CENTER FOR URBAN COMMUNITY SERVICES, INC. (CUCS)

NOTICE OF GENERAL PRIVACY PRACTICES

Effective Date: August 1st, 2009

General Privacy Policy

We at Center for Urban Community Services (CUCS) have created this General Privacy Policy to explain why we collect particular information and how we will protect your personal privacy within our website. The following information is designed to help you better understand the information we gather from our site (http://www.cucs.org/) and the dissemination practices involved. In order to fully understand your rights we encourage you to read this Privacy Policy. These policies do not pertain to other companies' or organizations' to which we link. CUCS reserves the right at any time and without notice to change this Privacy Policy. Any change will be effective immediately upon posting. By visiting this Site, you are accepting the practices described in this Privacy Policy.

Please note that this General Privacy Policy applies only to the website and is followed by a detailed Health Information Privacy Policy.

Information Collection and How We Use That Information

Our goal in collecting information is to provide you with an efficient experience that addresses your needs and is responsible with your concerns. In general our registration forms require users to give us contact information, including name, email address, format preference, address, interests and similar information. We seek such information to facilitate your donations and communicate with you about them. In addition we may use such information to improve marketing and promotional efforts as well as to improve our Site's services. We do not request and store sensitive information such as credit card and social security numbers from our visitors. Unless you specify that your gift be anonymous or name not be listed, we may list the names of the donors who give $250 or more in recognition of their generosity to our cause.

IP Address We automatically collect an IP address from all our visitors to our site. An IP address is a number that is assigned to your computer when you use the Internet. We use IP addresses to help diagnose problems with our server, administer our site, track a user's movement and analyze interests and behavior to better understand and serve you. We use such date only in the aggregate. The IP address is not linked to any personally identifiable information.

Cookies Our Site may use "cookies" which are small files placed on your hard drive to enhance your experience while on our Site. Cookies are pieces of information that each website can send to the computer that is browsing that website and are used for record keeping at many websites. You can configure your browser to accept all cookies, reject all or tell you when a cookie is set. You are always free to decline our cookies though it is possible some areas of our site will not function properly because of this.

CENTER FOR URBAN COMMUNITY SERVICES, INC. (CUCS)

NOTICE OF GENERAL PRIVACY PRACTICES

Security The security of your transactions is important to us and because of this we use up to date industry practices to safeguard your account information. We use high-grade encryption measures, which secures and guards against interception of the credit card information you give us. We also employ several security tools to protect your personal information from unauthorized access from those within and outside of the organization. However, no data transmission is "totally" or 100% secure over the Internet. While we will strive to protect your information we cannot guarantee or warrant that it will remain private.

Sharing and Usage We will never share, sell or rent individual personal information with anyone without your permission or unless ordered by the government under certain circumstances. Information submitted to us is only available to employees managing this information for purposes of contacting you or sending you emails based on your request for information and to contracted service providers for the purposes of providing services relating to our communications with you. If a user chooses to use our referral service for informing a friend about our site, we will ask for the friend's name and email address. That friend will then be sent one email inviting them to visit our Site. CUCS stores this information solely for this one time email.

How to Stop Receiving E-mail From Us Each email sent contains an easy, automated way for you to cease receiving email from us, or to change your expressed interests. If you wish to do this, simply follow the instructions at the end of any email. If this is not functioning, you can also always email cucsinfo@cucs.org to unsubscribe.

Submissions All remarks, suggestions, ideas, graphics and other information communicated to CUCS through to this Site will be the property of CUCS unless CUCS expressly states to the contrary. Further, CUCS will be entitled to use any submission for any purpose, commercial or otherwise, without compensation to you or anyone else.

Limitation of Liability CUCS and its affiliates will not be liable for any damages of injury, that result from the use or inability to use this Site and its contents.

Governing Law By your use of this Site you agree that any and all disputes relating thereto shall be governed in all respects by the laws of the State of New York. Any dispute relating to this site and Agreement shall be resolved in the state or federal courts in New York, New York.

Other Sites This Site may contain links to or from other sites that are not maintained by CUCS. CUCS does not endorse and is not responsible for the content of any unaffiliated site.

CENTER FOR URBAN COMMUNITY SERVICES, INC. (CUCS)

NOTICE OF PRIVACY PRACTICES

Effective Date: August 1st, 2009

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.

The CUCS Assertive Community Treatment (ACT) program and Intensive Wellness Program (IWP) is required by law to protect the privacy of health information that may reveal your identity and to provide you with a copy of this Notice, which describes our health information privacy practices. A copy of our current Notice will always be posted in our offices and facilities. You or your personal representative may also obtain a copy of this Notice by accessing our website at www.cucs.org or requesting a copy from our program staff. For purposes of this Notice, all references to "CUCS" mean the CUCS ACT Program and the CUCS IWP Program only. This Notice does not apply to information maintained by any other CUCS program or facility.

If you have any questions about this Notice or would like further information, please contact:

CUCS Chief Privacy Officer
198 East 121st street, 6th Floor
New York City, 10035
212-801-3300 (phone)
212-801-3325 (fax)

WHAT HEALTH INFORMATION IS PROTECTED

CUCS protects the privacy any information that identifies or could be used to identify you that relates to your health, your treatment, your case management services, or your health insurance benefits. If we obtain your name, address and other information about you in the course of providing you with health care services, this identifying information continues to be protected even if it is separated from information about your health, treatment or benefits.

HOW WE MAY USE AND DISCLOSE YOUR HEALTH INFORMATION

1. Treatment, Payment And Business Operations

Treatment. CUCS staff may use your health information without your written authorization in order to provide you with treatment or care. For example, we may share your health information

with case managers and other treatment providers at our program or *at another CUCS program*, or with Janian Medical Care (an affiliate of CUCS) who are involved in taking care of you, and they may in turn use that information to diagnose, treat, *or provide services* to you. We may also disclose your health information to others outside of CUCS without your written authorization if you have a medical emergency or in other special circumstances with the approval of our Chief Privacy Officer. For example, we may share information with a hospital emergency room if you are admitted there for emergency treatment.

Payment. We may use your health information or share it with others without your written authorization so that we may obtain payment for health care services we provide to you. For example, we may submit bills containing information about you to Medicaid in order to obtain reimbursement for our services. We may also share your information with other providers and payors for their payment activities.

Business Operations. We may use your health information or share it with others in order to conduct our business operations. For example, we may use your health information to evaluate the quality of our services or the performance of our staff in caring for you. We may also share your health information with other health care providers and payors with which you have a relationship for certain of their business operations.

Treatment Alternatives, Benefits and Services. In the course of providing treatment to you, we may use your health information to contact you in order to recommend possible treatment alternatives or health-related benefits and services that may be of interest to you.

Appointment Reminders. We may use your health information to remind you about appointments you have made to receive health care services or to encourage you to make such appointments.

2. Family And Friends

We may share your health information with family and friends involved in your care, without your written authorization. We will give you an opportunity to object unless you do not have the capacity to make decisions upon admission, in which case, we will discuss your preferences when you gain such capacity. We may also notify a family member, personal representative or another person responsible for your care about your location and general condition here at the program, or about the unfortunate event of your death. In some cases, we may need to share your information with a disaster relief organization that will help us notify these persons.

3. Emergencies Or Public Need

We may use your health information and share it with others without your written authorization in order to meet the following important public needs.

As Required By Law. We may use or disclose your health information if we are required by law to do so.

Public Health Activities. We may disclose your health information to authorized public health officials so they may carry out their public health activities. For example, we may share your health information with government officials that are responsible for controlling disease, injury or disability.

Health Oversight Activities. We may release your health information to government agencies authorized to conduct audits, investigations, and inspections of our facilities and programs.

Lawsuits And Disputes. We may disclose your health information if we are ordered to do so by a court or administrative tribunal that is handling a lawsuit or other dispute.

Law Enforcement. We may disclose your health information to law enforcement officials for certain law enforcement purposes such as: identifying or locating a suspect, fugitive or missing person; complying with a court order, subpoena or administrative request; providing information about a victim of a crime; or reporting a death that may be the result of a crime.

