

Oneida Tribe of Indians of Wisconsin

BUSINESS COMMITTEE



Oneidas bringing several hundred bags of corn to Washington's starving army at Valley Forge, after the colonists had consistently refused to aid them.



UGWA DEMOLUM YATEHE
Because of the help of this Oneida Chief in cementing a friendship between the six nations and the colony of Pennsylvania, a new nation, the United States was made possible.

P.O. Box 365 • Oneida, WI 54155

Telephone: 920-869-4364 • Fax: 920-869-4040

BC Resolution # 5-04-05-BB

Resolution Adopting Electronic Health Information Security Policies and Procedures for the Oneida Community Health Center and the Oneida Health Care Benefit Plan

- WHEREAS,** the Oneida Tribe of Indians of Wisconsin is a federally recognized Indian government and a treaty tribe recognized by the laws of the United States; and
- WHEREAS,** the Oneida General Tribal Council is the governing body of the Oneida Tribe of Indians of Wisconsin; and
- WHEREAS,** the Oneida Business Committee has been delegated the authority of Article IV, Section 1 of the Oneida Tribal Constitution by the Oneida General Tribal Council; and
- WHEREAS,** one of the purposes of the the Health Insurance Portability and Accountability Act (HIPAA) is to ensure the security of electronic protected health information (HIPAA Security Rules); and
- WHEREAS,** the Indian Health Service has stated that Tribes are required to comply with HIPAA requirements; and
- WHEREAS,** the Oneida Tribe of Indians of Wisconsin has complied with the HIPAA Privacy Rules;
- WHEREAS,** representatives of the Oneida Law Office, the Oneida Community Health Center, the Oneida Employee Insurances Department, and Oneida MIS, in conjunction with Michael Best & Friedrich LLP, have developed HIPAA compliant security policies and procedures for the Tribe's Group Health Plan and Oneida Community Health Center; and
- WHEREAS,** employees who violate the policies and procedures will be subject to discipline under the Personnel Policies and Procedures; and
- WHEREAS,** adoption of the HIPAA Security Policies and Procedures will fulfill the legal obligations imposed by HIPAA Security Rule by protecting the security of electronic health information.

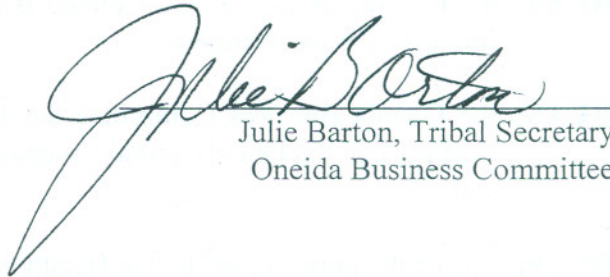
Resolution #5-04-05-BB

Page 2

NOW THEREFORE BE IT RESOLVED, that the attached HIPAA Security Policies and Procedures for the Oneida Community Health Center and the Oneida Health Care Benefit Plan are hereby adopted and shall be effective as of April 20, 2005.

CERTIFICATION

I, the undersigned, as Secretary of the Oneida Business Committee, hereby certify that the Oneida Business Committee is composed of 9 members of whom 5 members constitute a quorum. 5 members were present at a meeting duly called, noticed and held on the 4th day of May, 2005; that the foregoing resolution was duly adopted at such meeting by a vote of 4 members for; 0 members against, and 0 members not voting; and that said resolution has not be rescinded or amended in any way.



Julie Barton, Tribal Secretary
Oneida Business Committee

ONEIDA COMMUNITY HEALTH CENTER
· SECURITY OFFICIAL DESIGNATION

Purpose: This Form is used to designate the health care provider's Security Official.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

After careful consideration, the health care provider determined that it would be prudent to select **Victoria L. Krueger** as the interim Security Official of the (the "Provider"). The Security Official, working in conjunction with the Oneida HIPAA Security Committee, will be responsible for developing and implementing policies and procedures to ensure the confidentiality, integrity and availability of all electronic protected health information created, received, maintained or transmitted by the Provider. This designation is effective April 20, 2005 and shall continue indefinitely until modified by the Provider.

Unless otherwise specified in any policy and procedure, the Security Official shall: (1) take all actions required of the Provider to comply with the Security Rule of the Health Insurance Portability and Accountability Act of 1996; (2) have authority and responsibility to adopt a policy and / or procedure and complete any related forms; (3) have authority to modify a policy and / or procedure and any related forms; (4) have responsibility to retain all policies, procedures, forms, documents and training materials as required by the Security Rule; and (5) periodically review and update all relevant policies, procedures, forms, documents and training materials as needed, in response to environmental or operational changes affecting the security of electronic protected health information.

