Family Focus Inc.		**Policy Number:** AG-069
Subject:	HIPPA	
Section:	Administrative General	
Effective Date: 01/01/2011		**Review Date: 04/01/2015**
		Revised Date:
☐ **New Policy**		☐ **Supersedes Policy Dated:**
Issued by: HR Administrator		**Concurred with and Approved by:** Jim Burns, Director Initial: _____
Cross Reference:	CR-001 Client's Rights to Confidentiality	
Distribution:	All employees of Family Focus, Inc.	

PURPOSE

General:

It is the policy of Family Focus to commit to protecting the medical information of its plan participants. Family Focus is required by law to maintain the privacy of this medical information, provide a notice of privacy practices, and abide by the terms of that notice. To that end, all members of Family Focus's workforce who have access to protected health information (PHI) must comply with this Privacy Policy.

During the performance of their duties, individuals may be required to have access to and be involved in the processing of confidential information, including but not limited to, client records, indexes of information, client demographics, client billing and appointment history, confidential communications made for purposes of treatment of a client, employee personnel records, including employee health records and information regarding the business strategy, financial transactions, or performance of the corporation.

Confidential information is not confined to written materials or hard copy, but includes information derived from any source, including, without limitation to, computer data, verbal communications or recordings, faxes, phone conversations, dictation, and videotape.

Confidential information is to be handled with strict discretion and not to be read, discussed, utilized by or disclosed to any person without proper authorization. All persons should exercise a high degree of professionalism and restraint when discussing or utilizing client information. If an individual is uncertain about the confidentiality status of any information, he/she should solicit assistance from a supervisor or manager.

For purposes of this policy, the company's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, interns, contracted employees, and other

persons whose work performance is under the direct control of Family Focus, whether or not they are paid by Family Focus.

Electronic:
According to HIPAA, e-PHI (electronic protected health information) does not include paper to paper faxes, video teleconferencing, or messages left on voice mail. However, the Privacy Practice Rules apply to all forms of PHI and will be followed in regards to:

- Family Focus will follow all HIPAA guidelines in protecting all mental health information.
- Family Focus will ensure that the confidentiality and integrity of all electronically protected health information.
- Family Focus will protect against any responsible threats or hazards to secure the integrity of such records.
- Family Focus will reasonably protect against any unanticipated disclosures of PHI.
- Family Focus will ensure adequate security for all PHI that is created or received by Family Focus.
- Family Focus will regularly perform risk assessments on their security features for their electronic PHI.
- Family Focus will work to ensure that when an employee is no longer employed by Family Focus they can not access any PHI associated with Family Focus.
- Family Focus will properly train all staff of the proper security features of Family Focus e-PHI.
- Family Focus will safeguard all employee passwords that are used to get into their computers, emails, or voicemails.
- All Family Focus personnel will ensure that the organization's data, including medical, client, financial and personnel records, are kept confidential.
- It is the responsibility of all Family Focus personnel to use only their own identity, I.D, and password while using the organization's IT resources. A personal ID and password must not be shared with anyone else, either inside or outside the organization.
- Any Family Focus staff that neglects to follow any of these policies may be subject to dismissal.

Release of Client Information:
Family Focus will abide by all HIPAA and Indiana State laws when copying and/or releasing protected health information/records. Information will only be released with a signed *Release of Information* from the client except in HIPPA sanctioned situations listed below, in accordance with policy CR-009 Client Rights to Confidentiality, and for a fee of $.10 per page:

1. In a criminal proceeding involving a homicide if the disclosure relates directly to the fact or immediate circumstances of the homicide.
2. If the communication reveals the contemplation or commission of a crime or a serious harmful act.
3. In the event that there is a referring physician, psychologist, psychiatrist, or counselor.
4. To anyone part of the Family Focus, Inc. staff that is involved in the treatment of the client.
5. To any person required by federal, state, local laws to have lawful access to the treatment of the client.
6. To the Court if it orders any relevant information to be sent as progress or results of treatment, such as with a mental competency hearing.
7. If there is any type of civil or malpractice action against the clinician.
8. To any third party service in order for Family Focus, Inc. to receive payment for therapy/treatment of the client.
9. To any additional persons that the client gives specific written authorization to receive their information such as a legal representative.

