INFORMATION PRIVACY AND SECURITY

Purpose

This policy applies only to Behavioral Health and Prevention Services Program staff providing health-related services to student clients, the technology systems used to support them, and related supervisory staff. Specifically, this policy outlines Northwest Educational Service District 189 (NWESD 189) measures to provide commonly accepted standards of care for the privacy and security of the health-related information of its student consumers. These protections are delineated in the following six sections:

1) Information Privacy and Security Management Process

2) Information System User Procedures

3) Information Access Control Procedures

4) Information Privacy and Security Incident Response

5) Uses and Disclosures of Confidential Information

6) Individual Rights

Information Privacy and Security Management Process

NWESD 189 will establish procedures to create and maintain an Information Privacy and Security Management Process to ensure the confidentiality, integrity, and availability of consumer information. The procedures include the following components:

1) Risk Assessment. The NWESD 189 will document risk assessment of consumer information held by the organization at least annually or upon significant changes to operations or the environment.

   A) Risk analysis and assessment will be carried out using the processes and steps recommended in the National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (http://csrc.nist.gov/publications/PubsSPs.html#800-30) and any guidance issued by the US Department of Health and Human Services in support of *Health Insurance Portability and Accountability Act* (HIPAA) compliance and risk analysis.

   B) Risks will be mitigated and managed by NWESD 189 to the best of its abilities within reasonable constraints of cost, staff ability, and hardware/software capabilities.

C) Risk analysis and assessment will be reviewed and updated whenever there are material changes in systems or operations controlled by NWESD 189, or significant changes in the security environment in which NWESD 189 operates, or no less frequently than every two (2) years.

2) Information Security Evaluation. The NWESD 189 will perform ongoing evaluations of the information security-related technical measures, policies, and procedures in place to ensure they continue to provide the protection necessary for consumer information. The NWESD 189 will also perform an Information Security Evaluation whenever there is a change in environmental or operational conditions that may affect the security of consumer information.

3) Implementation of Secure Systems and Applications. The NWESD 189 will implement and maintain systems and applications using secure best practices, whether developed in-house or procured from an external vendor.

4) Backup and Disaster Recovery. The NWESD 189 will prepare for contingencies and ensure an appropriate response to emergencies or other occurrences that may damage systems that contain consumer information. Information not required to be maintained will be disposed of according to defined procedures. Procedures will be sufficient to restore lost or damaged data with a useful duplicate and to enable the NWESD 189 to continue secure operations while operating in an emergency situation, as practicable.

5) Information Security Incidents. The NWESD 189 will have in place an Information Privacy and Security Incident Procedure (6520-P), providing an orderly process for all appropriate workforce members to report and promptly handle security violations. It will include procedures for investigating, mitigating, reporting, processing, and responding to suspected or known information security incidents, as well as periodic review in order to identify risks to the privacy and security of consumer information.

6) Information System Usage Audits and Activity Reviews. The Behavioral Health and Prevention Services Program Director in consultation with the Technology Services Department will conduct, on an annual basis or as related to an incident or other event/ activity, reviews and audits of information access, system usage, and internal security controls.

7) Training. The NWESD 189 will establish an Information Security Awareness and Privacy Training Program for the purpose of ensuring that all appropriate workforce members, including management, are aware of the NWESD 189's privacy and security policies, procedures, and general principles of information security.

8) Contracts with Third Parties. The NWESD 189 will enter into written agreements with any entities that create, receive, maintain, or transmit protected consumer information on behalf of the organization, in order to require the protection of the security of any and all such information.

9) Documentation. The NWESD 189 will document any policies and procedures implemented as well as any actions, activities, and assessments required to be performed under these policies.

Documentation will be maintained for at least six (6) years from the date of issue or the date of last effect, whichever is later. The documentation will be periodically reviewed and updated as needed, in response to environmental or operational changes affecting the privacy or security of confidential information, or in response to modifications in regulations or guidance for compliance.