The Security Official is authorized to create and supervise a Security Committee to assist in carrying out these responsibilities.

Date: April 20, 2005

T:\clienta\045146\0001\A0960117.1

ONEIDA COMMUNITY HEALTH CENTER
RISK ANALYSIS

Purpose: This Form is used to help conduct a risk analysis of the confidentiality, integrity and availability of the health care provider's electronic protected health information. The risk analysis includes electronic protected health information both when it is in transit (for example, sent via email from one entity to another) and at rest (for example, stored on a computer disk).

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Identifying Individuals Involved in Routine Transmissions and Routine Storage.

The following is a list of the health care provider's workforce members who routinely transmit or store electronic protected health information.

1. Name / Position. **Computer Operations and Programming**
2. Name / Position. **Contract Health, Health Center Billing, Pharmacy Registration**
3. Name / Position. **Medical Records, Clinical Lab**
4. Name / Position. **Health Center Administration**
5. Name / Position. **PC Support, Network Administration**
6. Name / Position. **Optical, Dental, Community Health, Clinic**
7. Name / Position. **Anna John Nursing Home: Administration, Nursing, Dietary, Activities**

Note: Attach additional pages as necessary.

SECTION B: Identifying Routine Transmissions of Electronic Protected Health Information.

The individuals identified in Section A routinely transmit electronic protected health information to the following individuals or entities, as applicable. The risk associated with each transmission is also considered. The risk consists of :

- (1) Confidentiality Risk – Whether the information is made available or disclosed to unauthorized persons or processes;
- (2) Integrity Risk – Whether the information has been altered or destroyed in an unauthorized manner;
- (3) Availability Risk – Whether the information is not accessible and not useable upon demand by an authorized person.

1. Transmission of encounter data to Indian Health Service

Confidentiality Risk X Low Medium High

Explanation of analysis: Required government regulatory disclosure.

Integrity Risk X Low Medium High

Explanation of analysis: Transmission is made to a secure site. We receive confirmation of successful transmission.

Availability Risk Low Medium High

Explanation of analysis: N/A

2. Q/S1 Claim adjudication for pharmacy.

Confidentiality Risk Low Medium High

Explanation of analysis: Computer program to computer program communication. No Human intervention. Secured site.

Integrity Risk Low Medium High

Explanation of analysis: No human intervention. Immediate approval/denial response.

Availability Risk Low Medium High

Explanation of analysis: Have two discreet communication paths for adjudication.

3. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

4. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

5. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

6. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

7. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

Note: Attach additional pages as necessary.

SECTION C: Identify Routine Storage of Electronic Protected Health Information.

Electronic protected health information is routinely stored in the following manner and locations:

1. AS/400 databases at the Norbert Hill Center.

Confidentiality Risk Low Medium High

Explanation of analysis: Area is secured at NHC. Off site storage at ARMS.

Integrity Risk Low Medium High

Explanation of analysis: Daily backup with proven technology.

Availability Risk Low Medium High

Explanation of analysis: Access to backup data available on a 24 hour basis.

2. Intel Bases Server at the Health Center

Confidentiality Risk Low Medium High

Explanation of analysis: Automatic backup in a secured environment.

Integrity Risk Low Medium High

Explanation of analysis: Backup process verified daily for successful backup.

Availability Risk Low Medium High

Explanation of analysis: Backup data available on a 24 hour basis.

3. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

4. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

5. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

6. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

Note: Attach additional pages as necessary.

SECTION D: Policy Regarding Non-Routine Transmission and Storage of Electronic Protected Health Information.

It is the policy of the health care provider that transmission and storage of electronic protected health information in a manner other than that identified above will be considered on a case-by-case basis by the Security Official. The Security Official will consider, in each situation, the confidentiality risk, integrity risk and availability risk for each non-routine transmission and storage.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\cienta\045146\0001\A0960138.1

ONEIDA COMMUNITY HEALTH CENTER
SANCTION POLICY

Purpose: This Form is used to develop a sanction policy for the health care provider's workforce, in the event the workforce violates the provider's policies and procedures regarding the security of electronic protected health information.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider's workforce shall comply with the provider's policies and procedures relating to the security of electronic protected health information. Appropriate disciplinary procedures, up to and including termination of employment, will be imposed upon workforce members violating this policy.

SECTION B: Procedure.

1. The Security Official will work with the appropriate Supervisor and the Human Resources Department to determine an appropriate sanction consistent with the requirements of the Oneida Personnel Policies and Procedures or employee contract. Sanctions can include verbal warnings, written warnings, suspension of employment, termination of employment or other appropriate actions.
2. The Security Official shall review and update this Sanction Policy as needed.

