INDIANA STATE UNIVERSITY PSYCHOLOGY CLINIC
POLICIES AND PROCEDURES MANUAL
HIPAA Compliance Manual

Updated 7/26/21

Table of Contents

Introduction

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was designed to accomplish a number of objectives, one of which is to protect the privacy of individually identifiable health information. Protection standards exist for protected health information (PHI) in all forms, including electronic formats (ePHI).

The standards set forth by HIPAA apply to "covered entities," including health care providers and the agencies they work within. The ISU Psychology Clinic is a covered entity and is thus required to comply with the regulations specified by HIPAA. This manual details the policies and procedures established for the Clinic to ensure HIPAA compliance.

Administrative Safeguards. Administrative safeguards refer to the policies and procedures used by the ISU Psychology Clinic to comply with HIPAA standards.

Security Officer

The Clinic Director is the designated Security Officer for the clinic and is responsible for knowing HIPAA regulations, training the Clinic staff, student clinicians, and supervisors ("Clinic Personnel") in HIPAA compliance, and assuring that HIPAA-related policies and procedures are instituted and followed within the Clinic. Joey Newport, Human Resources, is the HIPAA Compliance Officer for the University. His contact information is: (812) 237-4120, joey.newport@indstate.edu.

The Clinic Director will:

- Update HIPAA policies and procedures.
- Oversee the implementation of the policies and procedures contained in this Manual.
- Ensure that all Clinic personnel are trained regarding HIPAA and the policies and procedures of the Clinic.
- Review activity that takes place in the Clinic to detect security risks.
- Respond to security incidents and take appropriate action in the event of a violation of clinic policy, and send this information to Joey Newport to investigate a potential breech in security, and eliminate or mitigate any damaging effects.

HIPAA Training Program

All Clinic personnel are required to participate in a formal HIPAA training program. The training program was instituted in the Clinic in the spring of 2013, and all existing personnel were required to complete the training at that time. Henceforth, all incoming clinical students and any new clinical faculty receive the training within 60 days of their arrival to ISU.

The training involves watching the HIPAA Training for Covered Entities tutorial, and then taking the HIPAA Training Quiz. Successful completion of the training and quiz is required in order to work in the Clinic. The Clinic Director/Security Officer reviews with each quiz-taker any content associated with a failed item on the quiz. Anyone receiving a grade less than 85% on the quiz must repeat the training.

Additionally, this Manual is given to all Clinic personnel. It is also available online and in hard-copy in the Clinic library.

Documentation of Training

Training of Clinic personnel is be recorded in the HIPAA Training Log.

HIPAA Notification

All clients who receive services in the Clinic are offered a HIPAA Notification document before their first session (see Appendix A) and sign a document indicating that they have been offered the Notification. Additionally, a HIPAA Notification document is visible and available in the Clinic waiting room. This information is emailed to telehealth only clients.

Consent for Release or Exchange of Information

Client PHI is typically released to another party only when the release is requested, in writing, by the client or client's legal guardian. The "Authorization for Release of Information" form is completed when a request is made (see Appendix B).

PHI may at times be released without client authorization, but only in accordance with strict policies (see HIPAA Notification for *Uses and Disclosures with Neither Consent nor Authorization* in Appendix A*).*

Client PHI may also be obtained from another covered entity when requested, in writing, by the client or client's legal guardian. The "Authorization for Release of Information" form is completed when a request is made.

Ensuring that Disclosures are the Minimum Necessary

When a request is received to disclose PHI, the request is reviewed by the case supervisor and the Clinic Director/Security Officer. Only the minimum necessary amount of information will be disclosed. The principle guiding the release of PHI is to limit disclosure of information that is not reasonably necessary to accomplish the purpose for which the request is made.

Accounting for Disclosures

The Clinic staff complete an Accounting for Disclosures form whenever a release of information is requested by a client (see Appendix C). In keeping with HIPAA Privacy Rules, the form specifies who has received access to the client's PHI and ePHI. Yearly requests for accounting of disclosures will be provided free of charge, and given within 60 days of a request for the information.

Requests for File Review and Copy

Clients who have records in the Clinic may request to inspect and obtain a copy of their PHI in the "designated record set," defined as the medical and billing records maintained by the Clinic and used to make decisions about the client. The request must be made in writing, and will be

fulfilled within 30 days of receipt. Note, however, that HIPAA does not allow clients to have access to their therapist's Psychotherapy Notes.

