

Medical Compliance

SUBJECT: Compliance Investigations

PURPOSE: To define the process of conducting medical compliance investigations.

STAFF GOVERNED BY THIS POLICY: Health and Medical Division, Cherokee Indian Hospital, Tsali Care Center

EFFECTIVE DATE: August 23, 2005

DATE REVIEWED OR REVISED:

DISTRIBUTION: HMD, CIHA, TCC

POLICY:

The Medical Compliance Officer shall investigate compliance concerns to detect possible violations in applicable laws, regulations, and guidelines. The extent of the investigation will vary depending upon the concern.

PROCEDURE:

1. Provide Complaint options.
 - a. All Providers and Entities will give Complainants the option of presenting their complaint in person or in writing to their Privacy Officer, or by phone to a Hotline. If the Privacy Officer is the subject of the complaint, it may be presented to Privacy Officer's immediate supervisor. If the supervisor is inappropriate, then to the Legal Division or Internal Audit.
 - b. These options shall be displayed prominently in a public area of each provider location, written in clear, simple language. They shall also be shown in each provider's Privacy Notice. For every person who has Provider responsibilities, his/her immediate supervisor shall ensure that she is trained to identify a complaint and refer the complainant to these options for reporting.
2. Who receives complaints: Privacy Officers/Compliance Officer will receive complaints of every nature and route them appropriately. Every Health Care Provider shall maintain a privacy officer. Each privacy officer may designate a back-up.
3. Maintain Complaint logs.
 - a. Each Privacy Officer/Compliance Officer shall establish and maintain a log for complaints. Privacy Officer's/Compliance Officer's immediate supervisors are responsible for periodically verifying that this is maintained. The log shall be organized to capture the following data for each complaint:
 - date and time complaint received
 - date and time received by Privacy Officer/Compliance Officer

- tracking number assigned by Hotline; other identifying number if given in writing or verbally
 - a short summary that does not give complainant's or staff member's name
 - the Privacy Officer's/Compliance Officer's signature
 - space to note any transfer of the complaint to another provider/entity
 - space to note the disposition of the complaint,
 - copies of acknowledgment letters.
- b. Logs shall be maintained in a place and manner that prevents access by unauthorized users, loss and destruction.
4. Send Complaint Acknowledgement letters.
 - a. The Privacy Officer or his designee will assess the nature of complaints. If the Privacy Officer in his/her best judgment determines it relates to HIPAA or other federal regulation, s/he will mail an initial response letter acknowledging receipt of the complaint. If there is any reasonable doubt whether the complaint is related to HIPAA or other federal regulations, err on the side of sending the acknowledgement letter. The letter shall be mailed within a priority time frame after the Privacy Officer's receipt of the completed complaint. If other applicable laws require shorter timeframes, then follow those laws.
 5. Conduct Investigations.
 - a. Investigate all complaints.
 - i. The Privacy Officer or designee will investigate all complaints, regardless of nature. S/he will establish and maintain procedures for categorization and prioritization of the seriousness of the complaints. These should take into account timeliness, potential for harm to life, property, privacy or reputation, as well as any costs related to remedying the problem or leaving the problem in place. "Costs" could include civil liability, as well as regulatory/criminal liability including jail and fines. If the complaint involves a HIPAA or other federally-regulated issue, s/he will notify the Privacy Officer/Coordinator of the complaint and work with the Coordinator during the investigation.
 - ii. Investigation shall include, but not be limited to, discussion with complainant, any involved patient/insured person, and any involved staff members; review of all relevant documents; and review of all applicable laws and regulations. Where it appears that the complaint suggests a threat to life or property, financial loss to EBCI or affiliate entity of \$5000 or more, or a potential violation of law, the Privacy Officer should contact the appropriate upper management, Legal Division and/or Internal Audit as appropriate. Each step of the investigation should be documented, showing the date and a brief description of the step taken.
 - b. Follow established timelines.
 - i. Investigation shall begin within a reasonable time frame.

- ii. A separate file shall be established for each separate investigation. The file should note, and be organized numerically by, the identifying number of the complaint (tracking number, if from Hotline), a copy of the acknowledgment letter, and the dates of receipt shown in the log. The files shall be maintained in a place and manner that prevents access by unauthorized users, loss and destruction.
 - iii. The Privacy Officer/Compliance Officer must conclude investigation and recommendations for action within a reasonable time frame.
- 6. Produce concluding report.
 - a. Upon conclusion of the investigation, the Privacy Officer will prepare a confidential report. It should list all persons contacted in the investigation, all documents reviewed, and all regulations potentially impacted. It should summarize the factual scenario ascertained in the investigation and analyze the accuracy of the facts alleged. It should then analyze the risks presented by those facts if true and conclude with recommendations for any action needed. That report should state steps recommended to mitigate any risk of violation of law, and any risk to the complainant, patient/employee, and Provider or state that no further action is needed.
 - b. The Privacy Officer shall file the conclusion report in the complaint file, and distribute it to appropriate upper level management and to any persons responsible for carrying out recommended actions. Distribute in a manner that maintains confidentiality.
 - c. The Privacy Officer shall note the final disposition of the complaint in the complaint log, stating at a minimum “investigation conducted, closed on ___/___/___ with delivery of report and recommendations for action” or for “no further action”.
- 7. File maintenance. Each Provider’s and Entity’s Privacy Officer shall preserve the closed investigatory files (confidentially and safe from loss by fire, flood, infestation, dry rot and theft) for 6 years beyond the “closed on” date noted on the file. Each Privacy Officer shall preserve logs for 6 years beyond the latest “closed on” dated noted on any entry on the log. Throughout the 6 years, both must be kept in a place and manner such that the Entity or Provider maintaining them, can produce them intact. These may be preserved and tracked for destruction in 12-month batches, rather than tracked as individual records, but such a batch must be preserved for 6 years beyond the last date-of-generation in the batch.