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

T:\cienta\045146\0001\A0960159.1

**ONEIDA COMMUNITY HEALTH CENTER
INFORMATION SYSTEM ACTIVITY REVIEW**

Purpose: This Form is used to develop a policy for the health care provider to help ensure that the health provider regularly reviews information system activity relating to electronic protected health information.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health provider that the provider will regularly review records of information system activity. The health provider will do so in order to determine "internal" access from within the health provider's workforce relating to: (1) what electronic protected health information is accessed; (2) who accessed the electronic protected health information; and (3) whether the access was proper.

SECTION B: Procedure.

1. Physical Access. The Security Official has determined that electronic protected health information in physical form (such as storage on a disk, CD-ROM or DVD) is located at the following locations:

- i. Norbert Hill Center (Secured area with proximity cards).
- ii. Oneida Community Health Center (Servers in locked room).
- iii. Social Services (Servers in locked room).
- iv. ARMS (Off site storage vault).
- v. Casino (Server in secured area).

The health provider establishes the following procedure for determining whether an individual has accessed this electronic protected health information stored in physical form: *Access to these areas is restricted and tracked by electronic access badge or manual sign in.*

2. Electronic Access. The Security Official has determined that electronic protected health information in electronic form (such as storage on a computer's hard drive) is located at the following locations:

- i. *Data is stored on Central AS/400 Server or Intel Server. All access to these servers requires authentication to the Network and authorization to any application data base.*

The health provider establishes the following procedure for determining whether an individual has accessed this electronic protected health information stored in electronic form:

The application software tracks who has modified the data. Access to the data is only provided to those individuals requiring access to perform their job duties.

Note: Attach additional pages as necessary.

3. Frequency of Review. The Security Official will conduct an information system activity review every *6 months*.

4. **Use of Information.** The Security Official shall use the information gathered in the review to determine whether electronic protected health information was accessed by an internal user, who accessed the information and whether the access was proper.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0920042.1

ONEIDA COMMUNITY HEALTH CENTER
AUTHORIZATION AND/OR SUPERVISION

Purpose: This Form is used to develop a policy for the health care provider to document whether the provider must have a procedure regarding the authorization and/or supervision of workforce members who will access electronic protected health information.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Authorization and Policy Regarding Authorization.

In *Form 3, Risk Analysis*, the health care provider determined which workforce members typically would need access to electronic protected health information. The Security Official now needs to determine whether it is reasonable and appropriate to pre-authorize or pre-screen workforce members before allowing them access to electronic protected health information. In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk if the health care provider does not pre-authorize or pre-screen a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the provider's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of the health care provider pre-authorizing or pre-screening a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the provider's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Background checks are a part of the standard hiring process.*

3. **Benefit.** Determine or estimate the benefit of the health care provider pre-authorizing or pre-screening a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the provider's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Background checks will detect prior criminal activity.*

4. **Feasibility.** Determine the feasibility of the health care provider pre-authorizing or pre-screening a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the provider's policies and procedures regarding electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: *See explanation in (2) above.*

5. **Policy.** Based on the above, it is the policy of the health care provider that the Security Official, acting through the Human Resources Department *will* pre-authorize or pre-screen workforce members as being trustworthy to obtain electronic protected health information and being able to follow the provider's policies and procedures regarding electronic protected health information.

SECTION B: Determination of Need for Supervision and Policy Regarding Supervision.

The Security Official now needs to determine whether it is reasonable and appropriate to supervise workforce members who access electronic protected health information. In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk that, if the health care provider does not supervise a workforce member, the workforce member will violate the provider's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Risk is medium. Background checks should screen out those individuals who would maliciously violate security policies and procedures.*

2. **Cost.** Determine or estimate the cost of supervising all workforce members to ensure that the member will follow the provider's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Such supervision falls within established chain of command.*

3. **Benefit.** Determine or estimate the benefit of supervising all workforce members to ensure that the member will follow the provider's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Supervision will ensure compliance with policies and procedures.*

4. **Feasibility.** Determine the feasibility of supervising all workforce members to ensure that the members follow the provider's policies and procedures regarding electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: *See (2) above.*

5. **Policy.** Based on the above, it is the policy of the health care provider that the applicable Supervisor will supervise all workforce members to ensure that the members follow the provider's policies and procedures regarding electronic protected health information.

SECTION C: Alternatives if No Authorization or Supervision is Selected

Complete this Section C only if, pursuant to Sections A or B, the health care provider chose not to enact a policy regarding authorization and/or supervision. If a policy was enacted regarding one or the other (for example, a policy was enacted regarding authorization but not supervision) complete this Section C only for the item not enacted (in this example, supervision).

