COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 28, Number 38. October 28, 2019
Questionnaire: Vendor Controls for ACH Payments and Wire Transfers

Here's a questionnaire to help health care organizations evaluate their internal controls around Automated Clearing House (ACH) payments and wire transfers, which are used to pay vendors, says Debi Weatherford, executive director of internal audit at Piedmont Healthcare in Atlanta. Wire transfers and payments may be manipulated internally or externally to steal money from health care organizations.[1] Contact her at debi.weatherford@piedmont.org.

Internal Control Questionnaire

Background: Many organizations utilize Automated Clearing House (ACH), an electronic funds transfer system that facilitates payments in the United States. The process relies on the accuracy of the ACH Direct Deposit Authorization Form to transfer payments to each vendor. Are your controls effective to detect an impersonator who requests a change to the ACH Direct Deposit Authorization Form? Are controls in place to prevent wire transfers requested by an unauthorized individual?

- Do you have documented policies and procedures that address ACH payments and wire transfers?
- Is a process in place to verify and validate not only requested changes in the electronic funds transfer system, but also any related accounts?
- How are requests for and actual changes to wire transfers handled?
- Who has access to make a wire transfer? How is this access monitored and managed?
- How is the ACH Direct Deposit Authorization Form independently verified?
- How are Treasury and Accounts Payable involved in new vendor setup and changes to vendors details?
- What mechanism is in place to notify Accounts Payable and Finance leadership of changes to vendor records?
- Are you independently verifying the ACH Direct Deposit Authorization Form with a "known" contact at the requesting company? If so, how is this documented and where is the documentary evidence maintained?
- Do you require a bank letter, and independently verify the validity of the letter with the bank? If so, how is this documented and where is the documentary evidence maintained?
- Is prenoting of the account implemented, and validation with the known contact conducted? An ACH prenote is a financial transaction with a $0.01 value submitted via the ACH network. Its purpose is to validate the banking information before committing the funds to transfer.
- Where are all verification documents maintained and housed?
- Is a routine vendor notification implemented to alert stakeholders of changes to vendor records?

- What monitoring is in place to review rejected payments and vendor accounts to effectively track required payments and rejected payments? What is the communication protocol regarding these rejected payments?
- Are you checking on a daily basis to review notifications –
    - When the funds were returned or the account closed?
    - When the banking information changed?
- What are your insurance coverage limits if an inappropriate payment is made as a result of a request from an impostor? Do you have additional approval of changes that are equal to or exceed this amount?
- What escalation parameters and actions are to be taken when suspected inappropriate activities are found? Who is on the Incident Response Team?
- Do you have a documented Social Engineering Fraud Incident Response Plan? A social engineering fraud is a confidence scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information provided to the employee in a written or verbal communication such as an email, fax, letter or even a phone call.
    - How are these groups involved:
        - Information Security
        - Finance
        - Legal
        - Risk Management
        - Compliance
        - Internal Audit
        - Other
    - How are these events handled:
        - Responsibility for internal investigation of events surrounding any incident
        - Notification of FBI, Secret Service or other Law Enforcement agencies
        - Communication with impacted vendors, if any
        - Communication with banking/financial partners
        - Notification of insurance carriers
        - Preservation of physical or electronic evidence