10. Family Focus, Inc. has the right to, by Indiana State Law; inform the proper agencies or authorities without the permission of the client with regard to any duty to warn obligations.
    a. When there is a risk of imminent danger to the client or another.
    b. When there is a substantial suspicion of any type of abuse or neglect.

Client Sign-In:
Family Focus will protect client confidentiality in accordance to HIPAA, federal, or state laws when they are signing-in for their appointments.

Disposal of documents/materials protected under HIPPA:
Family Focus will follow all guidelines set forth by HIPPA and update their process of disposal in accordance with HIPPA. Family Focus will educate all staff as to the appropriate method of disposal per HIPAA guidelines. (see policy AG-075 Document retention and destruction)

Physical and Technical Safeguards:
The protection of information against unauthorized access, modification or disclosure, whether storage, processing or transit. These resources include; all media that store or communicate information including, but not limited to, paper records (client records, business office records, personnel records, financial records, administrative records, etc.), computers (hardware, software, and storage media), Internet, copy machines, fax machines, telephones, answering machines, employees, printers, and typewriters.

Family Focus will allow minimal physical access to the electronic information system facility. Family Focus will safeguard the system facility and equipment. Family Focus will remove any electronic information, in accordance with HIPAA and federal laws, from any electronic media prior to the media being reused.

Access to Family Focus information resources will be granted based on the user's job function, business need, research requirement or legal authority including the following:

1. Family Focus Employees which includes contracted and non-contracted
2. Referral sources
3. Consultants
4. Authorized Government or Legal Representatives

PROCEDURES
General:
All responses to requests for PHI will be limited to the minimum amount of information needed to accomplish the purpose of the request or disclosure. An individual may authorize use, request restrictions, inspect his or her records, and amend and request an accounting of disclosures of his or her PHI. The NOTICE OF HIPAA PRIVACY PRACTICES describes in more detail how an individual's PHI may be used and disclosed.

The Family Focus HR Administrator will receive all requests, inquiries, questions, and complaints with regard to the use and disclosure of PHI and any questions under this Policy, related procedures, or the NOTICE OF HIPAA PRIVACY PRACTICES. The HR Administrator will maintain in written or electronic form any communication, action, activity, or designation to comply with the HIPAA privacy regulations. If an individual believes that it would be inappropriate to contact the HR Administrator, the individual may contact the Director.

The HR Administrator will assist in the interpretation of all laws and regulations related to this policy, the procedures and practices, and will guide the contact person and Family Focus in their implementation.

Any violations of this policy may result in disciplinary action up to and including termination. Individual obligations and responsibilities continue after termination of employment, contract, affiliation, etc. Individual access privileges are subject to periodic review, revision and if appropriate, renewal.

Electronic:

Family Focus will reside over the security and protection of the PHI and work to develop and maintain the following guidelines outlines by HIPPA for PHI:

- Family Focus will ensure that staff has access to either a private workstation or a shared workstation, both of which are secured and protected through a unique employee password.
- Family Focus will provide a separate email account and voicemail for each employee to which only the employee or director know the password for. Passwords are never to be shared with anyone.
- It is the responsibility of each Family Focus staff member to remove records from public access areas if observed unattended, and it to return the designated location for those records.
- Individuals are not authorized to install any software on any computer provided by Family Focus without prior approval of administration.
- Each Family Focus, Inc. individual who signs on to a computer must sign off or lock PC when leaving it unattended in a location where it is accessible to the public or unauthorized persons.
- Family Focus staff will secure personal computers against theft and physical damage.
- Individuals are to report any violation of the information security policy to their supervisors. All notifications will be logged and investigated.
- Workstation monitors in public-access areas are to be pointed away from public view when possible
- Printed reports containing confidential or sensitive information are to be stored in a lockable receptacle or secured area, inaccessible to unauthorized persons. When confidential printed reports are no longer needed, they should be shredded.
- Diskettes containing confidential information are to be labeled confidential and protected in a container or a secure area.
- Database backup will be stored in a safe location off-site (not exposed to heat or magnetic fields).
- Confidential originals will not be left in the copier feeder or on the copier glass unattended.
- Secure disposal containers will be provided near each copier for the proper disposal of pages or entire documents.
- Systems which support transmission of confidential information outside the Family Focus data network (e.g., Internet) are NOT authorized to transmit client or Family Focus.-proprietary confidential information unless:
    - Both the sending and receiving systems encrypt such data, OR
    - Such data is transmitted exclusively via a protected medium (e.g., fiber-optic cabling, point-to-point, dedicated data line or virtual private network technologies). This network security plan requires approval by the Director.
- Numbers which are programmed or entered into fax machines to receive confidential information MUST be validated before they are actually used.
- Secure disposal containers will be provided near fax machines.
- Fax machines will be placed in secure locations - inaccessible to the general public.
- Numbers used with frequency will be pre-programmed into the fax machine in order to decrease the likelihood of incorrect dialing.