To Avert a Serious and Imminent Threat to Health or Safety. We may use your health information or share it with others when necessary to prevent a serious and imminent threat to your health or safety, or the health or safety of another person or the public.

National Security and Intelligence Activities or Protective Services. We may disclose your health information to authorized federal officials who are conducting military, national security and intelligence activities or providing protective services to the President or other important officials.

Inmates and Correctional Institutions. If you become incarcerated at a correctional institution or detained by a law enforcement officer, we may disclose your health information to prison officials or law enforcement officers if necessary to provide you with health care, or to maintain safety, security and good order at the place where you are confined.

Coroners, Medical Examiners and Funeral Directors. In the unfortunate event of your death, we may disclose your health information to a coroner or medical examiner. We may also release this information to funeral directors as necessary to carry out their duties.

Organ and Tissue Donation. In the unfortunate event of your death, we may disclose your health information to organizations that procure or store organs, eyes or other tissues.

Research. We may use and disclose your health information for research purposes if we obtain approval through a special process to ensure that research without your written authorization poses minimal risk to your privacy. Under no circumstances will we allow researchers to use your name or identity publicly. We may also release your health information to people who are preparing a future research project, so long as any information identifying you does not leave our facility. In the unfortunate event of your death, we may share your health information with people who are conducting research using the information of deceased persons, as long as they agree not to remove from our facility any information that identifies you.

4. Special Treatment of Sensitive Information

The policies and practices described above do not always apply to certain types of sensitive health information that is subject to special protection under the law. We will disclose this information to others without your permission only for the following purposes.

HIV-Related Information. We will not disclose any information related to HIV or AIDS without your written authorization, except (i) for purposes of obtaining payment for our services or carrying out our business operations, (ii) in connection with organ or tissue donation and transplantation, (iii) to accreditation and oversight bodies, (iv) to a government agency as required by law, (v) in response to a court order, (vi) to the medical director of a correctional facility, (vii) to the Commission of Corrections for health oversight purposes, (viii) to funeral directors to enable them to carry out their duties or (ix) for treatment purposes as otherwise permitted by this Notice.

Mental Health Records. We will not disclose any information maintained by one of our mental health programs without your written authorization, except (i) pursuant to a court order, (ii) to the Mental Hygiene Legal Service, (iii) to your attorney in an involuntary hospitalization proceeding, (iv) to the Commission on the Quality of Care for the Mentally Disabled, (v) to the medical review board of the State Commission of Corrections for its official duties, (vi) to an "endangered individual" or law enforcement agency when a treating psychiatrist or psychologist determines that a client presents a "serious and imminent danger" to the individual, (vii) to the State Board for Professional Medical Conduct or the Office of Professional Discipline for its official duties, (viii) to agencies seeking to locate missing persons or conduct criminal investigations, (ix) to researchers operating under IRB approval if certain safeguards are in place, (x) to a coroner or medical examiner investigating a client's death, (xi) to the district attorney investigating client abuse, (xi) to a correctional facility or the Division of Parole, (xii) to a director of community services under the Mental Hygiene Law, (xiii) to the State Division of Criminal Justice Services for certain evaluative purposes, (xiv) for purposes of obtaining payment for our services or carrying out our business operations or (xv) for treatment purposes as otherwise permitted by this Notice.

Alcohol and Substance Abuse Treatment Records. The records of federally assisted alcohol and substance abuse treatment programs is governed by 42 C.F.R. Part 2. We will not disclose the records of federally assisted alcohol and substance abuse treatment programs in which you have received services without your written authorization, except (i) to medical personnel to provide emergency treatment to you, (ii) to medical personnel of the Food and Drug Administration for the purpose of identifying potentially dangerous products, (iii) for research purposes if certain safeguards are in place, (iv) to authorized individuals or organizations conducting on-site audits of our records as long as the individual or organization does not remove the information from our premises and agrees in writing to safeguard the information as required by federal regulations or (v) in response to a court order.

5. Business Associates

We may share PHI with a Business Associate (BA) who requires access to PHI in order to fulfill its contracted function and with whom we have a formal HIPAA Business Associate Agreement. The BA is required to treat the PHI with the same privacy and security protection as we would ourselves.

6. Obtaining Your Written Authorization.

We will not use your health information or share it with others for any purpose not listed in this Notice without your written authorization. If you give us your authorization, you may revoke it at any time, in which case we will no longer use or disclose your health information for that purpose, except to the extent we have already relied on the authorization. We will not deny you treatment if you refuse to sign an authorization unless the treatment is part of a research study or is being provided for the sole purpose of creating information for disclosure to a third party.

YOUR RIGHTS TO ACCESS AND CONTROL YOUR HEALTH INFORMATION

You have the following rights regarding your health information. Any requests regarding these rights should be submitted in writing to CUCS' Chief Privacy Officer.

1. Right to Inspect and Copy Records

You have the right to inspect and obtain a copy your medical and billing records. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies we use to fulfill your request. The standard fee is $0.75 per page and must generally be paid before or at the time we give the copies to you. We will provide the information electronically at your request if the information is held electronically. Under certain very limited circumstances, we may deny your request to inspect or obtain a copy of your information.

2. Right to Amend Records

If you believe that the health information we have about you is incorrect or incomplete, you may ask us to amend the information. Your request should include the reasons why you think we should make the amendment. We may deny your request if we believe our information is accurate or complete or for other limited reasons.

3. Right To An Accounting Of Disclosures

You have a right to request an "accounting of disclosures," which identifies certain disclosures we have made of your health information. Your request must state a time period within the past six years for the disclosures you want us to include. You have a right to receive one accounting within every 12-month period for free. However, we may charge you for the cost of providing any additional accounting in that same 12-month period.

4. Right to Request Additional Privacy Protections

You have the right to request that we further restrict the way we use and disclose your health information to provide you with treatment or care, collect payment for that treatment or care, or run our business operations. You may also request that we limit how we disclose information about you to family or friends involved in your care. We do not have to agree to all requests.

You have the right to a restriction to disclosure of PHI to a health plan for payment if the you have paid in full for the services and items provided in that visit.

5. **Right To Request Confidential Communications**

You have the right to request that we communicate with you or your personal representative by alternative means or at alternative locations. We will not ask you the reason for your request and we will try to accommodate all reasonable requests.

NOTIFICATION IN THE CASE OF A BREACH:

CUCS is required by law to notify our clients in case of a breach of their unsecured protected health information when it has been or is reasonably believed to have been accessed, acquired or disclosed as a result of a breach.

WHO MAY EXERCISE YOUR RIGHTS

If you have the capacity to make your own health care decisions under the law, you will generally exercise your own rights under this Notice. If you do not have such capacity, your legal guardian or any other person who has the right to make health care decisions on your behalf (for example, based on a health care proxy you have signed) may exercise your rights. This person is called your "personal representative." In addition to exercising your rights under this Notice, your personal representative may also sign any authorizations or give any other approvals required by this Notice on your behalf.

OTHER IMPORTANT INFORMATION

How To Obtain A Copy Of This Notice. You have the right to a paper copy of this Notice. You may request a paper copy at any time, even if you have previously agreed to receive this notice electronically. To do so, please request it from the CUCS Program Director. You or your personal representative may also obtain a copy of this Notice from our website at www.cucs.org, or by requesting a copy from our program staff.

How to Obtain a Copy of a Revised Notice. We may change our privacy practices from time to time. If we do, we will revise this Notice. The revised notice will apply to all of your health information. We will post any revised notice at our offices and facilities. You or your personal representative will also be able to obtain your own copy of the revised notice by accessing our website at www.cucs.org or requesting a copy from our program staff. We are required to abide by the terms of the Notice that is currently in effect.

