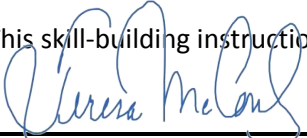



**SPECIALIZED FAMILY CARE
Provider Training**

Category:	Advocacy
Title:	Privacy in the Specialized Family Care Home
Materials:	Articles: "CED Notice of Privacy Practices, Jan. 2014", "West Virginia Executive Branch Privacy Policy: Security Safeguards", Privacy in the Specialized Family Care Home"
Goal:	Provider can protect the privacy of the individual in care
Credit Hours:	2 Hours
Date Developed:	March 2014, Updated March 2017
Developed by:	Donna McCune, SFC Program

This skill-building instruction has been approved for Specialized Family Care Provider training by:

	3/16/2017
Specialized Family Care Program Manager	Date
	3-15-2017
Content Reviewed by: Carol Brewster, FBCS	Date

Training Objectives:

- Specialized Family Care Provider can define Protected Health Information
- Specialized Family Care Provider can name examples of Personal Information
- Specialized Family Care Provider knows how to protect the Personal Information of an individual in care

Training Procedures:

- Specialized Family Care Provider initiated self-study
- Test completed by Specialized Family Care Provider
- Review of test responses by Family Based Care Specialist and Specialized Family Care Provider

I certify that I have completed all the materials associated with this training module. I feel that I have a basic understanding of the material completed.

Specialized Family Care Provider	Start Time	End Time	Date
---	-------------------	-----------------	-------------

Reviewed by: _____
Family Based Care Specialist **Date**

This Program is funded by the WV Department of Health & Human Resources, Bureau for Children & Families and administered by the Center for Excellence in Disabilities, West Virginia University.

WVDHHR/CED/SFC/PRIVACY IN THE SFC HOME Updated/MARCH 2017

PRIVACY IN THE SPECIALIZED FAMILY CARE HOME

YOU ARE PROTECTED

Specialized Family Care Providers are required to provide confidential information about themselves to the Center for Excellence in Disabilities and other agencies in order to be certified and paid for the work which they do. This information includes birth date, address, social security number, family history, health information, etc. This information is required to be kept confidential by the professionals who serve the SFC family and only shared with other professionals who have a need to know. WVU-Center for Excellence in Disabilities provides to all SFC applicants a copy of “Notice of Privacy Practices”. The document, which is part of this training module, specifically addresses your medical information, called Protected Health Information (PHI), and describes how it is protected.

You are a Protector

Did you know that you are a protector of the PHI (Private Health Information) for the individuals whom you serve in your home? Due to the nature of your work you will have medical knowledge about this individual. This information is not to be randomly shared with those who are not involved in the care of the individual.

There is other information, besides medical, which you must protect because it is sensitive in nature. This is called personal information (PI). Some examples of this are described in the attached handout on PI which includes social security numbers, financial information related to state benefits, etc.

Besides information which is protected by law, as described in the document attached. It is the responsibility of the Provider to protect other personal information about the individual in care. The Specialized Family Care Program requires that “The Provider shall treat all written

and oral information and documentation about an individual and the family in a confidential manner.” Do not share personal history information about your individual in care with others, who are unauthorized to receive it and do not have reason to know, but are just curious.

Protecting Personal Information of the Individual in Care

Ways to protect the personal information of the individual in your care include:

- Do not discuss details of your individual’s life in public settings
- Have a secure, private place in your home to store his/her documents
- Do not allow photos to be taken for publicity purposes unless you have the permission from the individual’s guardian
- Keep medication in a secure, out of sight location
- Never give out an individual’s information to an unknown caller on the telephone or over the internet
- Do not post information, including photos, about your individual on the internet, such as Facebook
- Be sensitive when introducing your individual in care, not labeling him/her as a “foster child/adult, personal care client” etc. A way to phrase your introduction could be “This is (name) who has joined (or is part of) our family.”
- When someone else is going to be providing care for your individual (such as a respite provider) they need to be informed about general behaviors and medical concerns affecting care, but not specific situations related to background, birth family, etc.
- Contact your Family Based Care Specialist, individual’s guardian or other professionals involved in the individual’s care with any questions regarding a request for disclosure of information.