Requests to Amend a Record

Clients have the right to amend their record if they believe the record is incomplete or not accurate. The amendment will become part of their ongoing file. Requests for record amendments must be made in writing. Clients may not expunge any prior information or part of the Record.

Policies and Procedures to Access Protected Health Information

Access to PHI is limited to Clinic personnel and business associates (see below), and further restricted by virtue of what information is needed by personnel to complete a job function and/or clinical training.

Security Assessment

The Clinic Director/Security Officer will engage in a yearly assessment of the Clinic's adherence to the policies detailed in this manual. As part of the annual assessment, teams consisting of faculty and student clinicians are asked to search the Clinic for any potential security problems and to recommend additional security measures.

Reporting of Security Violations

Clinic personnel are required to report any violations of HIPAA standards to the Clinic Director or Office Manager. Observing a violation and not reporting it may lead to disciplinary action.

Responding to Violations and Preventing Further Violations

When security incidents or deficiencies are reported or discovered, the Clinic Director investigates the situation and sends this information to the ISU Compliance Officer. They then institute appropriate corrective measures to help ensure that similar violations do not occur in the future. Corrective measures may include personnel re-education, policy revision, building modification, and/or equipment alterations. Violations may also lead to disciplinary action.

Responding to a Breach of Protected Health Information

According to the American Psychological Association (2013), a "breach" is defined as the acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule. Examples of a breach include stolen or improperly accessed PHI; PHI inadvertently sent to the wrong provider; the unauthorized viewing of PHI, and the like. A use or disclosure of PHI that violates

the Privacy Rule is presumed to be a breach unless the University Compliance Officer conducts a risk assessment (as prescribed by APA) and determines that there is a low probability that PHI has been compromised. In the event that the risk assessment indicates that there has been a breach, breach notification procedures will be followed.

Breach Notification Procedures

In the event of a breach of PHI, the Clinic Director/University Compliance Officer notifies the client(s) affected within 60 days after discovery. Notification complies with the procedures recommended by APA.

Business Associates

"Business associates" are defined by HIPAA as third parties who provide services to the Clinic and in so doing have access to electronic patient health information. The ISU Psychology Clinic does not currently have any business associates. In the event that the Clinic enters into an arrangement with a business associate a Business Associate Agreements will be adopted and utilized.

Research Activities

Client information may not be used for research purposes unless the client has agreed to allow his/her PHI to be used in this manner.

Clinic Visitors

In general, having visitors in the Clinic is discouraged. However, visiting is permitted on a brief and limited basis if the visitor is escorted by Clinic personnel who take care to ensure that PHI is not visible. Confidentiality statements must be signed by all visitors.

Physical Safeguards. Physical safeguards refer to the ways in which the ISU Psychology Clinic controls physical access to protected information.

Building Access

Access to the Clinic is limited to Clinic personnel who are given keys coded for full or limited access depending on job duties and need for access. Keys are dispersed by the Clinic Director/ Security Officer who maintains a record of key distribution. Keys are returned to the Clinic Director upon termination from ISU.

Mailboxes

Written communication pertaining to the Clinic and clinical work is distributed via personnel mailboxes housed within the Clinic. These mailboxes are kept in a locked room. No Clinic-related material should be put in faculty or student mailboxes that are outside the Clinic.

Session Recordings

Student clinicians record their work with clients so that it may be viewed by supervisors. Recordings are made automatically with cameras and microphones installed in each treatment room. Recordings are maintained for one month on a secure server and then erased. Only authorized Clinic personnel are given access to the computer program that plays the recorded sessions.

Keeping a Recording

At times for clinical or training purposes, a Clinical Supervisor may determine that a session should be kept for longer than the 1-month period that is available on the server. In this case the Supervisor may copy the session from Milestone onto an encrypted flash drive (available from the Office Manager). This recording will then be placed in the client's paper file and kept locked in the client file cabinet. Access to the recording will be monitored/allowed by Clinical Faculty.