How To File A Complaint. If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the Department of Health and Human Services (HHS). To file a complaint with HHS, you may contact them at 200 Independence Avenue, SW, Washington, D.C. 20201, or at 1-877-696-6775. In addition, the Federal Center for Deaf and Hearing Impaired can be contacted at 1-800-877-8339. To file a complaint with us, please contact CUCS' Chief Privacy Officer. *No one will retaliate or take action against you for filing a complaint.*

ACKNOWLEDGMENT

By signing below, I acknowledge that I have been provided a copy of this Notice of Privacy Practices and have therefore been advised of how health information about me may be used and disclosed by the program and the facilities listed at the beginning of this notice, and how I may obtain access to and control this information. I also acknowledge and understand that I may request copies of separate notices explaining special privacy protections that apply to HIV-related information, alcohol and substance abuse treatment information, mental health information, and genetic information.

_____

Signature of Service Recipient or Personal Representative

_____

Print Name of Service Recipient or Personal Representative

_____

Date

_____

Description of Personal Representative's Authority

80451809.2

CENTER FOR URBAN COMMUNITY SERVICES, INC. (CUCS)
& JANIAN MEDICAL CARE P.C.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION POLICY

Effective Date: August 1, 2009

SCOPE OF POLICY

This policy applies to all CUCS staff members and health care professionals providing care at CUCS service programs. Staff members include all employees, social work or other students, trainees, interns, volunteers, consultants, contractors and subcontractors at CUCS service programs. Health care professionals include physicians, allied health professionals and other licensed health care professionals providing treatment or care to service recipients, regardless of whether they are employees. The CUCS Chief Privacy Officer is responsible for overseeing compliance with this policy.

STATEMENT OF POLICY

CUCS is committed to protecting the privacy and confidentiality of health information about its service recipients. "Protected health information" (as defined below) is strictly confidential and should be used and disclosed only for those purposes authorized under CUCS' policies and applicable law.

All CUCS programs covered by this policy are subject to Section 33.13 of the New York Mental Hygiene Law and Article 27-F of the New York Public Health Law (with respect to HIV-related information). In addition, the CUCS ACT program is subject to the privacy rule issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The most stringent requirements of these laws and regulations are reflected in this policy.

IMPLEMENTATION OF POLICY

This policy applies to protected health information in any form, including spoken, written or electronic form. It applies to both internal "uses" of protected health information within CUCS and external "disclosures" of such information by CUCS to others.

A. Protected Health Information

For purposes of this policy, the term "protected health information" means any service recipient information that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual. Some examples of protected health information are:

- information about the service recipient's health condition (such as a psychiatric diagnosis, or a medical disease);
- information about health care services the service recipient has received or may receive in the future (such as therapy with a mental health professional, or an operation);

- information about the service recipient's health care benefits under an insurance plan (such as whether a prescription is covered); and
- information about whether a service recipient is receiving health care services from our service program or any other health care provider;

when combined with:

- demographic information (such as the service recipient's name, address, race, gender, ethnicity or marital status);
- geographic information (such as where the service recipient works);
- unique numbers that may identify the service recipient (such as a social security number, case record number, telephone number, or driver's license number); or
- other types of information that may identify who the service recipient is.

Basic demographic data such as age and address remains protected even if separated from the health information to which it relates. Employees may not identify an individual as a service recipient upon inquiry from a third party except as permitted by this policy.

It is the responsibility of every CUCS staff member to preserve the privacy and confidentiality of all protected health information and to ensure that protected health information is used and disclosed only as permitted under the service program's policies and applicable law. This includes, but is not limited to, compliance with the protective procedures below.

B. **Routine Disclosures**

CUCS Staff: For all routine disclosures, other then what is described in sections C through section H, CUCS staff should not disclose information without having first obtained a properly executed *Authorization to Disclose Information to/from* form. (see *Guidelines to Filling out the Authorization form* available in folder #5 of the Policy and Procedure Manual)

Janian Medical Care P.C. :

- For routine disclosures of PHI for treatment purposes to another provider, other then for HIV information and what is described in sections C through section H, Janian Medical Care P.C. providers are required to have at least verbal consent or implied consent from the patient[1].
- All routine disclosures to non-providers require a properly executed *Authorization to Disclose Information to/from* form.
- All routine disclosures containing HIV information require a properly executed *Authorization to Disclose Information to/from* form indicating that HIV information is permitted to be disclosed.

C. Treatment Purposes

Protected health information may be used internally by CUCS employees for treatment purposes without the service recipient's authorization.

[1] The requirement for verbal or implied consent is based on Section 6530 paragraph 23 of the education law that says it is professional misconduct to "Reveal personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law".

Protected health information may be shared between CUCS employees and Janian Medical employees for treatment purposes without the service recipient's authorization.

Protected health information may be disclosed by CUCS for treatment purposes **without the service recipient's authorization** to:

- a **mobile crisis team**,
- the service recipient's **AOT provider**,
- **Adult Protective Services**

If a disclosure is made for this purposes without an authorization, the employee making the disclosure must document in the client's record (i) his or her name, (ii) the name of the person and facility receiving the information, (iii) the date and time of the disclosure and (iv) the nature of the treatment purpose.

Protected health information may be disclosed by CUCS staff to other outside providers or agencies for treatment purposes without the service recipient's authorization:

- **in medical/psychiatric emergencies, or**
- **with the approval of the Chief Privacy Officer**.

If a disclosure is made for this purpose without an authorization, the employee making the disclosure must document in the client's record (i) his or her name, (ii) the name of the person and facility receiving the information, (iii) the date and time of the disclosure and (iv) the nature of the emergency.

For purposes of this policy, the term "treatment" means providing, coordinating or managing the service recipient's health/mental health care and any related services. Some examples of treatment activities involving the use or disclosure of protected health information are:

- using protected health information about a service recipient's disease or condition to diagnose or provide care to the service recipient;
- disclosures of protected health information to other health care providers who are involved in taking care of the service recipient;
- disclosures of protected health information to another health care provider in order to obtain advice about how best to diagnose or provide care to the service recipient; and
- disclosures of protected health information to another health care provider to whom the service recipient has been referred to ensure that this health care provider has the necessary information to diagnose or provide care to the service recipient.

D. Payment

Protected health information may be used or disclosed by CUCS employees, or Janian Medical employees for payment purposes without the service recipient's authorization.

For purposes of this policy, the term "payment" generally means the activities undertaken by CUCS to obtain or provide reimbursement for the provision of health care. Some examples of payment activities involving the use or disclosure of protected health information are:

- disclosing the service recipient's protected health information to a health insurance plan to determine whether it will provide coverage for the service recipient's treatment;
- disclosing the service recipient's protected health information to obtain pre-approval before admitting the service recipient to the service program; and
- disclosing the service recipient's protected health information to his or her health insurance plan to obtain reimbursement after the service program has treated the service recipient.

CUCS or Janian Medical may disclose information to a Funding agency if the disclosure is mandated in our contract, standards, regulations or funder guidelines which must be followed as a condition of payment.

Several examples:

- CUCS is required to follow the standards set forth in the "HASA Housing Program Desk Guide" which mandate certain disclosures between CUCS and HASA. Disclosures of this nature may be disclosed only with the approval of the Chief Privacy Officer.
- CUCS is required to input certain information which may include protected health information about the participants in the 350 Lafayette Transitional Living Community program through the DHS CARES system.
- CUCS is obligated to report information to the Homeless Management Information System (HMIS) for HUD funded programs.

Uses and disclosures of protected health information for the service program's payment purposes are subject to the **CUCS' Policy – Minimum Necessary Standard**.

E. Health Care Operations

Protected health information may be used by CUCS employees or Janian Medical employees for CUCS' health care operations without the service recipient's authorization. Protected health information may be disclosed for health care operations only with the approval of the Chief Privacy Officer.

For purposes of this policy, the term "health care operations" generally refers to those general business and administrative functions of CUCS that are required in order to operate and perform its health care functions. Some examples of uses and disclosures of protected health information for health care operations are:

- uses and disclosures of protected health information for quality assurance and utilization review purposes;
- uses and disclosures of protected health information for education and training of students or other trainees;
- uses and disclosures of protected health information to recommend possible treatment options or alternatives, or health-related benefits or services, that may be of interest to the

service recipient;
- uses and disclosures of protected health information for legal services, business planning, and other business management and general administrative activities; and
- uses and disclosures of basic demographic information to raise funds for the benefit of the service program.

