INFORMATION PRIVACY AND SECURITY INCIDENT PROCEDURES

This procedure 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:

Reporting Security Incidents

1) Any incident that affects network services or the confidentiality, integrity, or availability of personal or private information based in any electronic system or network will be reported to the Behavioral Health and Prevention Services Director, Technology Services Director (also designated the *Health Insurance Portability and Accountability Act* [HIPAA] Security Officer), and Assistant Superintendent for Operations (also designated the HIPAA Privacy Officer), who will collectively comprise the Information Privacy and Security Incident Response Team (ISIRT). The person receiving the report will document the particulars that are reported and immediately notify the ISIRT leader.

2) 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. Examples of information security incidents may include (but, are not limited to):

   A) An employee or contractor viewing protected information in a system or database the individual is not authorized to access under NWESD 189 policy.

   B) An employee or contractor downloading software that is not permitted under Policy 2022, *Electronic Information System (Networks)*, and its procedures/forms.

   C) Intrusion of a NWESD 189 system by an unauthorized third party (“hacker”) within which any Patient Health Information (PHI) resides. This scenario requires the operant assumption that there was a probable loss of confidential student consumer information.

   D) An unauthorized third party ("hacker") using a falsified user name and password to gain access to information systems.

   E) An unauthorized third party seeking information system access, control, or other information by pretending to be an individual authorized to obtain such information ("social engineering").

   F) An unauthorized third party ("hacker") who acquires access to any NWESD 189 system or device by any means or method.

G) An email or other communication purporting to be from an authorized party seeking protected information or information potentially useful in obtaining information system access ("phishing").

H) A software virus or worm ("malware") interfering with the functioning of personal computers that are part of an information system and which may also result in a compromise of the infected system by a remote "hacker", etc.

3) The ISIRT will review the initial report to determine if it constitutes a new incident, new information about an existing incident, or some other kind of service or information request. Information about new or existing incidents will be retained and acted upon as appropriate.

Security Incident Prioritization

The ISIRT leader will determine the priority of the incident according to its impact:

1) Critical. A critical level event is an event that can cause significant damage, corruption, or loss (compromise) of confidential, critical and/or strategic organization and student consumer information. The event can result in potential damage and liability to the NWESD 189 and to its public image, and may degrade community confidence concerning its services. Risks of critical incidents include exposure to criminal penalties; exposure to major financial losses; potential threat to life, health or public safety; and/or major damage to reputation or operations. Examples of critical incidents may include:

A) Known or potential theft or loss of confidential NWESD 189 or Protected Health Information (PHI).

B) Disruption of or denial of service attacks of critical systems, including clinical decision-support applications, financial reporting systems, and electronic medical records information.

C) Unauthorized access to security administrator applications or information.

D) All unauthorized computer intrusions, malware infections, any attacks against the technology system infrastructure, etc.

2) Moderate. A moderate level event is an event that may cause damage, corruption, or loss of replaceable information without compromise or may have a moderate impact on the NWESD 189's operations or reputation or may result in legal liability to the NWESD 189. Risks of moderate level incidents include exposure to minor financial losses or minor damage to reputation or operations. Examples of moderate level events may include:

A) An employee viewing the confidential information of a fellow employee without authorization.

B) A "hacked" NWESD 189 system used in attacks on other non-NWESD 189 systems and organizations.

C) A worm causing fraudulent mass emailing from infected systems.

D) A defaced website.

E) Misuse or abuse of authorized access.

F) Accidental intrusion.

G) Confined virus infection.

H) Unusual system performance or behavior.

I) System crashes.

J) Installation of unauthorized software.

K) Unexplained access privilege changes.

L) Unusual after-hour activities, etc.

3) Minor. A minor level event is an event that causes inconvenience, aggravation, and/or minor costs associated with recovery, unintentional actions at the user or administrator level, unintentional damage, or minor loss of recoverable information. The event will have little, if any, material impact on the NWESD 189's operations or reputation. Risks of minor level events include exposure to minimal financial losses, or minimal or no damage to reputation or operations. Examples of minor level events may include:

A) Receipt of a "phishing" email.

B) An employee accessing prohibited websites.

C) Sharing of passwords.

D) Policy or procedural violations, etc.