Information System User Procedures

The computer systems at NWESD 189 are provided to employees to perform their jobs. As such, NWESD 189 reserves the right to determine appropriate use of the equipment and software that employees use. No employee is allowed to employ these resources for personal use or gain. It is the responsibility of supervisors to monitor the appropriate behavior of their employees, with the guidance and support of Technology Services Department.

A) NWESD 189 workforce members will comply with the requirements of applicable privacy and security standards and regulations. Compliance will be ensured through the use of measures such as training, security reminders, policies and procedures, sanctions for policy violations, and monitoring of workforce activities.

B) Employees who are granted access to the computer systems at NWESD 189 agree to abide by the policies guiding the appropriate use of these systems, pursuant to policy 2022, *Electronic Information System (Networks)*, and its procedures/forms. Any employee found in violation of this policy will be subject to a security investigation and possible disciplinary action, up to and including termination. Some violations may also constitute a criminal offense and may result in legal action according to federal and state laws.

Information user procedures will address a variety of issues of which computer, system, and network users must be aware:

1) Monitoring, User Privacy, and Sanctions for Policy Violations. The NWESD 189 network and related systems are owned and operated by NWESD 189 for its own use and for administrative purposes. It is the policy of NWESD 189 to treat all transmissions over the NWESD 189 network as private; however, the use of the NWESD 189 network and of NWESD 189 computing resources is strictly by permission of the NWESD 189, and staff user confidentiality is not guaranteed.

A) All messages created, sent, or retrieved over NWESD 189 networks are the property of NWESD 189, which reserves the right to access the contents of any messages sent over its facilities if the NWESD 189 believes, in its sole judgment, that it has a business need to do so.

B) All information stored on NWESD 189 systems and networks are the property of NWESD 189, which reserves the right to access any data stored on NWESD 189 systems and networks if the NWESD 189 believes, in its sole judgment, that it has a business need to do so.

C) As appropriate, any member of the workforce who does not comply with the security policies and procedures of the NWESD 189, or who otherwise misuses or misappropriates personal or private information will be subject to disciplinary action, up to and including termination.

2) Access of Information Systems. The NWESD 189 grants role-based access to its network as well as other systems, and the organization Intranet and the Internet at large. Staff should be provided the minimum necessary access to perform their job functions, and all members of the workforce have only appropriate access to consumer information and do not have unnecessary or inappropriate access to consumer information. Users may access only those computer systems and resources that are necessary to perform their job. Technology Services Department is responsible for managing the process for the provision of access and passwords.

3) Acceptable Use. Each employee will be responsible for all computer transactions that are made with his/her User ID and password, and for the care and security of any computer or hardware assigned to him/her. Users will not knowingly engage in any activity that may be potentially harmful to any portion of the network or its users. They will also take the necessary precautions to protect any confidential or sensitive information from inappropriate or unauthorized access by others.

A) Workforce members may not access systems, files, documents, or other data to which they have not been properly granted access. Workforce members may not share their log-in or access codes or passwords with others.

B) Users leaving their work area are required to lock their computers (by logging off, using the ctrl-alt-delete or Windows-L key combination, or similar mechanism) to prevent use of their login by others.

C) Personal or private information may not be sent from a workstation by any method except as part of an approved business process.

D) Workstations will only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate reason to access that information, to the extent practicable. Staff will endeavor to identify any visitors to areas where personal or private information is handled and may be displayed, and escort them elsewhere.

4) The Internet and Email. Access to the Internet is available on most NWESD 189 computers. Email may be sent internally or over the Internet. Email sent internally should contain only minimal identification of the student/consumer, and detailed information should be sent by an encrypted attachment, such as a secured MS Word document. Email sent to outside entities should not contain any confidential consumer information unless as an encrypted attachment only. Email exchanged with the families of students may include confidential consumer information if reasonable and appropriate, and if requested in writing by the family.

5) Laptops, Portable Devices, and Removable Media. It is the responsibility of any employee who is connecting to the organizational network with a laptop, portable USB-based memory device, or via a tablet or smart phone to ensure that all components of his/her connection remain as secure as his/her network access within the office and to ensure that all security protocols normally used are also applied. Employees must take proper care to protect laptops, portable devices, and removable media from loss or damage, and must protect the confidentiality of any personal or private information held on such devices.