Uses of protected health information for the service program's health care operations are subject to the HIPAA Privacy Regulations' minimum necessary standard, as defined in **CUCS' Policy – Minimum Necessary Standard**.

F. Child Abuse Reporting

Protected health information may be disclosed by CUCS or Janian Medical to the NYC Administration for Children's Services for the purpose of making a report of an incident/s, or suspected incident/s, of child abuse, neglect or maltreatment without the service recipient's authorization in accordance with applicable law if the PHI is relevant to the report.

G. Other Purposes with Chief Privacy Officer Permission

The Chief Privacy Officer may approve the disclosure of protected health information without the client's authorization for any of the following purposes:

- Pursuant to a court order signed by a judge.
- To the Mental Hygiene Legal Service for programs other than ACT.
- To a client's attorney in an involuntary hospitalization proceeding.
- To the Commission on the Quality of Care for the Mentally Disabled.
- To the medical review board of the State Commission of Corrections for its official duties.
- To an "endangered individual" or law enforcement agency when a treating psychiatrist or psychologist determines that a client presents a "serious and imminent danger" to the individual. *(Tarasoff)*
- To the State Board for Professional Medical Conduct or the Office of Professional Discipline for its official duties.
- To law enforcement agencies seeking to locate missing persons or conduct criminal investigations but such information to be limited to dates of residence in our facility.
- To researchers operating under an IRB approval that includes a waiver of patient authorization for the release of protected health information.
- To a coroner or medical examiner investigating a client's death.
- To appropriate persons and entities when necessary to prevent "imminent serious harm" to the client or another person.
- To the district attorney investigating client abuse if certain conditions are satisfied.
- To a correctional facility or the Division of Parole. The disclosure must be limited to summary information specified in the statute. No disclosures to the Division of Parole are permitted by the ACT Program.
- To a director of community services under the Mental Hygiene Law.
- To the State Division of Criminal Justice Services for certain evaluative purposes.

Notwithstanding the foregoing, the disclosure of HIV-related information may be subject to additional restrictions. The Chief Privacy Officer shall determine whether any proposed disclosures of HIV-related information are permitted under Article 27-F of the New York Public Health Law.

H. Agreements with Recipients of Protected Health Information

No person or entity (other than a CUCS employee) may receive protected health information for the purpose of assisting the CUCS ACT Program in carrying out payment or health care operations unless the person or entity has entered into a Business Associate Agreement with CUCS. This requirement applies to, among others, billing companies, quality assurance consultants, attorneys, accountants and software maintenance vendors. A Business Associate Agreement is not required for disclosures that are made for treatment purposes or with the client's authorization. A Business Associate Agreement is not required for disclosures made by CUCS programs other than ACT.

The Chief Privacy Officer maintains CUCS' standard Business Associate Agreement. Any modifications of the standard agreement must be approved by the Chief Privacy Officer.

I. Authorization Forms

Employees should use only the standard authorization form, which is maintained by the Chief Privacy Officer and available in the Policy and Procedure manual and in Anasazi. Reliance on any other authorization form, including a form provided by an outside person or entity, must be approved by the Chief Privacy Officer.

J. De-identified Information Not Subject to Restrictions

Protected health information is considered "de-identified" when all elements that have the potential to identify the service recipient have been removed. Protected health information will be deemed de-identified when (i) a person with appropriate knowledge and experience in scientific and statistical principles for de-identifying information has determined that there is a very small risk that that the information can be used to identify the service recipient and has documented the analysis that justifies that decision, or (ii) certain specific identifying elements regarding the service recipient and his or her relatives, employers and household members have been removed and the remaining information cannot be used to identify the service recipient.

The elements that must be removed include the following:

- names;
- all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geocodes;
- all elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements (including year) indicative of such age, except that ages and elements may be aggregated into a single category of 90 or older;
- telephone numbers;
- fax numbers;

- electronic mail (e-mail) addresses;
- Social Security numbers;
- case record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- World Wide Web Universal Resource Locators (URLs);
- internet protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints;
- full face photographic images and comparable images; and
- any other unique identifying number, characteristic or code.

Because de-identified information is no longer considered protected health information, such de-identified information is not subject to the restrictions set forth in this policy and generally may be used and disclosed without limitation. However, CUCS staff must obtain approval from the Chief Privacy Officer that protected health information has been appropriately de-identified prior to treating such information as de-identified information.

K. Uses of Protected Health Information for Other Reasons

Service program staff are instructed to consult their program director or assistant program director if they are unsure whether a particular use or disclosure is permitted by this policy.

L. Retention of Protected Health Information

We retained all records which include PHI, electronic and paper, as mandated by applicable laws, regulations and contracts. Please see our *Record Retention Policy* for full details.

We require hard copy client case records to be disposed of through means such as cross cut shredding or pulverizing. See the policy *Procedures for Removal of EPHIi from Hardware and Media prior to Disposal* for details on disposal of electronic client records.

VIOLATIONS

CUCS' Chief Privacy Officer has general responsibility for implementation of this policy. CUCS staff members who violate this policy will be subject to disciplinary action up to and including termination of employment. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or CUCS' Chief Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, CUCS will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.

QUESTIONS

If you have questions about this policy, please contact your department supervisor or CUCS' Chief Privacy Officer immediately. It is important that all questions be resolved as soon as possible to ensure protected health information is used and disclosed appropriately.

80452991.2

CENTER FOR URBAN COMMUNITY SERVICES, INC. (CUCS)

CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

Effective Date: April 28, 2005

SCOPE OF POLICY

This policy applies to all CUCS and Janian Medical Care P.C. staff members and health care professionals providing care at CUCS service programs. Staff members include all employees, social work or other students, trainees, interns, volunteers, consultants, contractors and subcontractors at CUCS service programs. Health care professionals include physicians, allied health professionals and other licensed health care professionals providing treatment or care to service recipients, regardless of whether they are employees.

STATEMENT OF POLICY

CUCS is committed to protecting the privacy and confidentiality of health information about its service recipients. Protected health information is strictly confidential and should never be given, nor confirmed, to anyone who is not authorized under CUCS' policies or applicable law to receive this information.

CUCS' policies regarding minimum necessary standards is closely related to, and must be followed along with, this policy.

All staff members and other health care professionals providing care at CUCS service programs should be aware that special privacy protections apply to HIV-related information, alcohol and substance abuse information, and mental health information. Some activities which are permitted under this policy may not be permitted when using or disclosing these types of information. Staff and health care professionals providing care at CUCS service programs must comply with CUCS' policies on privacy and confidentiality of HIV-related information, alcohol and substance abuse information, and mental health information when using or disclosing these sensitive types of information for any reason. They are expected to be aware of the requirements under those policies.

IMPLEMENTATION OF POLICY

A. Definition of Protected Health Information

For purposes of this policy, the term "protected health information" means any information that (1) relates to the past, present, or future physical or mental health or condition of a service recipient, the provision of health care to the service recipient, or the past, present, or future payment for the provision of health care to the service recipient, and (2) either identifies the service recipient or could reasonably be used to identify the service recipient. Protected health information includes basic demographic information about service recipients maintained by CUCS, such as name and address, even if unaccompanied by health information.

This policy applies to protected health information in any form, including spoken, written, or electronic form. It is the responsibility of every staff member and health care professional to protect the privacy and preserve the confidentiality of all protected health information. This includes, but is not limited to, compliance with the protective procedures below.

B. Public Viewing/Hearing

Staff and health care professionals providing care at CUCS service programs are expected to keep protected health information out of public viewing and hearing. For example, protected health information should not be left in conference rooms, or on counters or other areas where the information may be accessible to the public or to other employees or individuals who do not have a need to know the protected health information. At the end of each day, employees should place any documents containing protected health information in locked drawers or file cabinets, and should not leave such documents on their desks or otherwise in plain view. Staff and health care professionals providing care at CUCS service programs should also refrain from discussing protected health information in public areas, such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more service recipients, in which case, every effort should be made to speak quietly and discretely.