- Conversations involving confidential information will be held in a private setting or with the maximum level of discretion. Verbal information should be held in the same regard as electronic and paper information.
- Access to playback of dictation and automated voice response systems will be controlled using unique PIN numbers.

Release of Client Information
Clients also have the right to know how their information is being or will be used as in the following:

1. *Request to Amend Health Records* form may be completed by the client if they feel something is in error. In accordance with HIPPA, clients may request, but Family Focus does not have to agree to the change.
2. *Request for Alternative Means of Confidential Information* form is completed when the client prefers to be notified/contacted by other means than their home address and phone.
3. *Release of Information* form is completed by the client when information is to be sent to a third party that falls outside of the HIPPA sanctioned situations listed above.
4. *Request for Listing of Disclosures of Client Records* form is completed by the client when they are requesting to know with whom we have shared their information and when it was shared.
5. *Record of Request for Client Information* form is completed when the client wants to know with whom Family Focus has gathered information and how that information was used.

Disposal of documents/materials protected under HIPPA:
In accordance with HIPPA guidelines, mental health records may be disposed of (e.g., shredded) six (6) years after the date of the service termination for that client.

Any electronically stored protected health information that is dated more than six years post the termination date of treatment should be deleted by a person with appropriate technical knowledge to ensure that the information can reversed.

Under no circumstances will any Family Focus staff dispose of any PHI or e-PHI outside of the Family Focus facility.

All records received during an internship program will be disposed of in accordance with HIPAA standards at the completion of the internship.

Physical and Technical Safeguards:
Integrity: All of Family Focus's data will be backed up daily. For security and safety reasons all data is externally backed up and maintained off premises daily. Family Focus's policies follow its data regardless on which computer system the data actually reside. Virus protection will be active on Family Focus's IT resources at all times and updated at least monthly.

Security: No IT services shall be provided to external organizations or individuals without the express permission of Family Focus, this includes file-sharing, web services, and internet access. All passwords granting any access to Family Focus's IT resources may be changed on a regular basis. The Director shall possess all existing, new, and routinely changed passwords, for the server and all network computers. Family Focus will provide each employee with their own individual username in order for Family Focus to tract their actions.

Security of Records: Family Focus will ensure doors of rooms that hold client charts are locked when staff is away from the office as well as locking cabinets that hold charts when they are not being used. Family Focus will not keep client records in a public access area or waiting areas. Family Focus will ensure that any records stored off site will be maintained in a secure environment.

Record Storage: Any non-active client record must be secured in a locked area. Family Focus will monitor any access to non-active patient records by Family Focus staff. When access to a physical record storage area is made by a workforce member, it is the responsibility of that workforce member making or providing the access to insure the record storage area is secured upon leaving.

Employee Education:
Employees will, upon acceptance of a position as an employee of Family Focus, review the Employee Handbook, which includes a Confidentiality Agreement. Upon receipt of the Handbook, the employee will sign a document acknowledging receipt of the handbook. Thereafter, an annual review and revision as necessary of the Employee Handbook will be distributed to all employees. Employees will sign documents acknowledging each updated Handbook, and the signed document will be maintained in the employee's personnel file. It is the responsibility of each employee to review the Employee Handbook including the confidentiality agreement and the conditions under which disciplinary action may be taken should a willful security breach occur.

Non-employees (defined as anyone working with or providing a service for Family Focus who is not an employee of Family Focus, including but not limited to, volunteers, consultants, or contract services individuals) may, as part of the normal execution of their duties, come in contact with confidential and/or client specific information. Non-employees entering into an engagement and/or contract with Family Focus are expected to complete a Confidentiality Agreement. Subsequent agreements must be completed annually thereafter or at the beginning of a new engagement/contract when a break in continuous service is greater than one year. Obtaining and storing Confidentiality Agreements from non-employees is the responsibility of the appropriate Department Head.