4) Suspicious Activities. Suspicious activities include observations that indicate possibility of past, current or threatened security incident, but that may be consistent with authorized or non-harmful activities. Examples of suspicious activities include:

A) Access logs showing limited number of unsuccessful attempts by authorized user.

B) An employee loitering near restricted work area beyond his/her authorization.

C) A user returning to workstation to find new application started without his/her authorization, etc.

Response to Security Incident Reports

1) All critical incidents must be investigated and documented as incidents. Moderate or minor incidents will be minimally investigated and documented as incidents, but will receive full investigation and documentation if it is deemed that the incident is unusual and can be learned from so that similar incidents may be prevented in the future. Suspicious activity incidents do not need detailed investigation and documentation as security incidents. However, suspicious activity incidents may be elevated to a higher level by the ISIRT, depending on the incident.

2) The ISIRT leader will notify appropriate persons, such as the Superintendent, law enforcement, etc.

3) Information concerning a computer security incident will be considered confidential and may not be released to individuals not directly involved with the incident and any investigation or response without permission from the Assistant Superintendent for Operations.

Public Response to a Security Incident

1) The ISIRT leader will notify the Superintendent in cases where an incident may have repercussions that need public announcement or response to inquiry by the public, a staff member, a resident, a student consumer, or a consumer's family member.

2) Any announcements to the public or responses to questions from the public about information security incidents will be made only by the Superintendent or his/her designee. The person making such announcements and responses will be advised by the ISIRT leader.

The Information Privacy and Security Incident Response Team (ISIRT)

1) The ISIRT will be responsible for responding to all critical and/or otherwise material security incidents, and will develop procedures and delegate responsibilities for responding to lesser priority incidents.

2) The ISIRT will include the Behavioral Health and Prevention Services Director, Technology Services Director, and Assistant Superintendent for Operations. The ISIRT will be chaired by the Assistant Superintendent for Operations.

3) The ISIRT is responsible for developing and maintaining incident response procedures, and for leading and coordinating responses to incidents.

4) The ISIRT will maintain relationships with and contact information for law enforcement agencies, Internet service providers, third party contractors, NWESD 189 legal counsel, and any other technology experts deemed appropriate or helpful.

Investigating Security Incidents

1) Security incident investigations will be managed by the ISIRT leader, who will call in assistance from other NWESD 189 staff and consultants as necessary to understand the incident, terminate the incident, mitigate any negative effects of an incident, and document the incident and its handling.

2) The owners of any accounts compromised will be notified appropriately so as to maintain confidentiality of the incident pending review by the ISIRT. Once forensic evidence is preserved and review is made possible by the ISIRT, account owners should change their passwords and scrutinize the integrity of the information in affected accounts, providing relevant information about the existence of any security violations to the ISIRT leader or other investigating officer.

3) Any workstations or systems affected by a security incident will be removed from service if it is deemed that doing so will help preserve evidence that may assist in determining the cause or source of the incident, or would help prevent any escalation of the incident. The ISIRT will refer to detailed incident response procedures and act appropriately.

4) Workstations or systems will be examined as appropriate to determine not only the cause of an incident and parties involved, but also what actions may be taken in the future to prevent similar incidents. Usage logs and system access audit tools, as well as any other appropriate forensic tools or activities, will be used as possible and appropriate to provide relevant information during investigation.

5) Information gathered in the investigation of security incidents will be developed and preserved to the greatest extent possible as potential evidence admissible in court in the event it is needed in legal proceedings. Individuals and entities which may be liable for harm caused by the incident will be identified.

6) The ISIRT leader will contact other appropriate responsible individuals or departments, as appropriate in the course of the investigation.

7) In investigating an incident, the investigators will endeavor to get the global picture of all the events that occurred coincident to the incident, and distinguish observations from any assumptions, hearsay, or hypothesis about the incident.

8) Security incidents should be categorized as one or more of the following:

   A) Denial of Service – an event that prevents or impairs the authorized use of networks, systems, or applications.

   B) Malicious Code – a virus, worm, Trojan horse, or other code-based malicious entity that infects a host.

   C) Unauthorized Access – logical or physical access without permission to a network, system, application, data, or other resource.

   D) Inappropriate Usage – a person violating acceptable computer policies.

   E) Social Engineering – an unauthorized attempt by someone masquerading as a legitimate party to elicit information from a staff member that may be used in attempts to compromise the security of systems or accounts.