Fax machines and printers shall be kept in secure areas to minimize the opportunity for unauthorized exposure.

Staff and health care professionals should also take care in sharing protected health information with families and friends of service recipients. Such information may generally only be shared with a personal representative of the service recipient in accordance with CUCS policy, or with a family member, relative, or close personal friend who is involved in the service recipient's care or payment for that care. Even in the latter circumstance, information cannot be disclosed unless the service recipient has had an opportunity to agree or object to the disclosure, and staff and health care professionals may only disclose information that is relevant to the involvement of that family member, relative or close personal friend in the service recipient's care or payment for the service recipient's care, as the case may be. Notwithstanding the foregoing, any HIV-related information, alcohol or drug abuse treatment records or mental health records may be disclosed only to a service recipient's personal representative (and not to other family members or friends) unless the service recipient provides written authorization for the disclosure.

C. Databases and Workstations

Staff and health care professionals providing care at CUCS service programs are expected to ensure that they exit Anasazi, any other confidential database, and any CUCS network upon leaving their work stations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. Staff and health care professionals providing care at the service program are expressly forbidden from saving files on their local hard drives that include protected health information or loading protected health information onto laptops that are removed from CUCS facilities. Staff and health care professionals are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including but not limited to, any password, personal identification number, token or access card, or electronic signature. Each staff member and health care professional will be liable for all activity occurring under his or her account, password and/or electronic signature. These activities may be monitored.

D. Downloading, Copying or Removing

Staff and health care professionals providing care at CUCS service programs should not download, copy or remove from the service program any protected health information, except as necessary to perform their duties at the service program and in accordance with protocols adopted by their supervisor.

If records are being transmitted from one location to another, they must be placed in sealed envelopes and a receipt shall be obtained documenting the delivery of said records.

Any downloads or copies should be deleted or destroyed upon return to the office or as soon as feasible. Upon termination of employment or contract with the service program, or upon termination of authorization to access protected health information, staff members and health care professionals must return to the service program any and all copies of protected health information in their possession or under their control.

E. Emailing and Faxing Information

CUCS staff may transmit protected health information to e-mail addresses in the cucs.org domain. Staff and health care professionals should not transmit protected health information over the Internet and other unsecured networks unless using a secure encryption procedure, or unless there is a particular exemption for email type or email recipient (see *Procedures for Encryption of Data Moved Over the Internet* for information on exemptions) Transmission of protected health information is permitted by fax only if the staff member or health care professional sending the information ensures that the intended recipient is available to receive the fax as it arrives, or confirms that there is a dedicated fax machine that is monitored for transmission of sensitive information. Staff and health care professionals providing care at CUCS service programs should use fax cover sheets that include standard confidentiality notices, and should request that the recipient call back upon receipt of the fax.

F. Shredding

Paper documents containing protected health information will be disposed of by cross cut shredding or pulverizing on a daily basis or through use of a vendor. If documents are shredded on-site, the shredding must be conducted by an authorized employee. If shredded off-site by a vendor, the vendor must provide a certificate of destruction verifying that all materials have been totally destroyed.

G. Incident Reporting

If an employee becomes aware of any privacy-related breach, violation or problem, the employee should promptly notify the Chief Privacy Officer. The Chief Privacy Officer will be responsible for investigating the report and coordinating corrective action if appropriate.

VIOLATIONS

CUCS' Chief Privacy Officer has general responsibility for implementation of this policy. Staff and health care professionals who violate this policy will be subject to disciplinary action up to and including termination of employment or contract. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or CUCS' Chief Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, CUCS will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract.

QUESTIONS

If you have questions about this policy, please contact your supervisor or CUCS' Chief Privacy Officer immediately. It is important that all questions be resolved as soon as possible to ensure protected health information is used and disclosed appropriately.

CENTER FOR URBAN COMMUNITY SERVICES

MINIMUM NECESSARY STANDARD POLICY

Introduction

All CUCS staff and health care professionals providing care at CUCS programs are generally expected to limit their uses and disclosures of protected health information, and requests for protected health information, to the minimum amount of information necessary to perform their duties at CUCS programs. This general expectation does not mean that CUCS staff and health care professionals should restrict exchanges of information required in order to treat service recipients quickly and effectively.

Policy

This policy, effective as of October 1, 2003, applies to all CUCS staff members and health care professionals providing care to service recipients at CUCS programs. Staff members include all employees, social work or other students, trainees, interns, volunteers, consultants, contractors and subcontractors at CUCS programs. Health care professionals include physicians, allied health professionals and other licensed health care professionals providing treatment or care to service recipients in CUCS programs, regardless of whether they are employees.

Please note: This minimum necessary policy is an integral part of CUCS' general policy on confidentiality of protected health information.

Procedure

Routine Activities

Members of CUCS' staff or health care professionals providing treatment to CUCS service recipients, routinely use protected health information about service recipients to carry out work related duties. Staff and health care professionals may also need to disclose protected health information about service recipients to persons outside CUCS programs or to request protected health information from these persons. CUCS and individual programs have specific policies and procedures explaining how much information may be used, disclosed or requested in situations that occur on a routine basis. Staff members are expected to know and follow these policies at all times. These policies have been carefully developed and are not intended to limit any communications required for CUCS staff and health care professionals to provide quick, effective and high quality health care. Questions regarding how these policies should be applied in a particular situation should be directed to Program Supervisors or CUCS' Chief Privacy Officer.

Non-Routine Situations
CUCS' agency and program policies are general policies that address routine activities. If the general policies and procedures do not address a particular situation or do not permit staff members to use, disclose, or request protected health information in a way that is necessary to carry out work related duties, staff and health care professionals should notify the appropriate Program Supervisor. Supervisors are responsible for providing guidance or directing staff to the appropriate department or individual to address the situation. When necessary, supervisors consult with CUCS' Chief Privacy Officer to determine how much information may be used, disclosed, or requested. Individual CUCS staff members and health care professionals providing care at CUCS programs should not make decisions on their own if the situation is not covered in CUCS' policies or procedures or in their specific program's policies and procedures. See the CUCS Minimum Necessary Standard in Non-Routine Situations policy, included herein, for additional information.

Violations of this Policy

CUCS' Chief Privacy Officer has general responsibility for implementation of this policy. CUCS staff and health care professionals who violate this policy will be subject to disciplinary action up to and including termination of employment or contract. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or CUCS' Chief Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, CUCS will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract.

Questions Regarding this Policy

If you have questions about this policy, please contact your supervisor or CUCS' Chief Privacy Officer immediately. It is important that all questions be resolved as soon as possible to ensure that protected health information is used appropriately.

CENTER FOR URBAN COMMUNITY SERVICES

MINIMUM NECESSARY STANDARD IN NON-ROUTINE SITUATIONS

Introduction

Staff and health care professionals at all CUCS service programs routinely use protected health information about service recipients to carry out their job related duties. CUCS staff and health care professionals may also need to disclose protected health information about service recipients to persons outside CUCS service programs or to request protected health information (PHI) from outside sources. CUCS has policies and procedures and each program also has specific policies and procedures governing the use of such information, including how much information may be used, disclosed or requested to carry out routine duties, and who may disclose such information.

The minimum necessary standard only applies to requests that seek protected health information from another *covered entity*. However, CUCS recommends that covered entities require that CUCS staff and health care professionals comply with the minimum necessary standard when making any requests for protected health information, whether or not from a covered entity. This approach will relieve staff members of the additional burden of having to identify whether the party from whom the information is requested is a covered entity.

Policy

This policy, effective as of October 1, 2003, applies to all supervisors, administrators, managers and CUCS' Chief Privacy Officer. These persons are expected to help ensure that all CUCS staff members and health care professionals providing care to service recipients at CUCS service programs limit their uses and disclosures of protected health information, and keep requests for protected health information, to the minimum amount of information necessary to accomplish their respective service related duties. Supervisors, administrators and managers are expected to ensure that these policies and procedures are followed by the members of their respective programs.