Each individual is responsible for understanding and observing the provisions of this policy. If an employee is in doubt whether information is confidential and how it should be protected, it is his or her responsibility to consult their immediate supervisor. Contractors' questions regarding this policy should be discussed with the appropriate department or business affiliate at Family Focus, Inc.

Failure to comply with Family Focus, Inc.'s Information Security policies and procedures may result in disciplinary action, including termination without warning or notice and civil or criminal legal penalties, at the discretion of Family Focus, Inc. administration.

Notice of Privacy Practices

PROCEDURE

A. Content and Changes to the Notice of Privacy Practices.
    1. The FAMILY FOCUS, INC. Notice of Privacy Practices (NPP) must contain the elements as listed in the Federal Register, HIPAA privacy regulations, section 164.520.

2. Whenever there is a material change to the FAMILY FOCUS, INC. uses and/or disclosure of client information, the client's rights, FAMILY FOCUS, INC.' legal duties regarding the privacy practices of client information, or other privacy practices stated in the NPP, FAMILY FOCUS, INC. will revise the NPP and post the revised notice in a clear and prominent location. The effective date of the revised notice will also be listed in the NPP. FAMILY FOCUS, INC. will also post the revised notice on the FAMILY FOCUS, INC. web site (when developed).
3. FAMILY FOCUS, INC. will provide its NPP to anyone who asks and allow the individual to take with him/her.
4. FAMILY FOCUS, INC. will keep the NPP on file 6 (six) years from its first effective date or the date last in effect, whichever is later.

B. Obtaining signed acknowledgment of receipt of the FAMILY FOCUS, INC. NPP.
1. FAMILY FOCUS, INC. personnel must make a good faith attempt to obtain a signed acknowledgment of receipt of the FAMILY FOCUS, INC. NPP as of the first service delivery date to each client during the registration process beginning no later than April 14, 2003. (See Section "C" below for obtaining signed acknowledgment during health fairs, public health screenings, etc.)

2. If there is no record of the client signing an acknowledgment of receipt of the FAMILY FOCUS, INC. NPP or if there is no electronic system to check in that department, the client is to be offered the NPP and asked to sign the acknowledgment of receipt of the FAMILY FOCUS, INC. NPP.
    a. If the client takes receipt of the FAMILY FOCUS, INC. NPP and signs acknowledgment of receipt, FAMILY FOCUS, INC. personnel "check" the appropriate box, complete the form, and follow their department protocol of where to route or store the signed acknowledgment.
    b. If the client refuses to take the FAMILY FOCUS, INC. NPP and signs they refuse to take the FAMILY FOCUS, INC. NPP, FAMILY FOCUS, INC. personnel are to "check" the appropriate box, complete the form, and follow their department protocol of where to route or store the signed refusal.
    c. If the client refuses to take the Family Focus, Inc. NPP and refuses to sign acknowledgment of their refusal, FAMILY FOCUS, INC. personnel are to "check" the appropriate box, complete the form, and follow their department protocol of where to route or store the refusal.
    d. See attachment "B" with department listings for routing/storing of signed acknowledgment or refusal.
3. If FAMILY FOCUS, INC. is unable to obtain the signed acknowledgment or refusal to receive the FAMILY FOCUS, INC. NPP despite good faith efforts, the FAMILY FOCUS, INC. staff member is to document in the client record the efforts made to obtain and the reason why the acknowledgment was not obtained.
4. If the reason the signed acknowledgment was due to an emergency situation or incapacity of the client, FAMILY FOCUS, INC. personnel are to attempt to obtain the signed acknowledgment of receipt of the FAMILY FOCUS, INC. NPP from the client and give the client the FAMILY FOCUS, INC. NPP as soon as it is feasible to do so.

C. Posting on Web Site

1. FAMILY FOCUS, INC. will post the currently effective FAMILY FOCUS, INC. Notice of Privacy Practices on the FAMILY FOCUS, INC. web site. The FAMILY FOCUS, INC. secretary will be responsible for this posting.

D. Enforcement

1. The Director is responsible for enforcing this policy and all FAMILY FOCUS, INC. personnel are responsible for adhering to this policy. FAMILY FOCUS, INC. personnel who violate this policy are subject to progressive discipline up to and including termination from association with FAMILY FOCUS, INC. in accordance with ER-006.