1. **Description of Alternatives.** If the health care provider determined under Sections A and/or B that no authorization and/or supervision was reasonable and appropriate, describe alternative measures the health care provider considered to achieve the same goals of the Authorization and/or Supervision Implementation Standard:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. If more than one alternative measure was proposed attach additional pages as necessary and indicate which alternative measure(s) were selected:

Cost Low Medium High

Benefit Low Medium High

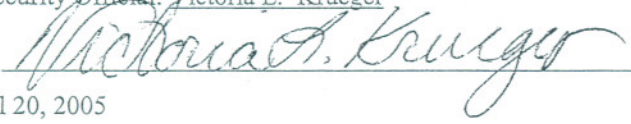
Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, it is the policy of the health care provider that the Security Official will will not enact the alternative measures discussed and selected above.

Name of Security Official: Victoria L. Krueger

Signature: _____



Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960273.1

**ONEIDA COMMUNITY HEALTH CENTER
WORKFORCE CLEARANCE PROCEDURE**

Purpose: This Form is used to document whether the provider must have a procedure regarding the appropriateness of a workforce member's access to electronic protected health information.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Workforce Clearance Procedure.

In *Form 3, Risk Analysis*, the health care provider determined which workforce members typically would need access to electronic protected health information. The Security Official now needs to determine whether it is reasonable and appropriate to have a procedure in place to verify whether it is appropriate for a workforce member to access all or some electronic protected health information. (If the Security Official already knows it is reasonable and appropriate, or has already implemented a Workforce Clearance Procedure, skip (1) – (4) and proceed directly to (5).) In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk if the health care provider does not have a procedure in place to determine whether the workforce member may access all or some electronic protected health information: Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of implementing a procedure to determine whether a particular workforce member may access all or some electronic protected health information: Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of the health care provider establishing a procedure to determine whether a particular workforce member may access all or some electronic protected health information: Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of the health care provider implementing a procedure to determine whether a particular workforce member may access all or some electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, it is the policy of the health care provider that the Security Official will _____ determine whether a particular workforce member may access all or some electronic protected health information.

Attached is the procedure and RFS for requesting access.

SECTION B: Alternatives if No Workforce Clearance Procedure is Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy to determine whether a particular workforce member may access all or some electronic protected health information.

1. Description of Alternatives. If the health care provider determined under Section A that no policy was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Workforce Clearance Implementation Specification:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. If more than one alternative measure was proposed attach additional pages as necessary and indicate which alternative measure(s) were selected:

Cost Low Medium High

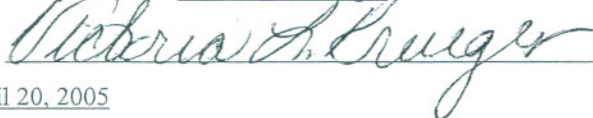
Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, it is the policy of the health care provider that the Security Official will will not enact the alternative measures discussed relating to whether a particular workforce member may have access to electronic protected health information.

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960311.1

January 25, 2001

STANDARD OPERATING PROCEDURE TO REQUEST USER ID'S

Assigning User ID's for training and production purposes for the ENCORE System will be run through the HIS Trainer for the component to be trained in.

HIS Trainer will fill out RFS and forward to appropriate MIS Staff, approximately 3-4 days prior to training session for assignment of User ID's.

These User ID's will be given to the employee at their scheduled training session. At this training, the employee will learn to sign-on to both training and production modules.

If employee does not attend a formal training session, employee will not have access to ENCORE System and no User ID will be assigned.

Approved by Steering Committee
April 5, 2001

c OCHC Supervisors/Directors
SSB Supervisors/Directos

Oneida Tribe of Indians of Wisconsin

Project No.
Assigned

MIS Request for Services

Request Date: March 3, 2005

Requester: Supervisor's Name

Dept: Department

Bldg: OCHC

Phone / Ext#: 869-2711

MIS Category (type an "X" to the left of all that apply)

PC / LAN / WAN AS / 400 RS / 6000 Telecommunications

Request Type (type an "X" to the left of all that apply)

Modification New Software Relocation Acquisition
 Installation Problem Computer Account Information
 User Setup/System Access * Other: **Disconnection and Disablement of User**

Full Time
 Temporary (LTE, ET, Intern) ** Termination Date (MM/DD/YY)
 Other (Please Explain)

Request:

Please disable (**employees name**), (**job title of employee**) @ OCHC from the network, groupwise, internet, and from the AS400 sessions.

Why Required / Expected Benefit:

Will no longer be working at OCHC as of (**termination/leave date**).