Documentation

Session notes are recorded on Titanium, a secure electronic medical records system. Students write reports about clients on encrypted flash drives that are used in the Clinic only. The documents are then transferred to Titanium and may also be put in client's paper file. Client documents that are typically written/saved on flash drives include intake reports, psychological assessment reports, treatment plans, termination reports, and treatment summaries. Client

documents MAY NOT be saved to a clinician's personal computer, unless the document is completely de-identified using the clinic de-identification procedure. Documents may not be emailed to supervisors, unless completely de-identified. It is also advisable to password protect any client de-identified client document prior to saving/emailing (use of the flash drive password is advised). Paper charts must stay in the Clinic at all times unless you are taking a chart to a supervision session upstairs. Paper charts and flash drives may not be taken home under any circumstances, as to do so is a security violation.

HIPAA Guidelines for PHI (how to de-identify client reports)

The following items need to be removed from a document to de-identify it and meet HIPAA standards:

(A) Names

(B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes.

(C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

(D) Telephone and fax numbers

(E) Email addresses

(F) Social security numbers

(G) Medical record numbers

(H) School name/city

(I) Any other unique identifying number

Document Retention

Electronic medical records on Titanium are maintained indefinably in that secure medium. Current client paper files are maintained in a file cabinet that is open during business hours and locked thereafter. The room holding these files is locked after hours as well. Paper files of terminated clients are housed in locked cabinets in a file room that is locked when the Clinic is not open for business.

Document Disposal

Client paper files are maintained for seven-year post termination (seven years past age 18 for minor clients). After that period, the file content is shredded.

Workrooms

Students work on client records in one of the workrooms within the Clinic, either a group workroom or a private workroom. These rooms are in the private section of the Clinic, and computer screens are not in direct view of unauthorized persons. PHI will not be left visible on computer screens or out on tables unattended when Clinic personnel leave the room. Do not leave charts or any client document out on tables in the work room.

In addition, student information will not be left visible on computer screens or out on tables unattended due to FERPA regulations. The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99. Education records are records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail.

Technical Safeguards. Technical safeguards refer to the ways in which the ISU Psychology Clinic controls access to computer systems and protects communications containing PHI transmitted electronically from being intercepted by anyone other than the intended recipient.

Electronic Medical Records System (Titanium)

The Clinic uses Titanium, an electronic medical records system designed specifically for university counseling centers and psychology training clinics. Titanium can only be accessed by Clinic personnel, each of which has a unique user name and password. Supervisors use a digital signature to ensure data integrity. Access is further restricted by safety measures in the system that keep users from being able to view records of clients who are not their own or for whom they are supervising. Once files are saved they cannot be changed or erased. Full access to Titanium is granted only to the Clinic Director and the clinical faculty member who is responsible for IT maintenance.

Computer Workstations

The reception computer in the Clinic logged off after business hours. Computer workstations in the student workrooms within the Clinic are on continuously but documents are not saved to the computer hard-drives. All Clinic personnel/clinicians log off of Titanium and documents before leaving them unattended. Drafts of documents are kept on encrypted flash drives until they are completed and maintained in Titanium and/or client files.

Computer Flash Drives

Drafts of documents that are not ready to be transferred to Titanium or a client file are kept on encrypted flash drives that are housed in the Clinic and leave the Clinic only to be reviewed within the building by supervisors. **Flash drives may not be taken home under any circumstances.** When documents are complete and have been transferred to the client's file, they can be erased from the flash drive.

Faxing

The fax machine in the Clinic is housed in the office of the Office Manager and is checked throughout the day to ensure that faxed documents are not left unattended. The office containing the fax machine is locked when the Clinic is not open.

The Clinic's policy is to mail PHI whenever possible. If faxing, only the PHI actually needed is sent, and a cover letter with a confidentiality statement accompanies the information to help prevent casual reading. Additionally, frequently used fax numbers are programed into the

machine to ensure accuracy in dialing, and new fax numbers are verified before PHI is transmitted. The machine does not have the capacity to save copies of faxed information.

Emailing

The emailing of client information between clinicians is discouraged. On the occasion that any information about a client is emailed, only the client's initials should be used. Verbal/written consent to communicate via email is obtained for all telehealth clients, and those clients indicating a preference for emailed communication.

