COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 32, Number 35. October 02, 2023
Internal Control Questionnaire for Physical Security

By Nina Youngstrom

This was developed by Piedmont Health in Georgia. It's used during audits of compliance with the HIPAA Security Rule's physical security requirements (see story, p. 4),[1] according to Debra Harris and Lisa Anderson, senior IT internal auditors at the Georgia health system. Contact Anderson at Lisa.Anderson@piedmont.org and Harris at Debra.Harris1@piedmont.org.

Internal Control Questionnaire: Physical Security

Prepared by: _____

Date: _____

Purpose

This questionnaire is designed to assist the person in charge of this business area in conducting a self-assessment of the adequacy of internal controls in place to ensure adequate monitoring procedures for physical security.

1. This questionnaire should be completed by the person delegated to be responsible for this area.
2. Save this file in your computer before completing and respond to each question below.
3. Please answer each question to the best of your knowledge.
4. Print a copy of this document for your records.
5. Electronically send the questionnaire back to the person that sent you the questionnaire.
6. Estimated completion time: 45 minutes

Questionnaire

1. Identify the responsible individuals for overseeing the facility's physical security.
2. Does a physical security policy exist? Please supply an electronic copy.
3. Do job descriptions exist for individuals with key security roles? Please supply an electronic copy.
4. Do policies and procedures exist for various security activities—theft, intrusion, physical threats/harm, etc.? If so, please provide an electronic copy.
5. Is the physical security of the facility included in routine risk assessments and adjusted as vulnerabilities change and new, emerging physical threats are identified? If so, please provide examples and any

supporting documentation.

6. Does the risk assessment include external and internal threats? If so, please provide examples and any supporting documentation.
7. How often are the facility's physical security policies, procedures and process reviewed, updated and approved by management?
8. Do policies/procedures exist for managing third-party/contract personnel (examples: data center hosting, IT infrastructure support, facility/building management, janitorial services, equipment support, suppliers, etc.) physical access and restricted access? If so, please provide an electronic copy.
9. How are third party/contract personnel screened, trained on the facility's local requirements (security, privacy, etc.) and monitored?
10. How are third-party/contract personnel monitored for adherence to the facility's local requirements?
11. Are the facility's local requirements for security, privacy, policies, etc., documented? If so, what is documented and where are the supporting documents stored?
12. Are third-party/contractors required to provide supporting documentation that their personnel meet all of the facility's awareness and training? If so, provide the list of the required training. (This question is similar to no. 17.)
13. Is there a physical access provisioning procedure for employees, medical staff, third-party/contract personnel, visitors, etc.? If so, please provide a copy.
14. Is security required to log rounds, incidents, activities, etc.? If so, please provide a copy of the logs for the prior month.
15. Do different badges exist for employees, visitors, third party/contract, medical staff? If so, please give a brief description of each type of badge.
16. Does a procedure exist for transfer, termination of badge access? If so, please provide an electronic copy and a brief description below.
17. Does a physical security training program exist for all employees, third-party/contract personnel, medical staff, etc.? If so, please provide a brief description below and please provide an electronic copy of the program. (See question no. 12.)
18. How is the local perimeter and critical infrastructure secured and protected? (Examples of areas: entrances, equipment, sensitive areas, controlled areas, IT infrastructure, drugs, etc. Examples of security: cameras, locks, fences, etc.)
19. Have any physical security reviews or audits been performed at the facility over the past 12 months? If so, please provide a copy of the report(s) and a status update on any findings noted during the review.
20. Have any physical security or security incidents occurred in the last 12 months? If so, please provide an electronic copy of the incident report, findings and updated remediation plan status for each incident. Where are these incidents logged?
21. How are the facility's outside areas such as parking, common areas, etc., monitored and secured?

22. If fences or barriers exist, are they routinely inspected and maintained properly? Please explain below.
23. Do cameras exist in the outside areas? If so, how are they tested and maintained? What is the retention policy for the video? For the security cameras located in internal critical areas, are these reviewed or consistently monitored? Do they follow the same testing maintenance and retention as outside cameras?
24. Is the outside lighting routinely inspected and maintained? If so, please give brief description below.
25. Does the local facility have any panic buttons or emergency notification stations? If so, please explain below along with the testing and maintenance process.
26. Have any drills (in-person or tabletop) been performed with the facility's security and local, state or other agencies to access the readiness and performance of responses for security incidents within the past year? If so, please provide a copy of the report, findings and status of remediation.
27. Any known concerns with the physical security of the facility?
28. Please list any shared site facility/building management arrangements for your location.
29. If any shared site facility/building management arrangements, were (1) utility requirements; (2) redundancies (power, HVAC, water communications, etc.); (3) shared communication closets and/or server rooms; (4) multiple connections to power for critical systems/equipment; (5) multiple telecommunication connections to prevent loss of voice services; (6) ground-to-earth conduit to carry excess power away from systems during power faults?

PLEASE PROVIDE AN ELECTRONIC COPY OF THE FOLLOWING ITEMS (most are included in the above questionnaire)

1. Physical security policy, procedures and process.
2. A list of individuals involved in physical security and job descriptions of the various levels included.
3. Security logs for rounding of prior month – including outside and internal areas.
4. Physical badging and access policy, procedures, process—including employees, third party/contract, medical staff, visitors, etc.
5. Termination and/or transfer procedures for badging and access.
6. Physical security training and awareness program.
7. Security equipment maintenance and testing policy, process, procedures.
8. Last risk assessments dealing with physical security.
9. Any audit and/or review of the physical security by internal, local, state, federal or third-party agencies in last year.
10. Physical security incident reports for last year, including any findings and updated remediation plan.