Impact on other areas (if any):

Protect Data Integrity and for Tribal Security and Confidentiality Controls

Requested Completion Date (MUST HAVE A DATE HERE FOR MIS TO ROUTE YOUR REQUEST):

GIVE AT LEAST A WEEK'S NOTICE IF POSSIBLE

* User Setup/System Access requires user has read Computer Resources Ordinance and has a signed acknowledgment form on file at HRD.

Supervisor initial this is completed.

Date Signed (MM/DD/YY)

** Supervisors must complete an RFS to terminate system access rights.

MIS Request for Services

Request Date: March 3, 2005

Requester: Supervisor's Name

Dept: Department

Bldg: OCHC

Phone / Ext#: 869-2711

MIS Category (type an "X" to the left of all that apply)

PC / LAN / WAN AS / 400 RS / 6000 Telecommunications

Request Type (type an "X" to the left of all that apply)

Modification New Software Relocation Acquisition
 Installation Problem Computer Account Information
 User Setup/System Access * Other:
 Full Time
 Temporary (LTE, ET, Intern) ** Termination Date (MM/DD/YY)
 Other (Please Explain)

Request:

1. Please set up new (employee name) on the computer station next to along the windows outside office CH-461 with the same access as (current user name of for profile set-up by operations).
2. Please include all G drive access to match that of (current user name of for profile set-up by operations).
3. Please set up AS400/PASS access for (employee name) to match the other Community Health Nurses.
4. Please set up (employee name) the phone with extension 4940 as and set up access to voice mail for her/him.
5. Please set up cell phone number 713-8310 for (employee name). Re-establish voice mail access and new security code.
6. Set up as provider in the IHS system for data entry purposes.

Why Required / Expected Benefit:

Needed in order to complete job duties.

Impact on other areas (if any):

New employee

Requested Completion Date (MUST HAVE A DATE HERE FOR MIS TO ROUTE YOUR REQUEST):

GIVE AT LEAST A WEEK'S NOTICE

* User Setup/System Access requires user has read Computer Resources Ordinance and has a signed acknowledgment form on file at HRD.

Supervisor initial this is completed.

Date Signed (MM/DD/YY)

** Supervisors must complete an RFS to terminate system access rights.

ONEIDA COMMUNITY HEALTH CENTER
TERMINATION PROCEDURES

Purpose: This Form is used to document whether the health care provider must have a procedure regarding the termination of a workforce member who had access to electronic protected health information.

Retention: This Form must be retained in the provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Termination Procedure.

In *Form 3, Risk Analysis*, the health care provider determined which workforce members typically would need access to electronic protected health information. The Security Official now needs to determine whether it is reasonable and appropriate to establish an access termination procedure for when a workforce member terminates employment or when it is reasonably required under the Workforce Clearance Procedure Implementation Specification. (If the Security Official already knows it is reasonable and appropriate, or has already implemented a Termination Procedure, skip (1) – (4) and proceed directly to (5).) In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk if the health care provider does not have a procedure in place regarding the termination of employment of a workforce member who had access to electronic protected health information: Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of implementing a procedure regarding the termination of employment of a workforce member who had access to electronic protected health information: Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of implementing a procedure regarding the termination of employment of a workforce member who had access to electronic protected health information: Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure regarding the termination of employment of a workforce member who had access to electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider x will will not adopt a policy and procedure regarding the termination of employment of a workforce member who had access to electronic protected health information. If selected, the policy and procedure is as follows:

It is the policy of the health care provider that the provider will take reasonable and appropriate steps to ensure that electronic protected health information is not accessed by workforce members who have terminated employment. The Security Official shall take all necessary steps to ensure this policy is implemented. These steps include the following, all to be taken as soon as reasonably possible:

- Determining what electronic protected health information the person had access to, in order to determine what the person may have retained or may still be able to access;
- X Requiring the return of all keys that can lead to access of electronic protected health information;
- X Turning off card keys or other electronic equivalents;
- X Requiring the return of laptops and other electronic media, such as computer disks, CD-ROMs and DVDs;
- X Removing the person as an authorized user; and/or
- _____

SECTION B: Alternatives if No Termination Procedure is Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding the termination of employment of a workforce member who had access to electronic protected health information.

1. Description of Alternatives. If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Termination Procedure Implementation Specification:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. If more than one alternative measure was proposed attach additional pages as necessary and indicate which alternative measure(s) were selected:

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: *[Describe policy and procedure; may want to base language off Section A(5), above.]*

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960425.1

Hiring Department; Employee Separations

When an employee separates employment, it is extremely important that the Separation Report is sent by the supervisor to the Human Resource Department Representative immediately.