Telephones

Calls are made to clients from the reception area only for routine appointment reminders and appointment clarification. At these times, only first names are used. Calls to clients that require more disclosure of information are made from the phones in the workrooms or private offices.

Data Maintenance and Emergency Procedures

Since January of 2009, most private health information in the Clinic is ePHI that is maintained by an Electronic Medical Records System (Titanium) that is disaster and damage proof. All other PHI is kept in locked, metal, file cabinets. In the event of a disaster or damage to these records every effort will be made to restore the lost or damaged data.

Telehealth safeguards. In March 2020, the ISU clinic began telehealth services due to the COVID-19 pandemic. The following policies are in place for telehealth services

- The ISU Psychology Clinic will use Zoom for Healthcare, a HIPAA compliant platform, and a BAA is in place.
- All telehealth services will be conducted from a clinic therapy room, unless specific permission has been granted from the clinic director or supervisor.
- The Waiting Room option will be used in Zoom to ensure only clients can access the session.
- Discuss and verify that the client is in a private space at the start of Zoom session.
- All telehealth consent forms and procedures were created in conjunction with Joey Newport (HIPAA officer) and ISU legal advisors.

Appendices

A: Notice of Privacy Practices

B: Authorization for Release/Exchange of Information

C: Accounting for Disclosures Form

D: Security Incident Report

E: HIPAA Consent to Participate in Research

Appendix A

INDIANA STATE UNIVERSITY

PSYCHOLOGY CLINIC
TERRE HAUTE, IN 47809
812-237-3317
INDSTATE.EDU

NOTICE OF PRIVACY PRACTICES
This Notice is effective January 15, 2014

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.
PLEASE REVIEW IT CAREFULLY

WE ARE REQUIRED BY LAW TO PROTECT MEDICAL INFORMATION ABOUT YOU

We are required by law to protect the privacy of medical information about you and that identifies you. This medical information may be information about healthcare we provide to you or payment for healthcare provided to you. It may also be information about your past, present, or future medical condition.

We are also required by law to provide you with this Notice of Privacy Practices explaining our legal duties and privacy practices with respect to medical information. We are legally required to follow the terms of this Notice. In other words, we are only allowed to use and disclose medical information in the manner that we have described in this Notice.

We may change the terms of this Notice in the future. We reserve the right to make changes and to make the new Notice effective for *all* medical information that we maintain. If we make changes to the Notice, we will:

- Post the new Notice in our waiting area.
- Have copies of the new Notice available upon request. Please contact our Privacy Officer at 812-237-3317 to obtain a copy of our current Notice.

The rest of this Notice will:

- Discuss how we may use and disclose medical information about you.
- Explain your rights with respect to medical information about you.
- Describe how and where you may file a privacy-related complaint.

If, at any time, you have questions about information in this Notice or about our privacy policies, procedures or practices, you can contact our Privacy Officer at 812-237-3317.

WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU IN SEVERAL CIRCUMSTANCES

We use and disclose medical information about patients every day. This section of our Notice explains in some detail how we may use and disclose medical information about you in order to provide healthcare, obtain payment for that healthcare, and operate our business efficiently. This section then briefly mentions several other circumstances in which we may use or disclose medical information about you. For more information about any of these uses or disclosures, or about any of our privacy policies, procedures or practices, contact our Privacy Officer at 812-237-3317.

1. Treatment
We may use and disclose medical information about you to provide healthcare treatment to you. In other words, we may use and disclose medical information about you to provide, coordinate or manage your healthcare and related services. This may include communicating with other healthcare providers regarding your treatment and coordinating and managing your healthcare with others.

2. Payment
We may use and disclose medical information about you to obtain payment for healthcare services that you received. This means that, within the health department, we may *use* medical information about you to arrange for payment (such as preparing bills and managing accounts). We also may *disclose* medical information about you to others (such as insurers, collection agencies, and consumer reporting agencies). In some instances, we may disclose medical information about you to an insurance plan *before* you receive certain healthcare services because, for example, we may need to know whether the insurance plan will pay for a particular service.