In addition, supervisors, administrators and managers are expected to adhere to this policy, which outlines the use and disclosure of PHI in non-routine situations. This should be followed when a CUCS staff member or health care professional believes that PHI must be used, disclosed or requested in a way that is not covered by CUCS' agency or program policies and procedures addressing routine situations.

Procedure

Uses of Protected Health Information
CUCS staff and health care professionals providing care at CUCS service programs are instructed to notify their supervisors, administrators or managers or the CUCS Chief Privacy Officer if they believe they need to *use* protected health information in a way that is not addressed by CUCS' agency or program policies and procedures. The supervisors, administrators or managers will be responsible for providing guidance or directing the individual to the appropriate department or individual better able to provide the necessary guidance.

If necessary, the supervisor, administrator or manager should consult with CUCS' Chief Privacy Officer to determine how much information may be accessed and used to appropriately address the situation, and by whom. If there is insufficient time to consult with the Chief Privacy Officer without jeopardizing service recipient care, the supervisor, administrator or manager may make this determination on his or her own and notify the Chief Privacy Officer as soon as possible afterwards.

Disclosures of and Requests for Protected Health Information
CUCS staff and health care professionals providing care at CUCS service programs are instructed to contact their supervisors, administrators or managers or the Chief Privacy Officer if they believe they need to *disclose* or *request* protected health information in a way that is not addressed by CUCS' agency policies and procedures or those of their respective programs. The supervisor, administrator, or manager will be responsible for providing guidance or directing the individual to the appropriate department or individual better able to provide the necessary guidance.

If necessary, the supervisor, administrator or manager should attempt to contact CUCS' Chief Privacy Officer. The Chief Privacy Officer should then determine what information may be disclosed or requested according to the following procedures. If there is insufficient time to consult with the Chief Privacy Officer without jeopardizing service recipient care, the supervisor, administrator or manager may make this determination on his or her own and notify the Chief Privacy Officer as soon as possible afterwards.

Many disclosures to persons outside CUCS service programs or requests for information from persons outside CUCS service programs will require a written authorization from the service recipient whose protected health information is involved. This policy discusses only how much information may be disclosed or requested and does not discuss when such authorizations are required.

Disclosures in Response to Requests from Selected Persons
When the following persons or organizations are making a request, the Chief Privacy Officer (or supervisor, administrator or manager) may disclose the protected health information without questioning the request or limiting the amount of information released:

- All professionals within CUCS.[1]
- Business associates of CUCS.[2]
- A health care provider that is required to comply with federal privacy regulations.
- A health plan that provides or pays the cost of medical care and is required to comply with federal privacy regulations.

- A health care clearinghouse that converts health information to and from standard and non-standard formats and is required to comply with federal privacy regulations.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board that meets the requirements of CUCS' policy on uses and disclosures of protected health information for research purposes.
- A public official or agency requesting protected health information for a public policy purpose that is explained in CUCS' policy on disclosures of protected health information for public policy purposes.

If the Chief Privacy Officer (or supervisor, administrator or manager) strongly believes that a request by one of the foregoing persons or organizations seeks more than the minimum information necessary, he or she should attempt to reach a compromise that meets the concerns and needs of both CUCS service programs and the person or organization making the request.

Disclosures in Response to All Other Requests

If the request is made by any other person or organization, the Chief Privacy Officer (or supervisor, administrator or manager) should decide how much information to disclose, using the following criteria:

- What is the *purpose* of the disclosure?
- What *type* of information does the recipient need to accomplish the purpose of the disclosure?
- Where is this information *located*? For example, is it in an X-ray? Is it in a case record? Is it on an electronic database?
- Is other information *attached* to this information? If so, is the attached information also needed to accomplish the purpose of the disclosure? If the attached information is not needed, a copy of the record should be made and the extraneous information should be redacted (whether electronically or by manually blacking out the information on the hard copy).

Requests for Protected Health Information from Others

When deciding what information may be requested from another person or organization outside CUCS, the Chief Privacy Officer (or supervisor, administrator or manager) should consider the following criteria:

- What is the *purpose* of the request?
- What *type* of information do CUCS' service programs need to accomplish this purpose (this may require consultation with the supervisor, administrator or manager)?
- What other information is likely to be *attached* to the information CUCS' service program is requesting? *If that information is not needed, the Chief Privacy Officer should specify in the request that this information need not be disclosed.*
- Can the request be phrased more *narrowly* to target only the information needed by CUCS' service program to accomplish this purpose?

Special Procedures for Using, Disclosing or Requesting the Entire Case record

CUCS staff and health care professionals providing care at CUCS service programs are instructed to contact their supervisors, administrators or managers or the Chief Privacy Officer if they believe that the entire case record should be used, disclosed or requested in a way not covered by CUCS' or their program's policies and procedures. The supervisor, administrator or manager will be responsible for consulting with CUCS' Chief Privacy Officer to determine whether there is a specific justification for using, disclosing or requesting the entire case record. If there is insufficient time to consult with the Chief Privacy Officer without jeopardizing service recipient care, the supervisor, administrator or manager may make this determination on his or her own and notify the Chief Privacy Officer as soon as possible afterwards. The specific justification for using, disclosing or requesting the entire case record should always be documented in the service recipient's case record.[3]

Special Requirements for Using, Disclosing or Requesting Certain Types of Information
CUCS staff and health care professionals providing care at CUCS service programs are advised that special concerns are raised when using, disclosing or requesting certain types of information, particularly alcohol and substance abuse treatment information, mental health information and HIV-related information. Specific program policies addressing these types of information should be consulted when these types of information are involved.

Exceptions
The following uses, disclosures and requests are not limited by the minimum necessary standard. The Chief Privacy Officer (and supervisor, administrator or manager) nevertheless should do his/her best to limit the amount of information used, disclosed or requested in these situations to what is appropriate under current social service, medical and ethical guidelines.

- ***Requesting*** service recipient information from, or ***disclosing*** service recipient information to, another health care provider for treatment purposes.
- ***Disclosing*** service recipient information to the service recipient, or to a personal representative who is authorized to make health care decisions for the service recipient or to administer a deceased service recipient's estate.
- ***Using*** or ***disclosing*** service recipient information pursuant to a service recipient's written authorization.
- ***Disclosing*** protected health information required by the Department of Health and Human Services (HHS) in connection with its investigation or determination of CUCS' compliance with the HIPAA privacy regulations.
- ***Using*** or ***disclosing*** protected health information as required by law (not just using or disclosing protected health information in a manner that is permitted by law).
- ***Using*** or ***disclosing*** protected health information in order to complete standard electronic transactions using standard transaction formats as required by HIPAA.[42]
- ***Incidental uses*** or ***disclosures*** of protected health information that occur in the course of other permitted uses or disclosures of protected health information.[5]

Violations of this Policy

CUCS' Chief Privacy Officer has general responsibility for implementation of this policy. CUCS staff and health care professionals who violate this policy will be subject to disciplinary action up to and including termination of employment or contract.[6] Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor, administrator or manager or CUCS' Chief Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, CUCS will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract.

Questions Regarding this Policy

If you have questions about this policy, please contact your supervisor or CUCS' Chief Privacy Officer immediately. It is important that all questions be resolved as soon as possible to ensure that protected health information is used appropriately.

---

1 The Privacy Rule permits a covered entity to rely upon requests for protected health information made by a "professional who is a member of its workforce." This includes requests made by in-house attorneys. *See* 45 C.F.R. §164.514(d)(3)(iii). A covered entity should specify in this policy the professionals or categories of professionals whose requests need not be second guessed. *See* 65 Fed. Reg. at 82,715 (Dec. 28, 2000)..

2 The Privacy Rule permits reliance upon requests for protected health information by a "professional . . . who is a business associate." *See* 45 C.F.R. §164.514(d)(3)(iii). A covered entity should specify the business associates whose requests need not be questioned.