6) Remote Access or Use of Information. Only secure processes approved by Technology Services Department may be used for remote access to electronic personal and private information by remote workers that have been properly granted access rights.

A) Strong cryptography and encryption techniques must be used to safeguard sensitive personal or private information during transmission over public networks.

B) Confidential information may not be maintained outside of NWESD 189 facilities without a valid business reason and approval by the employee's supervisor, and any such stored confidential information must be encrypted by a means that is approved by Technology Services Department.

C) Computer desktops used outside of NWESD 189 facilities by employees to access, store, or transmit confidential information must be used solely by the employee (not shared with other household members and not a public Internet access point) and must be configured with up-to-date virus protection, security patches, and firewall software.

D) Any access or use of NWESD 189 information outside of NWESD 189 offices must be performed in an area and in such a way that onlookers and passersby cannot see any private health information on the devices used.

7) Information Security Incidents. All users must immediately report to their supervisors and NWESD 189's Technology Services Department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc., according to 6520-P, *Information Privacy and Security Incident Procedures*. Incidents will be investigated and actions may be taken to prevent future similar incidents based on the results if the investigation. Persons reporting legitimate incidents will not be retaliated against by the NWESD 189. However, if the incident resulted from a failure to comply with this policy, progressive discipline may be administered.

A) An incident may be any event that affects the confidentiality, integrity, or availability of personal or private information based in any electronic systems or networks.

B) Reportable incidents may include known or suspected breaches of security, unusually slow or improper workstation or system operation, unusual or repeated system crashes, or other out-of-the-ordinary workstation or system behaviors.

Information Access Control Procedures

The NWESD 189 will require the implementation of technical procedures where practicable to limit access to consumer information to only those persons or software programs that have been properly granted access rights, and to ensure that the granting or modification of access to electronic personal and private information is consistent with applicable information security regulations. Specifically:

1) Authentication and Access. The NWESD 189 will have procedures for granting and modifying access to electronic confidential information, including a process to establish, document, review, and modify a user's right of access to a workstation, network, or system.

A) The Technology Services Department will manage the process of password provision for all systems at the NWESD 189.

B) Procedures will be established to verify the identity of the person or entity seeking access to confidential information. Persons may be authenticated by the use of passwords, cards, tokens, keys, biometrics, or other means of personal identification approved by the Technology Services Department.

C) Procedures will be developed to ensure that electronic confidential information will be accessible by approved personnel in an emergency situation in which normal access is not available.

D) Every user of systems holding or using electronic confidential information will have a unique user name or number, to enable the identification and tracking of user access. Users may not share their log-in or access codes or passwords with others. Group log-ins will not be used, except in situations where it is necessary to use such procedures to maintain quality of care, where permitted by an approved business process considering the organization's risk analysis. Where group log-ins are used, there will be procedural methods for recording the members of a group that have access under a single log-in.

E) Electronic procedures will be established, based on the NWESD 189's risk analysis, to terminate an electronic session after a predetermined period of inactivity. Procedures may include password-protected screen savers or forced logouts of systems and/or applications.

2) Perimeter Security. Perimeter security controls, such as firewalls, will be used to protect the electronic confidential information held within the NWESD 189's systems and allow access across the perimeter where appropriate. Systems contained within the perimeter should be protected via anti-malware (anti-virus, anti-spam, anti-keylogging, etc.) systems.

A) A perimeter firewall is in place to separate the NWESD 189's internal networks from the public Internet. Only necessary protocols and their associated ports are to be open on the firewall.

B) Any changes to the firewall configuration, deemed significant by the Technology Services Director, must be approved by the Assistant Superintendent for Operations. Change requests for the firewall must follow a defined, documented process.