Donna McCune, MSW
WVU-Center for Excellence in Disabilities
Specialized Family Care Program



PROVIDING LEADERSHIP IN THE DEVELOPMENT OF SERVICES AND SUPPORTS FOR PERSONS WITH DISABILITIES.

Notice of Privacy Practices

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.

Private medical information includes any past, present, or future health condition you might have, health service you receive, and any record of payment for health service that you make or are made on your behalf. This information is also called ***Protected Health Information (PHI)***.

Your Privacy Rights:

Your right to inspect and copy. You or your legal guardian have the right to inspect and obtain a copy of your protected health information. You may request copies at any time.

Your right to authorize.

- You or your legal guardian have the right to authorize the release of any or all your protected health information to other providers.
- Your authorization is required before your protected health information can be used for marketing or sale.

Your right to opt out of fundraising requests. You have a right to opt out of any fundraising requests we may make of you. An opt-out provision must be included with any fundraising communication or materials.

Your right to request restrictions and make corrections. You or your legal guardian have the right to request certain restrictions and limitations in how your medical information is used. You may also correct and amend information in your medical records. For example:

- **Restrict routine disclosures.** You may ask us not to use or disclose any part of your protected health information (PHI) to others who might otherwise be routinely involved in provision of services to you. We will comply with such requests but they may limit the services we can offer you.
- **Request confidential communications.** You have the right to request that we contact you and/or send your protected health information to an alternate location other than your home, and that we do not disclose your PHI to specific family members.
- **Request medical record corrections.** You have the right to make amendments to your protected health information. If the health care provider who wrote the entry that you would like to correct agrees with the correction, we will make the appropriate changes to the medical record. If the health care provider who wrote the original entry disagrees with your correction, we will not change the record but will include your corrections in the record to document your disagreement.
- **If you pay out of pocket for a medical service or test:** You have the right to instruct the medical provider of the test to NOT send the results to your medical insurer or health plan.

Your right to a paper copy and/or electronic copy of this notice.

Routine Disclosure of Your Protected Health Information

The law allows us to use and disclose your protected health information in certain routine ways. These are listed below.

In all cases, we will use and disclose the minimum amount of protected information necessary to fulfill each function.

For Treatment and Services. WVU CED providers working within specific programs or collaborating programs may discuss your protected health information (PHI) with other providers in those programs to discuss how to provide you with the best possible services. Students-in-training within those programs may also have access to your PHI. If you have an interdisciplinary treatment team or service coordination team, they may discuss your PHI with one another.

For Payment. Your protected health information could be disclosed to our in house accounting office as needed, in order to process billing claims or distribution of funds.

For Daily Activities and Organizational Operations. We may need to collect and disclose some of your protected health information when we provide service coordination, technical assistance, and treatment services. For example, we may disclose your PHI when referring you to other agencies, when making appointments for you, or when organizing a service coordination team or treatment team for you. In addition, we are obligated to conduct quality assurance activities of our privacy practices. In carrying out these activities, the quality assurance team may have access to your PHI.

If you are a WVU CED Clinic patient, your protected health information may be electronically collected and stored securely in a central WVU CED database. To assure continuity of care among WVU CED services, parts of this database may be viewed by authorized WVU CED personnel.

Research. Some WVU CED Programs conduct research studies. We will not use your protected health information for any research studies without your prior consent and written authorization.

De-identified Information. De-identified information is protected health information from which all personal identification has been removed. This means it can no longer be identified as yours and is no longer considered protected. Our center uses de-identified information for data collection, progress reports, research, and evaluation activities. For example, we might generate a report on the number of hours we spent giving technical assistance, or the number of people with spinal cord injury we have served, or the number of children with cerebral palsy we have seen who need new wheelchairs.

