POLICY & PROCEDURE

Corporate Privacy Policy

EFFECTIVE: 11/1/2017

1. Purpose for Policy

Citizens Trust Company places a high value on the privacy of its clients ("Clients") and the expectation that information regarding Clients remains confidential and is made available only to persons who have a legitimate right to know. In addition, Citizens Trust Company is contractually obligated to comply with the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Citizens Trust Company recognizes that all employees and temporary workers ("Employees"), as well as outside contractors, have an ethical and legal obligation to keep certain information about Clients confidential and to protect and safeguard this information against unauthorized use or disclosure.

2. Overview

This privacy policy concerns protected health information ("PHI"). PHI, as defined by federal law, means any individually identifiable health information of a Client, including, but not limited to: social security number, name, address, birth date, age, telephone number, subscriber number, policy number, e-mail address, fax number, medical records and genetic information. PHI is not confined to written materials, facsimiles or hard copy. It also includes information derived from any source, including, but not limited to: e-mail, computer data, data stored on electronic media, disks or handheld computing devices (such as PDAs and smartphones), verbal communications or recordings and visual observation.

3. Procedures

The following section outlines the basic procedures necessary to comply with this policy.

Disclosure of Information

- An Employee may access, discuss, use and disclose PHI only for Citizens Trust Company business as it relates to that employee's specific job functions and/or responsibilities.
- Employees may disclose PHI only to those who have a legitimate, Citizens Trust Company-related business need to know or who have prior written authorization. PHI about a Client may only be shared for purposes of claims payment or healthcare operations.
- PHI must never be the subject of casual conversation either inside or outside of the workplace. PHI must not be discussed in lobbies, stairwells, elevators, restrooms, hallways, or any other public area where conversation could be easily overheard by visitors and Employees who do not have a need to know.
- Only "Minimally Necessary" PHI may be disclosed. "Minimally Necessary" means only that amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

Access to Information

- PHI may only be accessed if related to specific job functions and responsibilities.
- Casual reading of PHI is not permitted.
- Employees with legitimate access to PHI will protect this information from casual or unauthorized access.

Security of PHI

- Employees may remove PHI from the facility only as it relates to specific job functions and/or responsibilities. Approval from an employee's direct manager is necessary to remove PHI from the facility. It is the responsibility of each Employee to protect and safeguard all such information.
- Employees are encouraged to review PHI in a secure area and are responsible for records that are checked out to them. It is the responsibility of the Employee to protect and safeguard all records that are removed from the secure areas.
- Technical security safeguards are used to store, process and transmit electronic PHI. Our IT staff has primary responsibility for the security oversight of electronic PHI. Employees are responsible for complying with these security safeguards. All workstations that store, process or otherwise access electronic PHI must be protected with a strong password. Open sessions will be disconnected after a period of inactivity.

POLICY & PROCEDURE

Corporate Privacy Policy

EFFECTIVE: 11/1/2017

Breach of Confidentiality

- Any Employee who believes he/she has observed a breach of security or confidentiality should promptly notify his or her direct manager or the Chief Privacy Officer.
- Employees found to be in violation of this policy may be subject to disciplinary action, up to, and including termination and/or legal action. PHI is protected by federal and state laws and regulations that define civil and criminal penalties for violations of confidentiality.
- Citizens Trust Company will periodically conduct unscheduled audits to ensure compliance with this policy.

Safeguarding PHI

- In order to maintain confidentiality, any item containing PHI must be discarded according to the standards identified below:

Item	Examples	Where/How Discarded
Paper	Medical records, applications, census files, or any other paper-based document containing PHI	Paper-based PHI should be placed in a sealed recycle bin for destruction or destroyed by shredding. Electronic copies stored in the Citizens Trust Company Document Management System will be password protected using encryption procedures.
Electronic	Computer hard drives, disks, e-mails and electronic files	The IT staff will remove the hard drive from each computer or laptop that is scheduled for disposal. These hard drives will be physically secured until they are destroyed or recycled. Computers that will be reused must cleared or purged to remove PHI. Disks should be destroyed or re-formatted. E-mails and electronic files should be purged from the system after use. Employees needing assistance in disposing of electronic files should contact a member of our IT staff.

- Employees must not leave any PHI on fax machines, printers or copiers.
- Employees are to clean their workspace of PHI at the end of their work day and place the PHI in a secure location.
- Employees must exercise caution and discretion when leaving voicemail messages containing PHI.
- Employees are to escort visitors through work areas.
- Employees must exercise caution and discretion when e-mailing PHI internally within Citizens Trust Company.
- Employees must use appropriate encryption software when e-mailing PHI outside of Citizens Trust Company.
- Employees must not store PHI on handheld devices, such as PDAs or smartphones.
- Employees must secure all hardcopy mail containing PHI.
- Employee workstations will be programmed to auto-lock after 10 minutes of inactivity.
- Employees should refrain from loading PHI on pooled laptops. Information stored on laptops will be routinely purged.