of potential unauthorized use or disclosure of PHI (continued).	Mitigation steps follow:
12. Corrective Action - steps to prevent reoccurrence.	See above. Mitigation activities also included [additional detail as needed]
13. Additional information – such as notification to other facility's units or Fraud Prevention and/or police, licensing boards, etc.	
14. Policies, procedures and processes adopted prior to the breach to address incident response (e.g., policy, procedure, incident response plan, plan testing schedule, etc.)	
15. [*Covered Entity/Business Associate or* independent third party v*endor remediation recommendations*]	After a review of the incident investigation report, interviews with compliance staff and the IT vendor, follow up question and answer and the existing incident response process, [*Covered Entity/Business Associate/ third party vendor remediation recommendations*] recommends the following:
Report Developed and Attested to by:	[Name & title] _____ Date_____