3 The Privacy Rule would appear to permit both routine and non-routine disclosures of the entire case record as long as a "specific justification" has been identified by the covered entity for these disclosures. The July 2001 Guidance supports this view, and further explains that there may be routine disclosures that require the entire case record. However, the Preamble to the Privacy Rule clouds the issue of whether there may be non-routine disclosures of the entire case record by stating that "[c]overed entities' policies and procedures must provide that disclosure of an entire case record will not be made except pursuant to policies which specifically justify why the entire case record is needed." 65 Fed. Reg. at 82,545 (Dec. 28, 2000). Moreover, HHS has stated that "a disclosure of the entire case record absent such documented justification is a presumptive violation of this rule." 65 Fed. Reg. at 82,545 (Dec. 28, 2000). In light of this guidance we recommend the following precaution: if a covered entity's policy permits non-routine disclosures of the entire case record (which may technically be permissible under the text of the Privacy Rule itself), the policy should require documentation of a "specific justification" in the case record when any such non-routine disclosure is made.

4 The Privacy Rule states that the minimum necessary standard does not apply to "uses and disclosures that are required for compliance with applicable requirements of this subchapter." 45 C.F.R. § 164.502(b)(2)(vi). The Preamble and the July 2001 Guidance explain that this sentence is intended to provide an exception to the minimum necessary standard for uses and disclosures required for compliance with standardized transactions under HIPAA. *See* 65 Fed. Reg. at 82,545 (Dec. 28, 2000).

5 While incidental uses and disclosures are permitted under the Privacy Rule, programs may individually evaluate whether to include such an exception in any policies and procedures implementing the minimum necessary standard. *See* 45 C.F.R. 164.502(a)(1)(iii) (as published in 67 Fed. Reg. 53,267 (August 14, 2002)). Including such language may alleviate anxieties and concerns CUCS staff and health care professionals may have about the scope of this policy and the effect it may have on their daily conduct. Including this exception may also mislead CUCS staff and health care professionals to characterize many uses, disclosures and requests as incidental rather than

applying reasonable precautions to limit the use, disclosure or request to the minimum amount of protected health information necessary.

6 A covered entity may refer to disciplinary action procedures already established in its policy manuals. Alternatively, it may establish disciplinary action procedures that responds specifically to violations of this policy. The Privacy Rule advises that covered entities may choose to vary the severity of the sanction (ranging from a warning to termination of employment or contract) according to the severity of the violation (*e.g.*, intentional violations, unintentional violations, or a pattern or practice of violations). 65 Fed. Reg. at 82,562 (Dec. 28, 2000).

CENTER FOR URBAN COMMUNITY SERVICES
CLIENT ACCESS TO
CLINICAL RECORD POLICY

Revision Effective 1/3/2012

Purpose of Policy

The purpose of this policy is to ensure that clients have appropriate access to clinical records maintained by CUCS in accordance with New York's Mental Hygiene Law. This policy applies to all CUCS programs other than the ACT Program.

Definitions

Clinical record means any information maintained or possessed by CUCS concerning or relating to the examination or treatment of an identifiable client who has been treated or is being treated by CUCS. Clinical records do not include data disclosed to a practitioner in confidence by other persons on the basis of an express condition that it would never be disclosed to the patient or client or other persons unless such data has been disclosed by CUCS or the practitioner to any other person.

Statement of Policy

Right to Access

Subject to the conditions and limitations set forth in this policy, each client has the right to inspect or obtain copies of his or her clinical record maintained by CUCS. Requests may be made by the client or any other person who is qualified to act as the client's personal representative under state law.

Clients do not have to formally request access to their treatment or service plans. Staff should offer a copy of the treatment or service plan to the client each time the plan is reviewed and completed and may provide any client with a copy of their treatment or service plan at any time it is requested thereafter.

Client Requests for Access for all Records except Treatment or Service Plans
CUCS staff should encourage clients to use CUCS's standard form for all access to records requests. If the client does not use this form, he or she must submit a written request that includes all of the information solicited by the form. All requests for access will be forwarded to the program's Program Director or designee and also to the treating practitioner.

The Program Director or designee will respond to client requests for access to their clinical record as soon as reasonably possible after the request is received and in accordance with the following deadlines.

Inspection of Records. If the client is seeking to inspect his or her clinical record, the Program Director or designee will respond to the request within 10 days from the date the request was received by CUCS. Inspection means viewing the records at CUCS's facilities rather than receiving a copy of the records.

Copies of Records. If a client is seeking a copy of his or her clinical record, the Program Director or designee will make every reasonable effort to respond within 30 days to requests for a copy of information maintained on-site at CUCS and within 60 days to requests for a copy of information maintained off-site at another facility. These deadlines set outside limits and staff are strongly encouraged to respond to requests as soon as possible.

Granting Client Requests For Access

Notify The Client. The Program Director or designee must notify the client that his or her request for access is being granted. The client must be notified in writing. If the client requested a copy of the clinical record, whenever feasible, the Program Director or designee should provide a copy to the client with the notice informing the client that the request has been granted. If the client requested an opportunity to inspect his or her clinical record, a staff member must explain how the client may arrange an appointment to visit CUCS and review the information.

Requests For Inspection Of Records. If CUCS is granting a client's request to inspect his or her clinical record, the Program Director or designee must arrange an appointment with the client. CUCS may make available for inspection either the original or a copy of the record.

Requests for Copies. Whenever possible, copies of records should be provided in the form or format requested by the client. If the information cannot be easily produced in the format requested by the client, staff may either provide the client with a hard paper copy of the information or may attempt to work out an alternative format that is acceptable to the client. However, if a clinical record is maintained electronically and the client requests an electronic copy, the record must be provided in an electronic form.

Copies should be delivered to the client in the method specified on the client's request form or letter. The client may visit CUCS to pick up the copies or request that the copies be delivered by mail or by fax to an address provided on the form or letter.

Applicable Fees

CUCS may charge clients a reasonable fee for providing copies of clinical records that covers copying costs and postage (if the information is mailed). The Program Director or designee will maintain a list of such charges that will be updated from time to time, provided that charges for paper copies may not exceed $0.75 per page. No client may be denied access to his or her records solely because of inability to pay. The Program Director or designee may waive collection of copying and postage fees in his or her discretion if he or she believes the client is unable to pay the fees.

Denial of Access

CUCS may deny access to clinical records if the client's treating practitioner determines that providing access is reasonably likely to cause substantial and identifiable harm to the client or another person.

Any denial of access to a clinical record will be communicated to the client on CUCS's standard form. **The Privacy Officer must review all denials.**

Summaries In Lieu of Access. If the client's request for direct access to his or her information is denied for one of these reasons, the Program Director or designee may provide the client with a prepared summary of the information prepared by the Program Director or designee or designee.

Partial Denial. If there are grounds to deny the client's access to only part of the clinical record requested, the Program Director or designee will provide the client with access to the rest of the information after excluding the parts to which access has been denied. The excluded parts should be summarized for the client as provided above. **The Privacy Officer must review all partial denials.**

Review of Denial of Access

If the client's request is denied, the Program Director or designee must provide to the client a request form that the client may use to appeal this denial before a clinical records access review committee appointed by the State of New York.

- If a client requests this review, the Privacy officer must transfer the client's information in dispute, the denial notice sent to the client, and (if appropriate) any further explanation of the reason for the denial to the specified state clinical records access review committee within 10 days.
- If the state clinical records access review committee decides that the client's request for access should be granted (in whole or in part), the Privacy Officer must follow the procedures granting access as outlined above.
- If the state clinical records access review committee decides that the client's request for access was properly denied, the client will be informed by the committee of any opportunity to seek judicial review in the court system.

In some cases, the client will be entitled to seek another level of review by appealing the state clinical records access review committee's decision to the court system. If staff receive notice that a client has sought judicial review, this notice should be delivered to the Privacy Officer immediately. Staff should not grant access to the client or personal representative unless the Privacy Officer directs the staff to do so.