The Document has several purposes which benefit the employee, supervisor, and the organization:

- It immediately stops the employee's benefits at Midnight of the date of separation.
- Employee Insurance Department will send information regarding COBRA to offer continuing employee medical coverage.
- It immediately stops all Payroll Deductions.
- Payroll, upon receiving the separation date, will payout all vacation and personal time to the employee.
- HRD will have the correct Workforce Levels for Reporting Purposes to Department Managers and external agencies as required by law.

As a supervisor, you need to do more than just send the Separation Form to HRD, here's a checklist to help you remember to:

- Notify MIS to revoke all PC access.
- Collect Tribal property, such as; keys, Kronos badge, cell phone, laptop, PDA, etc....
-

Please send Separations to Your HR Representatives by Division:

Gaming Division: Terry Skenandore or Marilyn Jourdan

Governmental Services, Development Division, Enterprise Division and Compliance Division: Lisa Hock or Wanita DeCorah

Internal Services Division, Land Management Division, Transit, Oneida Police Department, Non-Divisional Departments, Boards, Committees, Commissions: Lisa Duff

HRD Telephone Number: 496-7900

SEPARATION SECURITY FORM

Form #HRD203

Employee's Name: _____ Employee Number: _____

Employee's Department: _____ Employee's Division: _____

Employee's Separation Date: _____ Employee's Title: _____

Supervisor's Name: _____ Supervisor's Title: _____

Listed below are Tribal items which must be returned prior to the employee separating from employment. If the employee does not have the particular item, please write N/A for not applicable.

<u>ITEM</u>	<u>DATE RETURNED</u>
a. Employee Badge	a. _____
b. Desk Keys	b. _____
c. Door Keys	c. _____
d. Security Access/Code	d. _____
e. Beeper	e. _____
f. Cell Phone	f. _____
g. Lap Top Computer	g. _____
h. Tribal Documents taken Home	h. _____
i. Uniforms	i. _____

Supervisor must follow through with the items listed below, as applicable:

<u>ITEM</u>	<u>DATE COMPLETED</u>
1. Contact the Kronos Administrator to have employee removed from Kronos	1. _____
2. Contact MIS to have the employee removed from Group Wise, Infinium, and computer access.	2. _____
3. Schedule appointment for return of items listed as Employee Property.	3. _____

<u>ITEM</u>		<u>DATE COMPLETED</u>
4.	Complete the Separation Report and/or the Disciplinary Form and send to HRD for the Employee to be paid our vacation/personal time.	3. _____
5.	Contact Accounting to remove all sign-off Authority.	4. _____
6.	Contact Building Administrator to remove Building Security codes, eye dots, etc.	5. _____
7.	Assess whether work area locks and security codes need to be changed	6. _____

EMPLOYEE SEPARATION REPORT

(Print)

Name: _____ Empl #: _____
Last First M.I.

Job Title: _____ Separation Date: _____

Department: _____ Division: _____

TYPE OF SEPARATION:

- Resignation (attach letter)
 Termination
 Deceased
 Denial of LOA
 Transfer/Reassignment
 Retirement
 Lay-Off (26 wk)
 Other _____

REASON FOR SEPARATION:

- Working Conditions
 Reduction in Force
 Job Change within Oneida Tribe Where: _____
 Policy Violation _____
 Other _____

INVESTIGATION PENDING AT TIME OF SEPARATION: Yes No

EMPLOYEE EVALUATION (please check appropriate boxes):

	Unsatisfactory	Satisfactory	Excellent
Attendance			
Cooperation			
Initiative			
Job knowledge			
Quality of work			

REHIRE: Yes No (See attached documentation)

Additional Comments: _____

 Supervisor Signature

 Date

 Supervisor Name (Print)

ONEIDA COMMUNITY HEALTH CENTER
INFORMATION ACCESS MANAGEMENT

Purpose: This Form is used to document the health care provider's decision whether to implement policies and procedures regarding the Access Authorization and Access Establishment and Modification Implementation Specifications. If either Specification is selected, this Form establishes the provider's policies and procedures regarding the selected Specification(s).

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Access Authorization and Access Establishment and Modification.

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Access Authorization—Implement policies and procedures for granting access to electronic protected health information.
- Access Establishment and Modification—Implement policies and procedures that, based upon the health care provider's Access Authorization policies, establishes, documents, reviews and modifies a user's right of access to a workstation, transaction, program or process.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Access Authorization and Access Establishment and Modification Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- Access Authorization Low Medium High
- Access Establishment and Modification Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Access Authorization Low Medium High
- Access Establishment and Modification Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Access Authorization Low Medium High
- Access Establishment and Modification Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Access Authorization Feasible and Not Difficult Feasible but Difficult Not Feasible
- Access Establishment and Modification Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider **will not** adopt a policy and procedure regarding the following Implementation Specifications:

- X Access Authorization
- X Access Establishment and Modification

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

It is the policy of the health care provider that the provider will take reasonable and appropriate steps to ensure that only approved workforce members or others may have access to electronic protected health information. It is the policy of the provider that the granting of such access may be modified by the Security Official when the Security Official deems reasonable and appropriate. The Security Official shall take all necessary steps to ensure this policy is implemented. These steps include the following:

- X Ensuring that access is granted only on a case-by-case basis and is not automatic for every workforce member;
- X Establishing passwords on computer systems and providing passwords only to approved workforce members and others;
- X Establishing screen savers on computers with passwords required in order to access the computer after a certain period of inactivity;
- X Communicating passwords to workforce members in a secure manner (e.g., not using interoffice routing in a non-secure envelope);
- X Working with the Human Resources Department and MIS so that the Security Official is notified promptly of any new members added to the provider's workforce and of any termination of a workforce member or change in that member's job functions that could affect the member's ability or authority to access electronic protected health information;
- X Documenting any granting of access or modification of access and notifying the following departments or areas of the granting of such access or modification of such access:

Oneida MIS

Oneida Community Health Center

X Establishing different categories of electronic protected health information and establishing passwords to ensure that workforce members have access only to the category of electronic protected health information appropriate to the particular member; and/or

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows:

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960432.1

**ONEIDA COMMUNITY HEALTH CENTER
SECURITY AWARENESS AND TRAINING**

Purpose: This Form is used to document the health care provider's decision whether to implement policies and procedures regarding the Security Awareness and Training Standard. The Form also establishes any selected policies and procedures related to the Standard.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Security Awareness and Training

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement none, some or all of the Implementation Specifications:

- Security Reminders—Periodic security updates.
- Protection From Malicious Software—Guarding against, detecting and reporting malicious software.
- Log-in Monitoring—Monitoring log-in attempts and reporting discrepancies.
- Password Management—Creating, changing and safeguarding passwords.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented a particular Specification, skip (1) – (4) for that Specification and proceed directly to (5).)

1. Risk. Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- Security Reminders Low Medium High
- Protection From Malicious Software Low Medium High
- Log-in Monitoring Low Medium High
- Password Management Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Security Reminders Low Medium High
- Protection From Malicious Software Low Medium High
- Log-in Monitoring Low Medium High
- Password Management Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Security Reminders Low Medium High
- Protection From Malicious Software Low Medium High
- Log-in Monitoring Low Medium High
- Password Management Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Security Reminders Feasible and Not Difficult Feasible but Difficult Not Feasible
- Protection From Malicious Software Feasible and Not Difficult Feasible but Difficult Not Feasible
- Log-in Monitoring Feasible and Not Difficult Feasible but Difficult Not Feasible
- Password Management Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider will will not adopt a policy and procedure regarding the following Implementation Specifications:

- X Security Reminders.
- X Protection From Malicious Software.
- X Log-in Monitoring.
- X Password Management.

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Security Reminders.** The health care provider's policy is to issue security reminders to relevant workforce members as reasonable and appropriate. The provider will determine the topics for the reminder and the method of distributing the reminder. The provider will document, and retain for six (6) years, proof of the reminder. The reminder will be distributed on an as needed basis.

• **Protection From Malicious Software.** The health care provider's policy is to have protection from malicious software. The provider will examine its vulnerability to particular, known malicious software. The provider will:

X License or purchase software designed to combat malicious software; and / or

The health care provider will take steps to ensure that it maintains current knowledge about malicious software. These steps include:

X Updating the software used to combat malicious software;

X Subscribing to trade publications, newsletters and other periodic resources that provide information on current developments; and / or

The health care provider will take steps to ensure that appropriate, current software (if selected above) is placed on each computer or server that could be affected by malicious software, including portable computers such as laptop computers.

All incoming email messages will be scanned for malicious software. If a workforce member has security concerns about an attachment to an email message the member shall contact the Security Official prior to opening the attachment. Workforce members are not allowed to download software onto their computers unless the Security Official has approved the software. The Security Official shall, if appropriate, use Form 11, Workforce Member Training, to train all workforce members on these policies and procedures regarding Protection From Malicious Software.

• **Log-in Monitoring.** The health care provider's policy is to monitor log-in attempts of users. If the log-in is successful on the first attempt no log-in report will be generated. If the log-in is unsuccessful after 3 (three) consecutive attempts, the user will be locked out of the system. The user will be required to contact MIS operations to access the network after being locked out.