3. Healthcare Operations
We may use and disclose medical information about you in performing a variety of business activities that we call "healthcare operations." These "healthcare operations" activities allow us to, for example, improve the quality of care we provide and reduce healthcare costs. For example, we may use or disclose medical information about you in performing the following activities:

- Reviewing and evaluating the skills, qualifications, and performance of healthcare providers taking care of you.
- Providing training programs for students, trainees, healthcare providers or non-healthcare professionals to help them practice or improve their skills.
- Cooperating with outside organizations that evaluate, certify or license healthcare providers, staff or facilities in a particular field or specialty.
- Reviewing and improving the quality, efficiency and cost of care that we provide to you and our other patients.
- Improving healthcare and lowering costs for groups of people who have similar health problems and helping manage and coordinate the care for these groups of people.
- Cooperating with outside organizations that assess the quality of the care others and we provide, including government agencies and private organizations.
- Planning for our organization's future operations.
- Resolving grievances within our organization.
- Reviewing our activities and using or disclosing medical information in the event that control of our organization significantly changes.
- Working with others (such as lawyers, accountants and other providers) who assist us to comply with this Notice and other applicable laws.

4. Persons Involved in Your Care
We may disclose medical information about you to a relative, close personal friend or any other person you identify if that person is involved in your care and the information is relevant to your care. If the patient is a minor, we may disclose medical information about the minor to a parent, guardian or other person responsible for the minor except in limited circumstances. For more information on the privacy of minors' information, contact our Privacy Officer at 812-237-3317.

We may also use or disclose medical information about you to a relative, another person involved in your care or possibly a disaster relief organization (such as the Red Cross) if we need to notify someone about your location or condition.

You may ask us at any time not to disclose medical information about you to persons involved in your care. We will agree to your request and not disclose the information except in certain limited circumstances (such as emergencies) or if the patient is a minor. If the patient is a minor, we may or may not be able to agree to your request.

5. Required by Law
We will use and disclose medical information about you whenever we are required by law to do so. There are many state and federal laws that require us to use and disclose medical information. For example, state law requires us to report gunshot wounds and other injuries to the police and to report known or suspected child abuse or neglect to the Department of Social Services. We will comply with those state laws and with all other applicable laws.

6. National Priority Uses and Disclosures
When permitted by law, we may use or disclose medical information about you without your permission for various activities that are recognized as "national priorities." In other words, the government has determined that under certain circumstances (described below), it is so important to disclose medical information that it is acceptable to disclose medical information without the individual's permission. We will only disclose medical information about you in the following circumstances when we are permitted to do so by law. Below are brief descriptions of the "national priority" activities recognized by law. For more information on these types of disclosures, contact our Privacy Officer at 812-237-3317.

- **Threat to health or safety:** We may use or disclose medical information about you if we believe it is necessary to prevent or lessen a serious threat to health or safety.
- **Public health activities:** We may use or disclose medical information about you for public health activities. Public health activities require the use of medical information for various activities, including, but not limited to, activities related to investigating diseases, reporting child abuse and neglect, monitoring drugs or devices regulated by the Food and Drug Administration, and monitoring work-related illnesses or injuries. For example, if you have been exposed to a communicable disease (such as a sexually transmitted disease), we may report it to the State and take other actions to prevent the spread of the disease.
- **Abuse, neglect or domestic violence:** We may disclose medical information about you to a government authority (such as the Department of Social Services) if you are an adult and we reasonably believe that you may be a victim of abuse, neglect or domestic violence.
- **Health oversight activities:** We may disclose medical information about you to a health oversight agency – which is basically an agency responsible for overseeing the healthcare system or certain government programs. For example, a government agency may request information from us while they are investigating possible insurance fraud.

- **Court proceedings:** We may disclose medical information about you to a court or an officer of the court (such as an attorney). For example, we would disclose medical information about you to a court if a judge orders us to do so.
- **Law enforcement:** We may disclose medical information about you to a law enforcement official for specific law enforcement purposes. For example, we may disclose limited medical information about you to a police officer if the officer needs the information to help find or identify a missing person.
- **Coroners and others:** We may disclose medical information about you to a coroner, medical examiner, or funeral director or to organizations that help with organ, eye and tissue transplants.
- **Workers' compensation:** We may disclose medical information about you in order to comply with workers' compensation laws.
- **Research organizations:** We may use or disclose medical information about you to research organizations if the organization has satisfied certain conditions about protecting the privacy of medical information.
- **Certain government functions:** We may use or disclose medical information about you for certain government functions, including but not limited to military and veterans' activities and national security and intelligence activities. We may also use or disclose medical information about you to a correctional institution in some circumstances.

