For minor substance abuse clients, the minor must sign all authorizations. Parental signatures may be included, but are not sufficient.

Although Geminus is not a provider of medical services, because Geminus works in close collaboration with Regional, as well as with other health service providers, Geminus does keep certain medical record information received from providers authorized by the client or guardian. This information is not Geminus-owned, so it cannot re-disclose this information even if requested to do so by a client or guardian; it must be managed by Protected Health Information standards. Requests by the client for information originating from outside medical providers must be requested from the originating provider.

A Geminus program exception: Circle Around Families (CAF) is a DCS Cross System contracted service. Geminus is responsible for brokering services from multiple community providers. By local program design, every CAF service plan is determined by a Family Team facilitated by a CMHC Care Coordinator and signed off by a CMHC Physician. For that reason every CAF record needs to be treated by Geminus as a medical record to assure all information is treated with appropriate confidentiality.

Please see Medical Records procedures (links are provided below) for information regarding the proper completion of authorizations to disclose Protected Health Information and procedures for the release of such information.

5) Multiple Geminus service records will contain Health Information received from health care providers authorized by individuals or a parent/guardian. For example, Head Start and Early Head Start are early childhood education services with strong family engagement components that include assuring parents are receiving secure adequate health care services for their child. HS/EHS nurses keep school records to monitor and assure health needs of these young children have been met.

    a) Whatever medical record information may have been provided to Geminus by an individual or guardian, that part of the Geminus record must be managed in full compliance with HIPAA or 42 CFR Confidentiality Standards. Since Geminus is not the health care provider, they are not authorized to re-disclose that medical information

6) Other Geminus programs maintain PII, Personally Identifying Information that must be maintained as confidential and kept secure. These include the NW Indiana Child Care Development Fund, and the Child Care Resource and Referral program. These programs have sites on Corporation property as well as off-site locations. Whether personally identifying information is collected electronically or on paper, each facility must protect the PII.

    a) Paper records will be stored in a locked file, and be maintained in an office with a door that locks, and is secured from unauthorized entry. Paper records being transported needed to be kept in locked transport containers.

b) Inactive paper files from these programs are stored in secured locked locations until permission is received from the Office of Early Childhood and Out of School learning for them to be shredded. The room must be locked with limited restricted authorized access.

7) In situations where a court orders, or where there is a clear and present danger to self or others, information will be disclosed without authorization only in accordance with federal law, including Health Insurance Portability and Accountability Act (HIPAA) Regulations, Indiana law, and in consultation with the treating psychotherapist. Workers in substance abuse programs should refer to section 2.63 of the Federal Register regarding the release of objective data only in response to court orders. Refer to Medical Records procedures whenever there is a need to release information without authorization. Please consult with the Privacy Officer as a record of any such disclosures must be maintained.

8) Clients 18 years of age or older wishing to access their medical information must do so on Corporation-approved forms. The right to access personal medical information may be refused under certain limited circumstances by the supervising physician. Inpatients are not permitted a copy of their medical record while they are on the inpatient unit. Parents/guardians, both custodial and non-custodial, have access to information for clients less than 18 years of age unless they are substance abuse clients. In that case, minors must give authorization for information to be released to their parents.

9) Nothing in this procedure and accompanying policy should be construed as contradicting federal law relating to the confidentiality of substance abuse clients. The protection for substance abuse records described in the Federal Register supersedes any related state laws.

10) It is each individual employee's responsibility to respect the confidentiality of the client. All clients will be fully informed about confidentiality, the purposes for which information is obtained, and how it may be used. The Corporation will provide each client with a Notice of Privacy Practices, which describes how medical information may be used and disclosed. Limits of confidentiality such as: discussing case with treatment team members and supervisors, group treatment, and mandated disclosures should be discussed with clients.

11) Information regarding a client’s treatment, finances, or other confidential information should be shared among co-workers only for professional purposes, and then the minimal information necessary to accomplish that purpose.

12) No recording (audio or video), observing of sessions, school observations, photographs, etc., will be done without the client's written consent, thus ensuring the privacy of the client. In addition, no client listings of any kind will be placed in view of anyone not authorized to have that information.

13) Client information not included in the medical record, such as billing or insurance lists, statistics, ride/transportation lists, phone messages, video, audio or computer tapes should be secured and not open to public viewing. When these documents are no longer needed they

are to be shredded. Materials needing to be shredded should be brought to the shredding receptacles on a daily basis and should not be left unattended in staff offices.

14) Telephone conversations with or regarding a client will take place in a confidential manner, especially when others are in the area. Messages left for clients on answering machines will not contain confidential information, and messages left by clients will be retrieved in a confidential manner.

15) Computer terminals with access to client data should be turned off when staff is away from their desks. Refer to the Information Services Security Policies (links provided below) for further instruction on the confidentiality of client data.

16) Faxes will include a cover sheet with a confidentiality statement to inform the recipient that the information cannot be re-released without the client's authorization. The sender will verify fax number before transmitting the information. Faxes will be used for clinical information only after verifying that the intended recipient is there to receive the information. The use of facsimile machines to receive authorizations is acceptable.

17) Neither unsecured E-mail nor texting shall be used for the transmission of confidential clinical client information. When using e-mail within the corporation's network to submit client information for purposes of Treatment, Payment or Operations (TPO), staff should only identify the clients by account number and/or partial name or initials and should transmit only the minimum necessary to accomplish the intended purpose.

18) Encrypted mail (secured) can be used when sending confidential information to other treatment providers and funders. See policy and procedure on email encryption provided below.

19) All US mail delivered to corporate addresses are to be opened by employees trained to receive, sort and properly route and US Mail that may contain PI or PHI.

20) Office security: Badges and keys are assigned to all new employees and must be returned upon leaving employment. Certain locked doors have restricted access authorization either by ID badge or by assignment of keys.

21) Any employee who absolutely must remove client information from the Center becomes totally responsible for the preservation of confidentiality and possesses the extra burden of ensuring that no other individual obtains access to that information. The Corporation provides locked bags to use for this purpose. An example of where it is acceptable to remove

client information is the printing of a form like a treatment plan that needs to be taken to a client home for signature.

22) All clinicians are expected to be familiar with the Federal Register, including HIPAA Regulations, and Indiana State Law regarding confidentiality and with the particular ethical standards of their profession.

23) All new employees will be trained on the HIPAA regulations no later than thirty (30) days after their initial hire date.

24) The clinician's obligation to report suspected child or adult abuse supersedes client/therapist confidentiality. If a report to Protective Services is made regarding a substance abuse client, the report should make no reference to substance abuse treatment. Other HIPAA exceptions are contained in the Notice of Privacy Practices.

25) Without the consent of the client, mental health, but not substance abuse records, may be released to other health care providers or mental health care providers, if the mental health records are needed to provide health care or mental health services to the client.

26) Unsecured confidential material to be disposed of will be shredded or incinerated.

27) Any privacy violations must be reported to the Privacy Officer. Security violations are reported to the Security Officer. Violations are subject to disciplinary action.

28) If through an omission or careless act an employee allows another to obtain confidential information, the disciplinary action will be dependent on the following considerations:
   a) Overall performance
   b) Prior disciplinary record
   c) Employee's efforts to protect confidentiality
   d) Other circumstances regarding the occurrence

29) Any second occurrence of omission or carelessness causing the improper release of confidential information will be grounds for immediate termination, dependent on the circumstances.

30) Any willful or knowledgeable breach of client confidentiality will be treated in accordance with the discipline section of the HR discipline policy and procedure.

31) HIPAA Privacy and Security violations are also subject to criminal and civil fines, penalties