Non Routine Situations Where We Must Disclose Your Protected Health Information.

The law requires us to disclose your protected health information under certain circumstances. In these cases, we can disclose your protected health information without your permission. Examples of such cases include: subpoenas or other court orders; suspected cases of domestic violence, abuse, or neglect; workers' and veterans' compensation requirements; to avert a serious threat to public health or safety; or to comply with governmental regulations.

In these cases, you have the right to know which individuals or agencies have received or reviewed copies of your protected health information. WVU CED staff will be happy to provide you with this information if you ask for it.

Change of WVU CED Ownership.

If the WVU CED becomes part of another organization in the future, your medical information will become the property of that new organization.

If You Think Your Right To Privacy Has Been Violated.

If you think we have violated your privacy rights, you may submit a written complaint to the West Virginia University School of Medicine Legal Services. You may also file a complaint with the U.S. Department of Health and Human Services (DHHS). All complaints filed with the U.S. DHHS must be filed within 180 days of when you first learned of the incident.

Paper copies of complaint forms are available at our receptionist’s desk on the second floor of the WVU CED. If you prefer to contact the departments directly, here is contact information:

To request a complaint form
from the WVU School of Medicine,
please call (304) 293-3584

To request a complaint form
from the U.S. Department of HHS,
please call (800) 368-1019
or visit the website
<http://www.hhs.gov/ocr/504file.html>

The WVU CED reserves the right to change this notice at any time in the future. The effective date of this notice is at the top of page one. You may request a copy of any revised notice of privacy practices. Notices can be requested in person, by contacting your WVU CED staff by phone or email, or by visiting our website <http://www.ced.wvu.edu> .

West Virginia Executive Branch
Privacy Policy: Security Safeguards

Handling Sensitive PI

Questions:

What makes some personal information sensitive?

Answer:

We all recognize that some type of personal information (PI) are more sensitive than others. We are usually willing to give our office phone number to people, but we would not give our Social Security number to someone without a good reason.

The West Virginia Executive Branch Security Safeguards Policy requires each Department to protect PI, taking into account its sensitivity. This means that Departments are expected to have strict procedures to protect the most sensitive PI, while more flexibility can be offered for less sensitive PI. For Example:



All Department workers may be access to the employee directory, containing coworker names, office locations and office phone numbers. This PI isn't sensitive and broad access enables us to locate and call coworkers as needed.



A database containing employee medical records would only be accessible by a small number of HR workers who need the information to process leave requests. Health information is very sensitive, so access is limited to people who have a need-to-know.

Everyone should be familiar with the types of PI that are considered sensitive. Here are some examples of sensitive PI:

- Social Security numbers and other government-issued identification numbers, such as driver's license numbers,
- Financial account and payment card information (such as credit card numbers),
- All health-related information, medical records, and biometric data (e.g., fingerprints),
- PI contained in personnel records,
- All records pertaining to recipients of state benefits, such as foster care, welfare, food assistance programs, protective services, etc.,
- Information used to access computer systems (such as login names and passwords),
- Law enforcement records/files containing PI,
- Information from consumer reports, such as employee background screening reports, or reports from third party investigators, and
- Records containing information that individuals generally consider sensitive, such as race, religion, national origin, sexual orientation, and political affiliation.

If you handle sensitive PI as part of our job, be sure that you understand the security and confidentiality processes that apply. Even if you don't routinely handle sensitive PI, be aware that you likely still have access to lots of sensitive PI. For example, you may know your coworkers' health information, sexual orientation, or religion. Before you use or share any sensitive PI, consider whether that use or disclosure is appropriate and consistent with your obligations under the WV Executive Branch Privacy Policies. If you aren't sure, ask your manager or your Privacy Officer?