7. Authorizations

Other than the uses and disclosures described above (#1-6), we will not use or disclose medical information about you without the "authorization" – or signed permission – of you or your personal representative. In some instances, we may wish to use or disclose medical information about you and we may contact you to ask you to sign an authorization form. In other instances, you may contact us to ask us to disclose medical information and we will ask you to sign an authorization form.

If you sign a written authorization allowing us to disclose medical information about you, you may later revoke (or cancel) your authorization in writing (except in very limited circumstances related to obtaining insurance coverage). If you would like to revoke your authorization, you may write us a letter revoking your authorization or fill out an Authorization Revocation Form. Authorization Revocation Forms are available from our Privacy Officer. If you revoke your authorization, we will follow your instructions except to the extent that we have already relied upon your authorization and taken some action.

The following uses and disclosures of medical information about you will only be made with your authorization (signed permission):

- ❑ Uses and disclosures for marketing purposes.
- ❑ Uses and disclosures that constitute the sales of medical information about you.
- ❑ Most uses and disclosures of psychotherapy notes, if we maintain psychotherapy notes.
- ❑ Any other uses and disclosures not described in this Notice.

YOU HAVE RIGHTS WITH RESPECT

TO MEDICAL INFORMATION ABOUT YOU

You have several rights with respect to medical information about you. This section of the Notice will briefly mention each of these rights. If you would like to know more about your rights, please contact our Privacy Officer at 812-237-3317.

1. Right to a Copy of This Notice
You have a right to have a paper copy of our Notice of Privacy Practices at any time. In addition, a copy of this Notice will always be posted in our waiting area. If you would like to have a copy of our Notice, ask the receptionist for a copy or contact our Privacy Officer at 812-237-3317.

2. Right of Access to Inspect and Copy
You have the right to inspect (which means see or review) and receive a copy of medical information about you that we maintain in certain groups of records. If we maintain your medical records in an Electronic Health Record (EHR) system, you may obtain an electronic copy of your medical records. You may also instruct us in writing to send an electronic copy of your medical records to a third party. If you would like to inspect or receive a copy of medical information about you, you must provide us with a request in writing. You may write us a letter requesting access or fill out an **Access Request Form**. Access Request Forms are available from our Privacy Officer.

We may deny your request in certain circumstances. If we deny your request, we will explain our reason for doing so in writing. We will also inform you in writing if you have the right to have our decision reviewed by another person.

If you would like a copy of the medical information about you, we will charge you a fee to cover the costs of the copy. Our fees for electronic copies of your medical records will be limited to the direct labor costs associated with fulfilling your request.

We may be able to provide you with a summary or explanation of the information. Contact our Privacy Officer for more information on these services and any possible additional fees.

3. Right to Have Medical Information Amended
You have the right to have us amend (which means correct or supplement) medical information about you that we maintain in certain groups of records. If you believe that we have information that is either inaccurate or incomplete, we may amend the information to indicate the problem and notify others who have copies of the inaccurate or incomplete information. If you would like us to amend information, you must provide us with a request in writing and explain why you would like us to amend the information. You may either write us a letter requesting an amendment or fill out an **Amendment Request Form**. Amendment Request Forms are available from our Privacy Officer.

We may deny your request in certain circumstances. If we deny your request, we will explain our reason for doing so in writing. You will have the opportunity to send us a statement explaining why you disagree with our decision to deny your amendment request and we will share your statement whenever we disclose the information in the future.

4. Right to an Accounting of Disclosures We Have Made
You have the right to receive an accounting (which means a detailed listing) of disclosures that we have made for the previous six (6) years. If you would like to receive an accounting, you may send us a letter requesting an accounting, fill out an **Accounting Request Form**, or contact our Privacy Officer. Accounting Request Forms are available from our Privacy Officer.

The accounting will not include several types of disclosures, including disclosures for treatment, payment or healthcare operations. If we maintain your medical records in an Electronic Health

Record (EHR) system, you may request that include disclosures for treatment, payment or healthcare operations. The accounting will also not include disclosures made prior to April 14, 2003.