3) Data Encryption. Where indicated by a formal risk analysis or as required under applicable regulations, confidential information at rest will be encrypted to prevent access or use by unauthorized personnel. Confidential information residing on easily movable devices such as laptops, smart phones, memory sticks and other portable electronic devices must be encrypted. In order to avoid reportable information security breaches, any encryption used must meet the requirements specified in guidance provided by the US Department of Health and Human Services (HHS), available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html.

A) Confidential information may not be sent from a workstation by any method except as part of an approved business process. Electronically or physically transmitted personal or private information must be protected from unauthorized access or modification. Procedures will be established for the encryption of all electronic confidential consumer information transmitted over the Internet, in email traversing outside networks, and in text messaging.

B) The requirement for encryption of transmitted confidential information will not be established, so long as Technology Services Department assertively regulates who is provided access to the NWESD 189 physical network and that network operates in a switched environment. If encryption is required at a future date, it may only be waived if the individual concerned has a) requested that unencrypted communications be used, b) been advised of any risks, and c) acknowledged the risks.

4) Physical Access Controls. The NWESD 189 will establish procedures to limit or enable, as appropriate, physical access to the building, the office, files, systems, and devices containing personal or private information. Areas and facilities housing network and/or computer server systems, network switches, and patch panels will be secured so that such devices contained therein are inaccessible to unauthorized personnel.

A) Workstations will only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate business or healthcare reason to access that information, to the extent practicable.

B) The physical security of the premises will be reviewed regularly, and appropriate alarm and/or surveillance technology will be utilized, both for monitoring entry and exit during business hours, and for securing the premises after hours.

5) Media Management and Disposal. There will be procedures to record the movement of hardware and electronic media containing electronic confidential information into, out of, and within organization facilities, to ensure that all devices used by the NWESD 189 to access or retain electronic confidential information are known and locatable, and that any portable hardware or media retaining electronic confidential information are in the care of known responsible parties.

A) The disposal or reuse for another purpose of any hardware or electronic media containing confidential information, including all forms and types, such as computers, servers, portable devices, copiers, and multifunction machines, will include the destruction of any such confidential information before ultimate disposal or reallocation to a new use. The destruction of electronic confidential information will be carried out by physical or electronic means that ensures the actual destruction of the information.

B) In order to avoid reportable information security breaches under the HIPAA Breach Notification regulations at §164.400 et seq., any and all disposal methods used must meet the requirements specified in guidance provided by the US Department of Health and Human Services (HHS), available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

Information Privacy and Security Incident Response

The NWESD 189 will have in place procedures for the reporting, processing, and response to suspected or known information security incidents in order to investigate, mitigate, and document such incidents, so that security violations and breaches may be reported and handled promptly using an orderly process known to all appropriate workforce members. Specifically, NWESD 189 employees providing medical services to students will be aware of:

1) How to determine what qualifies as an "incident."

2) How to report incidents (including the designation of to whom incidents and alerts must be reported on a 24/7 basis).

3) Steps to take in an investigation.

4) Roles and responsibilities of the response team.

5) Steps to be taken and information to be included when documenting incidents.

6) Steps to be taken to mitigate the effects of incidents (where possible and/or allowed by law).

7) Steps to be taken to provide business recovery and continuity, including the use of adequate backup procedures.

8) Who may release information about the incident and the procedures for doing so.

9) To which entities incidents involving breaches must be reported, such as payment card information, acquirers and card associations, consumers, and relevant local, state, and/or federal agencies.

10) Who will be authorized to release a system following investigation.

11) How a follow-up analysis should be performed and who should participate.

A) Computer Security Incident Response Team members will be provided appropriate training.

B) The incident response plan will be reviewed regularly and tested/modified as appropriate according to lessons learned and to incorporate current security best practices.

Uses and Disclosures of Confidential Information

The NWESD 189 will only use and disclose confidential consumer information (CCI) as permitted or required by applicable regulations. (Note the following procedures are modeled on compliance with the more restrictive HIPAA Privacy Regulation at 45 C.F.R. Part 164, Subpart E, and the use or disclosure of CCI may be further limited by restrictions under 42 C.F.R. Part 2, FERPA, or Washington State Regulation.) Specifically:

1) Uses and Disclosures and Minimum Necessary. Once consents are in place, CCI may be used or disclosed as necessary for treatment and health care operations without a specific authorization from the student consumer. Members of the NWESD 189 workforce may not use, request or disclose to others, any protected health information (PHI) that is more than the minimum necessary to accomplish the purpose of the use, request or disclosure.

