

DEPARTMENT: Treasury	POLICY DESCRIPTION: Vendor Profile Management
PAGE: 1 of 2	REPLACES POLICY DATED:
EFFECTIVE DATE: June 1, 2022	REFERENCE NUMBER: TRE.003
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All HCA Healthcare-affiliated (“Company”) facilities, its subsidiaries, and managed affiliates, including but not limited to, hospitals, ambulatory surgery centers, home health agencies, hospice agencies, physician practices (including 501A practices), outpatient imaging centers, shared service centers, joint ventures, and all Corporate Departments, Groups, Divisions and Markets. This policy does not apply to HCA Healthcare UK, which is subject to follow the Vendor Creation and Amendments Policy, as noted in the Reference section.

PURPOSE: To outline the data requirements that establish and maintain vendor information utilized for payment processing by the Company while ensuring completeness and accuracy of vendor profile data, particularly focusing on avoiding fraudulent or fictitious vendor payments.

POLICY:

The Company operates multiple business units with vendor payments processed by respective accounts payable operations and systems (i.e., Supply Chain, PSG, and Corporate Disbursements). As a result of multiple initiation points within the Company where vendor payments are processed, increased control is necessary to prevent fraudulent payments.

Fraudulent payment requests can occur via phone calls, fictitious invoices, or Business Email Compromise (BEC). Typically related to payments, BEC is a scam where criminals imitate or hack email accounts from vendors and business associates to request an action on the part of our colleagues. The Company routinely receives BEC scam attempts, which are disguised as valid requests from the associated vendor, many of these emails are attempting to change vendor payment information. A rigorous approach, and a highly skeptical mindset, to validating all vendor file changes is required, and any payment must wait until all required documentation outlined below is completed.

PROCEDURE:

- A. **Vendor Set-Up** – For each new vendor, the initial set up requires specific information entered into the vendor master file using approved forms. Depending on the business unit, specific procedures for vendor establishment should be followed, including, but not limited to, obtaining each of the following:
1. **IRS Form W-9:** Form W-9 provides personal identifiable information to a person or business used for reporting income paid to self-employed people like independent contractors, freelancers, vendors or other customers through a Form 1099 issued for each year’s payment activity.
 2. **Demographic Information:** Vendor demographic information (i.e., address, phone number, contact name, email address, etc.) should be obtained.
 3. **Electronic Payment Information (if applicable):** All vendor bank information and any changes to such information should be independently verified with the vendor and/or banking institution before any change is finalized and a payment is made.

DEPARTMENT: Treasury	POLICY DESCRIPTION: Vendor Profile Management
PAGE: 2 of 2	REPLACES POLICY DATED:
EFFECTIVE DATE: June 1, 2022	REFERENCE NUMBER: TRE.003
APPROVED BY: Ethics and Compliance Policy Committee	

4. **Physician Ownership Form:** Unless a vendor classification (e.g., governmental unit, utility, etc.) is specifically excluded, a Physician Ownership Form should be completed in accordance with Relationships with Physician Connected Vendors Policy, LL.027.
 5. **OIG Sanction Report:** Vendors should be checked for sanctions against the OIG website in compliance with Prohibition Against Contracting with Any Ineligible Person, MM.001.
- B. Vendor Information Update** – Vendor information should be verified/updated based on information received from the vendor (with appropriate verification) to ensure accurate information:
1. **Requirements for Banking Information Updates:** Any change to existing EFT information requires independent verification of changes requested by either confirming the changes in person or conducting the verification via an independently obtained phone number. This is facilitated by the use of the forms as described below:
 - a. **[HCA Healthcare Vendor Electronic Funds Transfer Change Request Form](#):** This form is to be completed by the Vendor and returned to the applicable Accounts Payable personnel.
 - b. **[HCA Healthcare Internal Electronic Funds Transfer Change Verification Form](#)** (to be completed by HCA Healthcare colleagues): All fields should be completed by Accounts Payable colleagues either in person or via a phone conversation with vendor personnel. It is important to verify all information, especially the phone number which must be independently verified/obtained. The form must be completed in its entirety and approved prior to making any EFT changes.

****NO BANKING INFORMATION CAN BE CHANGED IN THE VENDOR DATA FILE USING ONLY EMAIL COMMUNICATION. A CHANGE VERIFICATION FORM MUST BE COMPLETED AND REVIEWED BEFORE AN ELECTRONIC PAYMENT TO THE VENDOR CAN BE MADE TO THE NEW BANK ACCOUNT.****
 2. **Non-Banking Information Update (Corporate Only):** Updated W-9 and Physician Ownership forms should be updated if a vendor's address or ownership changes.

- REFERENCES:**
1. Code of Conduct
 2. [HCA Healthcare Vendor Electronic Funds Transfer Change Request Form](#)
 3. [HCA Healthcare Internal Electronic Funds Transfer Change Verification Form](#)
 4. Relationships with Physician Connected Vendors Policy, [LL.027](#)
 5. Prohibition Against Contracting with Any Ineligible Person, [MM.001](#)
 6. HCA Healthcare UK Corporate Vendor Creations and Amendments Policy
 7. Atlas Connect Sites:
 - a. [Corporate Disbursements](#)
 - b. [HealthTrust/Supply Chain](#)
 - c. [Physician Services Financial Services](#)
 - d. [Information Protection and Security](#) (IPS)
 - e. [IPS Business Email Compromise](#)