If you request an accounting more than once every twelve (12) months, we may charge you a fee to cover the costs of preparing the accounting.

5. Right to Request Restrictions on Uses and Disclosures
You have the right to request that we limit the use and disclosure of medical information about you for treatment, payment and healthcare operations. Under federal law, we must agree to your request and comply with your requested restriction(s) if:

1. Except as otherwise required by law, the disclosure is to a health plan for purpose of carrying out payment of healthcare operations (and is not for purposes of carrying out treatment); and,
2. The medical information pertains solely to a healthcare item or service for which the healthcare provided involved has been paid out-of-pocket in full.

Once we agree to your request, we must follow your restrictions (except if the information is necessary for emergency treatment). You may cancel the restrictions at any time. In addition, we may cancel a restriction at any time as long as we notify you of the cancellation and continue to apply the restriction to information collected before the cancellation.

You also have the right to request that we restrict disclosures of your medical information and healthcare treatment(s) to a health plan (health insurer) or other party, when that information relates solely to a healthcare item or service for which you, or another person on your behalf (other than a health plan), has paid us for in full. Once you have requested such restriction(s), and your payment in full has been received, we must follow your restriction(s).

6. Right to Request an Alternative Method of Contact
You have the right to request to be contacted at a different location or by a different method. For example, you may prefer to have all written information mailed to your work address rather than to your home address.

We will agree to any reasonable request for alternative methods of contact. If you would like to request an alternative method of contact, you must provide us with a request in writing. You may write us a letter or fill out an **Alternative Contact Request Form**. Alternative Contact Request Forms are available from our Privacy Officer.

7. Right to Notification if a Breach of Your Medical Information Occurs
You also have the right to be notified in the event of a breach of medical information about you. If a breach of your medical information occurs, and if that information is unsecured (not encrypted), we will notify you promptly with the following information:

- ❑ A brief description of what happened;
- ❑ A description of the health information that was involved;
- ❑ Recommended steps you can take to protect yourself from harm;
- ❑ What steps we are taking in response to the breach; and,
- ❑ Contact procedures so you can obtain further information.

8. Right to Opt-Out of Fundraising Communications
If we conduct fundraising and we use communications like the U.S. Postal Service or electronic email for fundraising, you have the right to opt-out of receiving such communications from us. Please contact our Privacy Officer to opt-out of fundraising communications if you chose to do so.

YOU MAY FILE A COMPLAINT ABOUT OUR PRIVACY PRACTICES

If you believe that your privacy rights have been violated or if you are dissatisfied with our privacy policies or procedures, you may file a written complaint either with us or with the federal government.

We will not take any action against you or change our treatment of you in any way if you file a complaint.

To file a written complaint with us, you may bring your complaint directly to our Privacy Officer, or you may mail it to the following address:

Clinic Director
ISU Psychology Clinic
424 N. 7th Street
Terre Haute, IN 47809

To file a written complaint with the federal government, please use the following contact information:

Office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHH Building
Washington, D.C. 20201

Toll-Free Phone: 1-(877) 696-6775

Website: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

Email: OCRComplaint@hhs.gov

Appendix B

Indiana State University
Psychology Clinic
AUTHORIZATION FOR RELEASE OF INFORMATION

I hearby authorize the **ISU PSYCHOLOGY CLINIC, 424 N. 7th Street – Root Hall, Terre Haute, IN 47809** to Release/Exchange protected information to/from the facility/person you designate.

_____	_____
Name of Client	Organization / Person to disclose information
_____	_____
Street Address	Street Address
_____	_____
City/State/Zip Code	City/State/Zip Code
_____	
Date of Birth	

I authorize and consent to the release of the following information to/from the ISU Psychology Clinic.

_____ Intake Report
_____ Summary of Treatment Report
_____ Medical or Court Records
_____ Verbal communication
_____ Psychological Evaluation Report
_____ Treatment Plan
_____ School Records
_____ Other, as specified below

_____

The information is being released for the purpose of:

_____ Assessment/Evaluation
_____ Coordination of care/treatment planning and implementation
_____ Attorney request
_____ Other, as specified here_____

This consent may be revoked by me in writing at any time, and will expire in 180 days *or* as specified below:

_____

I understand that information to be released may include information regarding drug or alcohol abuse, psychological or psychiatric impairments, confidential communications, HIV and/or AIDS, physical conditions or other information which may be privileged or confidential under State and/or Federal law. I also understand that the information disclosed may be subject to re-disclosure by the recipient of the information and may no longer be protected by the HIPAA Privacy Rule.

