Protected Health Information (PHI) and Client Privacy (HIPAA)

Policy	#ADM032
First Effective Date	10/2018
Revision Dates	2/2021
Page	1 of 3

Purpose

- CFAC team members may have access to Protected Health Information (PHI). Any PHI, whether oral, written, photographic, or electronic, should be maintained in a manner that ensures its privacy and security.
- PHI must be treated with respect and care by any team member who is authorized to have access to this information. Team members who are authorized to use or disclose PHI also have the responsibility to safeguard access to such information and a responsibility to limit uses and disclosures to those that are allowed by permission, by authorization and/or by law. The access must be appropriate to the team member's job responsibility. A breach is a violation of CFAC's privacy or security policies and/or state or federal regulatory requirements resulting in the unauthorized or inappropriate use, disclosure or access of PHI. Any team member's behavior, that compromises a patient's or a human subject's privacy or PHI, is covered by this policy.

Policy

Definitions

Disclosure: The release, transfer, access to, or divulging in any other manner protected health information outside of the CFAC. An example would be the release of protected health information to a third party who is not engaged as a relevant MDT member of the Cochise Family Advocacy Center.

Privacy Breach: The use or disclosure of oral, paper or electronic Protected Health Information by an individual for purposes other than those for which s/he is authorized, or a violation of a privacy or security requirement resulting in potential for such an unauthorized use or disclosure.

Protected Health Information (PHI) includes:

Protected Health Information (PHI) and Client Privacy (HIPAA)

Policy	#ADM032
First Effective Date	10/2018
Revision Dates	2/2021
Page	2 of 3

- Individually identifiable health information in any form (paper, electronic, oral) that is transmitted and/or stored by CFAC or a business associate that relates to the past, present, or future health of an individual, provision of health care, or payment for health care that is linked to a patient.
- Identifying or personal information, as defined in Federal Trade Commission's Red Flags Rules, including any name or number that may be used in conjunction with any other information to identify a specific person, e.g. social security number, credit card number or passwords.

Use: The authorized sharing, application, review or analysis of PHI within CFAC.

Team Members: Employees, volunteers, trainees, interns, medical staff, Board of Directors and any other persons whose conduct, in the perfom1ance of work for CFAC, is subject to the control of such entity, whether or not they are paid by the CFAC.

Reporting Responsibilities

The individual who commits, observes or becomes aware of an unauthorized or inappropriate access, use or disclosure of PHI is responsible for promptly reporting such to one of the following:

- A supervisor
- The Executive Director

When a potential breach occurs the supervisor or Executive Director will coordinate a review of the potential breach and, when applicable, review the circumstances surrounding the breach, mitigation steps and any harmful effect that may result from the breach. The supervisor and Executive Director will determine appropriate sanctions concerning the breach.

Process

The following process should be followed when a potential breach occurs:

Protected Health Information (PHI) and Client Privacy (HIPAA)

Policy	#ADM032
First Effective Date	10/2018
Revision Dates	2/2021
Page	3 of 3

- Upon receipt of a potential breach, the supervisor shall report this potential breach to the Executive Director immediately upon awareness of such a potential breach. The confidentiality of all participants shall be maintained to the extent possible, within reason, throughout the investigation.
- Upon notice of the potential breach by a team member, the supervisor or Executive Director will assess and/or investigate the potential breach and determine any corrective action as warranted. Investigations may include, but are not limited to interviews, electronic user access audit trails, review of telephone logs, or other activities.
- The supervisor or Executive Director may investigate the circumstances of the potential breach, including interviews or request for written statement(s) from staff.
- When a breach is substantiated, the supervisor will review the findings with the Executive Director to coordinate the communication of corrective action. In the case of CFAC interns, the supervisor will inform the Executive Director and will coordinate the communication of corrective actions with the intern's academic institution.
- Such factors as the nature and severity of the potential breach will be taken into consideration in determining the appropriate level of sanction.
- It may be appropriate to delay corrective action if the action adversely affects or compromises client care.

Corrective Action

Corrective action, if warranted, will be imposed based on the nature and severity of the violation, whether intentional or not, circumstances surrounding the privacy breach or whether the violation demonstrates a pattern or practice of improper use or disclosure of confidential information on the part of the team member. Corrective action relating to this policy shall be applied fairly and consistently.

All corrective actions will be documented in writing and maintained in the appropriate personnel record. If warranted, corrective actions. up to and including termination may be reported to the applicable licensing board.