   A) The NWESD 189 may contact individuals to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to them. Student consumers may request that they be contacted at home, school, or at a certain location. All reasonable requests will be accommodated.

   B) If family members or close personal friends are assisting in the care of a student consumer, the NWESD 189 may release important health information about the student consumer to those individuals, only as allowed under all applicable regulations.

   C) As required by law and standards of ethical conduct, the NWESD 189 may release health information to the proper authorities if it is believed, in good faith, that such release is necessary to prevent or minimize a serious and approaching threat to the student consumer or the public's health or safety.

2) Requests for Disclosures of CCI. The NWESD 189 will limit routine and recurring requests for, and disclosures of, CCI to the minimum amount of information that is reasonably necessary to accomplish the purpose of the request or disclosure, in compliance with applicable federal and state law/regulations.

   A) The Behavioral Health and Prevention Services Director will review requests for disclosure of CCI that are not routine and recurring and will determine the amount of PHI to be disclosed or requested in each non-routine situation.

B) In the event of requests that are supported by subpoena, court order or request from a regulator or law enforcement officer, the Behavioral Health and Prevention Services Director will ensure that information is released only under the advice of counsel.

C) For disclosures that require an *Authorization for Release* of CCI, documented authorizations must be obtained and recorded prior to the disclosure.

D) All individuals of the workforce (staff) who authorize the disclosure of PHI will take reasonable steps to verify the identity of the person to whom the PHI is disclosed, and verify the person's authority to receive the PHI.

3) Authorization for Release of CCI. For uses and disclosures of CCI that are not otherwise permitted under regulations without an *Authorization for Release* of CCI, the NWESD 189 will obtain an authorization from the student consumer for such use or disclosure. The authorization will have the required elements called for in applicable regulations, will be documented in writing, and will be signed and dated.

4) Disclosure of CCI to Workers' Compensation Programs. As the NWESD 189 limits it health-related services to student consumers, it is unlikely it will disclose CCI to any state workers' compensation agencies. However, in those rare situations in which a student consumer is/was employed and the CCI is requested by state workers' compensation agencies and/or by insurance companies that provide benefits under state workers' compensation laws, the NWESD 189 will provide the CCI without obtaining the written authorization of the student consumer for whom the information pertains. Likewise, in the case of employers who self-insure for workers' compensation benefits, the CCI may be disclosed to the employer. The CCI disclosed will be limited to that which is necessary to establish an individual's eligibility for benefits or to adjudicate the individual's claim for benefits.

5) De-Identification of Data and Limited Data Sets. De-identified CCI is not treated as CCI and may be used or disclosed for any purpose. However, de-identification is not a simple process and a professional experienced in data de-identification must review any de-identification process and data to ensure it is truly de-identified.

A) If CCI is to be used in research or de-identified, procedures must be in place, and the NWESD 189 *Notice of Privacy Practices* (NPP) must include that such de-identification may take place.

B) Limited data sets are partially de-identified information. Because limited data sets potentially could be used to identify the individuals who are the subject of the information, the recipient of a limited data set must enter into a data use agreement.

C) A limited data set may only be used or disclosed for the purposes of research, public health, or health care operations.

D) If CCI is to be used in a limited data set, procedures must be in place, and the NWESD 189 *Notice of Privacy Practices* (NPP) must include a statement that such use of CCI in a limited data set may take place. Data use agreements must be in place and reviewed by NWESD 189 legal counsel to ensure they meet regulatory requirements.

6) Fundraising. If fundraising activities are to use CCI, the NWESD 189 must first have procedures in place to ensure the proper protection of CCI, and the use of such CCI must be mentioned in the NWESD 189 *Notice of Privacy Practices* (NPP).