Requests For Access By A Client's Personal Representative

If a client's personal representative requests access to the client's clinical record, the Program Director or designee will generally grant or deny access according to the procedures in this policy as though the personal representative were the client, *unless one of the following exceptions applies:*

Client Objection. The Privacy Officer may notify a client who is over the age of twelve years of the request for access by a personal representative. If the client objects to access by the personal representative, the Program Director or designee, in consultation with the client's treating practitioner, and the Chief Privacy Officer, may deny the personal representative's request. The personal representative should be notified in writing of the reason for this denial.

Detrimental Effect From Access By Parent Or Guardian. A parent or guardian of a minor may be denied access to the minor's clinical record if a treating physician certifies that such access by the parent or guardian would have a detrimental effect on: (1) the physician's or CUCS's professional relationship with the minor; (2) the care or treatment of the minor; or (3) the minor's relationship with his or her parent or guardian. The personal representative should be notified in writing of the reason for this denial and given the opportunity to seek review of the decision as provided in this policy. This denial must be reviewed with the Chief Privacy Officer.

Detrimental Effect From Access By Parent, Spouse or Adult Child of Client. A parent, spouse or adult child of a client may be denied access to the minor's clinical record if a treating physician certifies that such access by the parent or guardian would have a detrimental effect on: (1) the physician's or CUCS's professional relationship with the client; (2) the care or treatment of the client; or (3) the client's relationship with his or her parent, spouse or adult child. The personal representative should be notified in writing of the reason for this denial and given the opportunity to seek review of the decision as provided in this policy. This denial must be reviewed with the Chief Privacy Officer.

Record Retention

A copy of all correspondence and other documents related to requests made by clients for access to clinical records will be placed in the client's clinical record by the Program Director or designee and maintained for six years from the date of the request.

Enforcement

Employees who do not comply with this policy will be subject to disciplinary action by CUCS. Depending on the facts and circumstances of each case, CUCS may reprimand, suspend or dismiss any employee who fails to comply with this policy.

Responsible Party

Any questions pertaining to this policy should be directed to the Privacy Officer.

CENTER FOR URBAN COMMUNITY SERVICES
POLICY ON AMENDMENT OF
INFORMATION IN CLINICAL RECORDS

Effective August 1st, 2009

Purpose of Policy

The purpose of this policy is to ensure that CUCS provides clients with an opportunity to request amendments of clinical records maintained by or on behalf of CUCS in accordance with New York's Mental Hygiene Law. This policy applies to all CUCS programs other than the ACT Program.

Definitions

Clinical record means any information maintained or possessed by CUCS concerning or relating to the examination or treatment of an identifiable client which has been treated or is being treated by CUCS. Clinical records do not include data disclosed to a practitioner in confidence by other persons on the basis of an express condition that it would never be disclosed to the patient or client or other persons unless such data has been disclosed by CUCS or the practitioner to any other person.

Statement of Policy

Scope of Right to Challenge Accuracy

Subject to the conditions and limitations set forth in this policy, each client has the right to challenge the accuracy and request an amendment of clinical records maintained by CUCS. Amendments may be requested by the client or any other person who is qualified to act as the client's personal representative under state law.

CUCS is required to review requests challenging the accuracy of ***factual*** information in a clinical record. For example, a client may challenge the accuracy of his or her birth date, weight or a test result recorded in a clinical record. Clients do not have the right to challenge the accuracy of a provider's observations, inferences or conclusions.

Process for Handling Requests

All requests for amendments shall be received and responded to by the Privacy Officer who shall seek the advice of other CUCS personnel or advisors as deemed necessary. All requests for amendments must be made in writing and must provide a reason to support the amendment. The Privacy Officer will respond to any request for an amendment within 30 days of receipt of the request.

Adjudication of Requests

If the Privacy Officer determines that a client's challenge to the accuracy of factual information in the clinical record is valid, a correction will be included in the clinical record and the client will be notified of the correction. The original information will not be deleted. If the Privacy Officer determines that such a challenge is invalid, the clinical record will not be revised but the client's statement will become a permanent part of the clinical record. The client will be notified of the determination. If a client has submitted a written statement challenging the accuracy of information that the Privacy Officer determines to involve provider's observations, conclusions or inferences, the Privacy Officer shall notify the client that the request was rejected because it does not relate to factual information. All notices shall be in writing.

Record Retention

CUCS's Privacy Officer will maintain documentation pertaining to requests for amendments made by clients under this policy for six years from the date of the request.

Enforcement

Employees who do not comply with this policy will be subject to disciplinary action by CUCS. Depending on the facts and circumstances of each case, CUCS may reprimand, suspend, dismiss or refer for criminal prosecution any employee who fails to comply with this policy.

Responsible Party

Any questions pertaining to this policy should be directed to the Privacy Officer.

80453935.1

CENTER FOR URBAN COMMUNITY SERVICES
ACCOUNTING OF DISCLOSURES
OF CLINICAL RECORDS POLICY

Effective August 1st, 2009

Purpose of Policy

The purpose of this policy is to ensure that CUCS provides an accounting of disclosures of information in a client's clinical record to the client in accordance with the New York Mental Hygiene Law. This policy applies to clients of all CUCS programs other than the ACT Program.

Statement of Policy

Subject to the conditions and limitations set forth in this policy, each client has the right to receive an accounting of disclosures of his or her clinical record. An accounting may be requested by the client if he or she has the right to act on his or her own behalf, or by any person who is qualified to act as the client's personal representative under state law.

Clinical record means any information maintained or possessed by CUCS concerning or relating to the examination or treatment of an identifiable client which has been treated or is being treated by CUCS. Clinical records do not include data disclosed to a practitioner in confidence by other persons on the basis of an express condition that it would never be disclosed to the patient or client or other persons unless such data has been disclosed by CUCS or the practitioner to any other person.

Disclosures Subject to an Accounting

All disclosures of clinical records made by CUCS to outside persons or entities will be subject to an accounting, except for disclosures:

- To government entities for purposes of obtaining reimbursement for CUCS's services.
- Made to persons reviewing information or records for compliance with quality of care standards.
- Made to the Mental Hygiene Legal Services.
- Disclosures made for treatment or pursuant to the patient's authorization are not subject to the accounting requirement.[6]
-

Tracking Disclosures

Employees must promptly document each disclosure made by the employee that is subject to the accounting requirement in a progress note in the applicable client's clinical record. Disclosures

made to insurance companies need only be entered at the time the disclosure is first made.

Provision of an Accounting

Employees should encourage clients to use CUCS's "Request for an Accounting of Disclosures Form" for any accounting requests. All requests received by employees from clients should be directed to the Program Director, who will be responsible for coordinating a response.

Progress notes documenting disclosures must include the following information for each disclosure subject to the accounting requirement:

- The date of the disclosure;
- The name of the recipient and, if known, the recipient's address;
- A brief description of the protected health information disclosed; and
- A brief statement of the purpose of the disclosure.

If CUCS has made disclosures for a research study involving 50 or more individuals, in lieu of the information set forth above, the accounting may include the following:

- The name of the research protocol or study;
- A description of the research protocol or study, including its purpose and the criteria for selecting particular records;
- A description of the type of protected health information disclosed;
- The date or time period of the disclosures, including the last date;
- The name, address and telephone number of the entity sponsoring the research and the lead researcher; and
- A statement that the client's information may or may not have been disclosed as part of the research.

Time Frame for Providing Accounting

CUCS should provide an accounting within 60 days of a client's request.

Record Retention

The Program Director will maintain documentation of all accountings requested by and provided to clients under this policy for a period of six years.

Enforcement

Employees who do not comply with this policy will be subject to disciplinary action by CUCS. Depending on the facts and circumstances of each case [and in compliance with any applicable collective bargaining agreements], CUCS may reprimand, suspend or dismiss any employee who fails to comply with this policy.

Responsible Party

Any questions pertaining to this policy should be directed to the Privacy Officer.