_____	_____
Signature of Client	Date
_____	_____
Signature of Parent/Guardian (if client is a minor)	Date
_____	_____
Signature of Witness	Date

_____
(Name of ISU Clinic Clinician)
ISU PSYCHOLOGY CLINIC
424 N. 7th Street – Root Hall
Terre Haute, IN 47809
Phone: (812) 237-3317 Fax: (812) 237-8595

Appendix C

Indiana State University Psychology Clinic
Accounting for Disclosures
Form

_____There were no applicable disclosures made of your protected health information for the period your specified.

_____Disclosures of your protected health information were made by this office to:

Date of Disclosure	Name of Whom Information was Disclosed	Address	Description of Information Disclosed	Purpose of Information Disclosed

We are temporarily unable to process the accounting for disclosures you have requested due to:

_____A suspension required by law.

_____Other, specify: _____

However, your request will be provided by _____
(Month/Day/ Year)

If you have any questions concerning this accounting for disclosures, please contact:

_____ at : _____ (Signature of Psychologist or Staff Member) (Telephone number)

_____ _____
Printed Name Date

Appendix D

ISU Psychology Clinic
Security Incident Report

Date: _____

Description of Security Incident:

_____
_____
_____
_____
_____
_____
_____
_____

Measures Taken to Resolve the Problem or Mitigate Effects:

_____
_____
_____
_____
_____
_____
_____
_____

Steps Taken to Prevent Recurrence:

_____
_____
_____
_____
_____
_____
_____
_____

_____
Security Officer

_____
Signature of Security Officer

E: HIPAA Consent to Participate in Research

Indiana State University
Psychology Clinic
HIPAA Consent to Participate in Research

1. **Purpose.** As a research participant, I authorize (faculty name) and the researcher's staff to use and disclose my (and my child's) individual health information for the purpose of conducting the research project entitled (enter title of the study).

2. **Individual Health Information to be Used or Disclosed.** Individual health information from my (my child's) evaluation that may be used or disclosed to conduct this research includes: (list all components of the evaluation).

3. **Parties Who May Disclose My Child's and My Individual Health Information.** The researcher and the researcher's staff may obtain my (my child's) from:

Indiana State University Psychology Clinic, 750 N 7th, Terre Haute, IN 47809

4. **Parties Who May Receive or Use My Individual Health Information.** The individual health information disclosed by parties listed in item 3 and information disclosed by me during the course of the research may be received and used by (list all researchers and assistants).

5. **Right to Refuse to Sign this Authorization.** I do not have to sign this Authorization. If I decide not to sign the Authorization, I may not be allowed to participate in this study or receive any research related treatment that is provided through the study. However, my decision not to sign this authorization will not affect any other treatment, payment, or enrollment in health plans or eligibility for benefits.

6. **Right to Revoke.** I can change my mind and withdraw this authorization at any time by sending a written notice to (researcher's name) to inform the researcher of my decision. If I withdraw this authorization, the researcher may only use and disclose the protected health information already collected for this research study. No further health information about me (or my child) will be collected by or disclosed to the researcher for this study.

7. **Potential for Re-disclosure.** My individual health information (and that of my child) disclosed under this authorization may be subject to re-disclosure outside the research study and no longer protected. For example, researchers in other studies could use my and my child's individual health information collected for this study without contacting me if they get approval from an Institutional Review Board (IRB) and agree to keep the information confidential.

   Also, there are other laws that may require my (or my child's) individual health information to be disclosed for public purposes. Examples include potential disclosures if required for mandated reporting of abuse or neglect, judicial proceedings, health oversight activities and public health measures.

This authorization does not have an expiration date.

I am the research participant or personal representative authorized to act on behalf of the participant.

I have read this information, and I will receive a copy of this authorization form after it is signed.

_____

Signature of research participant or research participant's personal representative Date

_____

_____

Printed name of research participant or research participant's personal representative Date

Description of personal representative authority to act behalf of the research participant:

_____

_____