7) Marketing Activities and Sale of PHI. Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

A) Marketing does not include a communication made:

i) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication; and/or,

ii) for the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(1) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(2) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about (a) the entities participating in a health care provider network or health plan network; (b) replacement of, or enhancements to, a health plan; and, (c) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(3) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

If marketing takes place, the NWESD 189 must first have procedures in place, and indicate in the *Notice of Privacy Practices* (NPP) that marketing activity may take place. An *Authorization for Release* of CCI is required for the use of CCI in marketing activity.

A) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

B) Subject to the exceptions outlined below, the "sale of protected health information" means a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

C) If CCI is to be sold by the NWESD 189, procedures must first be in place and the activity must be noted in the *Notice of Privacy Practices* (NPP). An *Authorization for Release* of CCI that indicates that the PHI is being sold for remuneration must be in place for any CCI that is sold.

D) Sale of PHI does not include a disclosure of protected health information:

i) For public health purposes.

ii) For research purposes, where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes.

iii) For treatment and payment purposes.

iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described the definition of health care operations.

v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, and the only remuneration provided is by the covered entity to the business associate or by the business associate to the subcontractor, if applicable, for the performance of such activities.

vi) To an individual, upon written request of an accounting for disclosures of his/her CCI provided by NWESD 189.

vii) As required by law.

viii) For any other purpose permitted by and in accordance with the applicable requirements of regulations, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

Individual Rights

The NWESD 189 will provide its student consumers with the following individual rights:

1) Alternative Communications of CCI. Individuals may request that any communication of CCI from the NWESD 189 be sent to them by alternative means or to an alternative address. The request may apply to all communications, or only to communication of certain specific information. The NWESD 189 will comply with any such written request that is reasonable. If the request is to communicate via insecure means such as regular email or texting, the individual must understand and accept the risks of insecure communication.

2) Accounting of Disclosures of CCI. The NWESD 189's consumers have a limited right to receive an accounting of the disclosures of their CCI made by the NWESD 189, according to applicable regulation, such as HIPAA Privacy Rule §164.528.

3) Designated Record Sets. Designated Record Sets (DRS) include records that are created or used by the NWESD 189 to make decisions about the consumer's health care or payment for services. The DRS information will be accessible to an individual to copy or request amendments. The DRS will only include HIPAA-covered CCI and will not include information used for the operational purposes of the NWESD 189, such as quality assurance data and incident reports. The types of information that will be included in the DRS are medical records and student consumer/parent signature forms.

4) Notice of Privacy Practices. The NWESD 189 will prepare a HIPAA-type *Notice of Privacy Practices* (NPP) and make it available to any student consumer or his/her representative that wishes to view it.

A) The NPP will be provided in hard copy upon the first visit to facilities, and the receipt will be noted on a log, including a signature by the student consumer and/or his/her representative acknowledging receipt of the NPP, or a notation by the staff present if the student consumer or his/her representative does not wish to sign the acknowledgement of receipt.

B) Each office will post a copy of the NPP, or a summary, on the wall for the student consumer or his/her representative to read. If a summary is posted, a full printed version must be readily available nearby without asking.

C) A copy of the NPP will be made available electronically on the NWESD 189's web site. Any student consumer or his/her representative may ask for a paper copy of the NPP, whether or not an electronic copy has been provided.

D) If policies and procedures or student consumer rights are modified, the NPP must be modified as necessary to reflect any changes. New NPPs must be posted and distributed, but do not need to be re-distributed to those who have received a prior NPP.

5) Individual Access, Amendment, and Restriction on Use or Disclosure of CCI. Student consumers or their representatives have the right to access and to request amendment or restriction on the use of their CCI that is maintained in designated record sets (DRS). Handling of such requests pertaining to CCI that are subject to HIPAA regulations will be handled according to processes meeting the requirements of 45 C.F.R. § 164.524 (Access), 164.526 (Amendment), and 164.522 (Restriction on Use or Disclosure).

First Reading: 09/24/15
Second Reading: 10/28/15
Revised: 10/26/16