



Citizens Ambulance Service Protected Health Information (HIPAA) ADMINISTRATION – POLICY AND PROCEDURE

INTRODUCTION

The *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”) established a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The HIPAA Privacy Rule protects all “*individually identifiable health information*” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “*protected health information*” (“PHI”).

PURPOSE

Citizens Ambulance Service, also known as CAS, has specific obligations as required by the HIPAA Privacy Rule. This policy establishes the requirements and best practices for CAS personnel to follow to ensure Privacy Rule compliance.

SCOPE

This policy applies to all employees (paid and volunteer) of the CAS and agencies who would assist CAS as EMS assist and/or mutual aid. Failure of current EMS assist and mutual aid agencies to comply with this policy could result in penalties against that agency(ies) via The U.S. Department of Health and Human Services (“HHS”). See Section F. PENALTIES FOR HIPAA VIOLATION for more information.

NOTE: ANY PHI disclosed to agencies who would assist CAS as EMS assist and/or mutual aid will be used ONLY to the extent necessary to meet activities authorized by the HIPAA Privacy Rule. Patients may exercise their rights through CAS to access, amend, restrict, and request an accounting, as well as lodge a complaint with either CAS or the Secretary of the HHS against the agency.

POLICY

CAS has developed and maintains Privacy Practices for the protection of PHI. All individuals who receive medical assessment or treatment from CAS personnel shall be provided with an opportunity to obtain the CAS Notice of Privacy Practices, receipt of which is acknowledged by the patient’s signature on the CAS Ambulance Billing Authorization and Privacy Acknowledgement. CAS Notice of Privacy Practices can be found on our website at www.citizensambulance.com/privacy and the Clipboard in Medic 1. Management and control of PHI which is used for approved purposes, including patient care documentation as required and shall be compliant with HIPAA in that the PHI shall be protected from unauthorized disclosure by:

1. Maintenance of business associate agreements with entities with which the CAS is authorized to share a patient’s PHI.

Effective Date of the Notice: June 6th, 2017

2. Covering or securing PHI while it is being used by CAS personnel for the purposes of patient care documentation, bill processing or authorized disclosure activities.
3. Segregating PHI from other documents by placing PHI in specially designated privacy envelopes for transmittal, if required.
4. Storage of paper PHI for a period of not less than seven years in a secured storage facility, access of which is limited to authorized personnel.
5. Storage of electronic PHI in password protected computers.
6. Shredding of PHI older than seven years, which is conducted at a CAS facility and supervised by an authorized CAS employee.
7. Electronic transmission to the CAS contracted billing service via a secure, independent web site.

Disclosure of PHI shall only be allowed if authorized by the patient, or as documented by the CAS Notice of Privacy Practices in adherence with HIPAA allowable disclosures. Patients may obtain information regarding the use and disclosure of their PHI as set forth in the CAS Notice of Privacy Practices.

A. PRIVACY OFFICER DESIGNATION

In compliance with the HIPAA Privacy Rule CAS has a designated Privacy Officer, which can be found on the CAS Notice of Privacy Practices. In the absence of the designated Privacy Officer, questions, concerns, reports or comments regarding PHI or HIPAA compliance should be directed to the EMS Coordinator.

B. PRIVACY RULE TRAINING

All CAS personnel are required to undergo Privacy Rule training as scheduled by the Privacy Officer in accordance with the HIPAA Privacy Rule within a reasonable time upon association with CAS or receiving this protocol. All personnel will be required to undergo additional training as scheduled by the Privacy Officer within a reasonable time should subsequent material changes to the HIPAA Privacy Rule and/or CAS policies and procedures regarding privacy practices occur. All Privacy Training will be conducted in a manner designated by the Privacy Officer.

C. ELECTRONIC PATIENT CARE REPORT (PCR)

1. All preparatory documentation and paper signature forms used by CAS personnel to assist in the creation or modification of a PCR is considered PHI and is the sole property of the CAS.
2. All CAS personnel that may be required to complete a PCR will be given a password to access the EMS Charts online program. This is unique to the individual. **DO NOT SHARE THIS PASSWORD**
3. No CAS personnel may disclose his/her password.
4. CAS personnel are to access only his/her PCR and associated PHI unless directed otherwise by the Privacy Officer or as permitted by CAS policy for compliance or quality improvement purposes.
5. Printed PCRs and their associated PHI are to be placed in a secure location when not being used. A specially designated privacy drop box shall be used for this purpose when any of these items are not in the possession or control of the person that prepared the information.

6. All scratch paper or draft PCR paperwork used by CAS personnel in the preparation of a PCR must be shredded immediately after the PCR is completed.
7. CAS personnel may not retain any PHI other than for purposes of completing the required PCR.

D. ACCESS TO PHI

Access, disclosure and use of PHI will be to the extent necessary to meet activities authorized by the HIPAA Privacy Rule. Patients may exercise their rights to access, amend, restrict, and request an accounting, as well as lodge a complaint with either CAS or the Secretary of the HHS.

E. INCIDENTAL DISCLOSURES

The Privacy Rule is not intended to impede common practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers. Incidental disclosures should be kept to a minimum and related to required patient care practices.

F. PENALTIES FOR HIPAA VIOLATION

There are significant legal penalties against agencies and individuals that do not adhere to the HIPAA Privacy Rule. Failure of CAS personnel to comply with this policy could result in penalties against CAS and discipline against the individual(s).

Failure to comply with HIPAA can result in civil and criminal penalties ranging from \$100 to \$50,000 per violation (42 USC § 1320d-5).

Failure of current EMS assist and mutual aid agencies to comply with this policy could result in penalties against that agencies via The U.S. Department of Health and Human Services (“HHS”).

By Signing below I have read all of the above, understand the above, and agree to uphold the HIPAA Standards of The U.S. Department of Health and Human Services (“HHS”). I also agree to report all NON-INCIDENTAL DISCLOSURES to the EMS Coordinator Immediately.

Employee Name: _____

Employee Signature: _____

HIPAA Trainer Name: _____

HIPAA Trainer Signature: _____

EMS Coordinator Name: _____

EMS Coordinator Signature: _____

Effective Date of the Notice: June 6th, 2017