9) If an incident appears to have been related to illegal activity, or is a security breach of significant scope, the following should be notified, as appropriate, by the Assistant Superintendent for Operations:

   A) State Police

   B) FBI

   C) US Secret Service

10) In cases where civil or criminal charges may be involved, the ISIRT leader will work with the Superintendent and legal counsel to take any legal action required.

11) The Human Resources Department should be involved in any incident investigation that may involve improper activities by employees. Human Resources will be notified by the Assistant Superintendent for Operations.

12) The ISIRT will develop additional procedures to define more detailed steps to be taken in the investigation of and response to various types and priorities of incidents (including response times), and to define the roles of various ISIRT members during an investigation and/or response.

Reporting Breaches of Confidential Information

1) Per the *Health Insurance Portability and Accountability Act* (HIPAA) Breach Notification Rule §164.400 et seq., all breaches of protected health information (PHI) must be reported promptly to the individual, unless A) the PHI is encrypted using processes meeting the requirements of guidance published by the US Department of

Health and Human Services (HHS), or failing that, B) the disclosure is one of the three exceptions to the definition of a breach, as described by HHS, at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html or, failing that, C) a risk assessment determines that there is a low probability of disclosure of PHI.

2) If a disclosure that may be a breach is unencrypted by HHS standards and does not meet one of the three exceptions for reporting as a breach, the disclosure must be treated as a breach unless a risk assessment indicates there is a low probability of disclosure of the PHI involved. In order to determine if there is a low probability of disclosure, the HIPAA breach risk assessment must consider four factors:

   A) the nature of the information (how detailed, how much identifying information, sensitivity, including the potential for "adverse impact" to the individual?);

   B) to whom it was released (was it another healthcare provider?);

   C) whether or not it was actually accessed, used, or disclosed (was it discarded without reading?); and,

   D) how the incident was mitigated (are there assurances that the information disclosed cannot be further used, disclosed, or retained?).

3) Breaches of PHI involving more than 500 individuals must be reported to HHS at the same time the breach is reported to the individual. Breaches involving fewer than 500 individuals must be reported to HHS within sixty (60) days of the end of the calendar year in which they occurred.

4) Breaches of PHI must be reported to individuals, HHS, and the public according to the requirements of HIPAA Breach Notification Rule §164.400 et seq. and any other applicable regulation. See http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html for details.

5) Under Washington State Law, RCW 19.255.010 and 42.56.590, breaches of unsecured personal information must be reported to the affected individuals, unless the information is secured according to the National Institute of Standards and Technology (NIST) standards, or the breach is not likely to cause harm.

6) "Personal Information" under Washington state law is first name or initial, last name, and one or more of the following in unprotected form: (a) Social Security Number, (b) driver's license number or non-driver identification card number, or (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, and does not

include publicly available information lawfully made available to the general public from federal, state, or local government records.

7) Notice under Washington state law must also include notice to the Washington State Attorney General's office, including the number of individuals affected or an estimate thereof.

8) For HIPAA entities, notice under Washington state law may be provided according to HIPAA requirements, as described above in this procedure, but the notifications to individuals and the Attorney General must be made within forty-five (45) days, not the sixty (60) days allowed by HIPAA.

9) Any breaches that may be reportable under law are critical incidents that require involvement by NWESD 189 legal counsel and senior management to ensure that federal and state laws are followed correctly in the provision of various notices and reports to agencies. (Note that breaches of individual information may also be subject to the laws of the state of residence of the individual outside of Washington state, if appropriate.)

Documenting Security Incidents

1) Security incidents, breaches, and any HIPAA breach risk assessments performed to determine whether or not an incident is a reportable breach will be documented according to the documentation procedures identified in this procedure. Incidents must be included in the analysis conducted as part of any compliance evaluation procedures, usage audit, and/or activity review procedures, as appropriate.

2) Information gathered in the investigation of security incidents will be developed and preserved to the greatest extent possible as potential evidence admissible in court in case it is needed in legal proceedings. Whenever possible, any individual or entity that may be liable for harm caused by the incident will be identified, and the ISIRT may seek to have damages quantified for possible use in administrative or legal proceedings.

Presented to Board: 09/24/15
Revised: 10/26/16