• **Password Management.** The health care provider's policy is that passwords are an important security provision and appropriate steps will be taken to ensure the use and confidentiality of passwords. The health care provider implements the following requirements regarding passwords:

X Passwords will have a minimum length of 8 characters;

Passwords will include both numeric and alphabetic characters;

Passwords should contain both upper and lower case characters (e.g., a-z, A-Z);

Passwords should not be based on personal information (e.g., spouse's name, street address);

Passwords shall not be composed of only one character (e.g., aaaaaa);

X Publishing or sharing of passwords is not allowed;

X Passwords should not be written down but, if they are written down, shall be stored in a secure (preferably locked) location;

X Passwords will be changed every 90 days;

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: [*Describe policy and procedure; may want to base language off Section A(5), above.*]

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960437.1

ONEIDA COMMUNITY HEALTH CENTER

WORKFORCE MEMBER TRAINING

Purpose: This Form is used to determine which components of the Security Rule, if any, should be explained to the health care provider's workforce as part of the provider's training under the Security Rule.

Retention: This Form should be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Identification of Potential Components Requiring Training.

The Security Official should review the following list of Security Rule components. The Security Official should determine which, if any, components should be explained to the provider's workforce. For example, the Security Official may determine that only a few components (such as changing passwords and informing workforce members about proper workstation use) should be explained to the provider's workforce. The Security Official should document the selected components.

ADMINISTRATIVE SAFEGUARDS

Standards	Implementation Specifications	Workforce Training/Explanation Required?	
Security Management Process	Risk Analysis	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Risk Management	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Sanction Policy	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Information System Activity Review	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Assigned Security Responsibility		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Workforce Security	Authorization and/or Supervisions	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Workforce Clearance Procedure	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Termination Procedures	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Information Access Management	Isolating Health Care Clearinghouse Function	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Access Authorization	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Access Establishment and Modification	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Security Awareness and Training	Security Reminders	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Protection from Malicious Software	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Log-in Monitoring	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Password Management	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Security Incident Procedures	Response and Reporting	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Contingency Plan	Data Backup Plan	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Disaster Recovery Plan	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Emergency Mode Operation Plan	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Testing and Revision Procedure	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Applications and Data Criticality Analysis	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Evaluation		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Business Associate Contracts and Other Arrangement	Written Contract or other Arrangement	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

PHYSICAL SAFEGUARDS

Standards	Implementation Specifications	Workforce Training/Explanation Required?	
Facility Access Controls	Contingency Operations	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Facility Security Plan	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Access Control and Validation Procedures	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Maintenance Records	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Workstation Use		<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Workstation Security		<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Device and Media Controls	Disposal	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Media Re-use	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Accountability	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Data Backup and Storage	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

TECHNICAL SAFEGUARDS

Standards	Implementation Specifications	Workforce Training/ Explanation Required?	
Access Control	Unique User Identification	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Emergency Access Procedure	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Automatic Logoff	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Encryption and Decryption	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Audit Controls		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Integrity	Mechanism to Authenticate Electronic Protected Health Information	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Person or Entity Authentication		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Transmission Security	Integrity Controls	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Encryption	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

SECTION B: Preparation of Training Materials.

The Security Official should prepare appropriate training materials that will inform the workforce members of the items specified above. These training materials can include any appropriate items, such as an electronic presentation or written materials.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960443.1

ONEIDA COMMUNITY HEALTH CENTER

RESPONSE AND REPORTING

Purpose: This Form is used to develop a policy for the health care provider to: identify and respond to suspected or known security incidents involving electronic protected health information; mitigate, to the extent practicable, harmful effects of security incidents known to the health care provider; and document security incidents and their outcomes.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will:

- Identify and respond to suspected or known security incidents involving electronic protected health information;
- Mitigate, to the extent practicable, harmful effects of security incidents known to the provider; and
- Document security incidents and their outcomes.

All such actions shall be taken by the Security Official as promptly as possible after learning of a security incident or suspected security incident.

SECTION B: Procedure.

1. Once the health care provider becomes aware of a security incident or potential security incident, the Security Official will use the Security Incident Type Matrix, below, to verify that a security incident occurred and determine the level of severity of the security incident.

- Description of Security Incident or Potential Security Incident, including workforce members and equipment involved: _____
- _____

SECURITY INCIDENT TYPE MATRIX

INCIDENT TYPE	INCIDENT DESCRIPTION	EXAMPLES
<u>Low Risk</u>	Isolated incidents attributable to common non-malicious behavior that are determined to be non-threatening.	<ul style="list-style-type: none"> • Typographical errors • Forgotten passwords
<u>Moderate Risk</u>	Any event or pattern of events (malicious or unintentional) that indicate a potential threat to electronic protected health information.	<ul style="list-style-type: none"> • Patterns of repeated Low Risk incidents • Suspicious patterns of incoming data from external sources • Information that email attachments are being opened without proper consideration of risks • Unattended workstation • Backup failure • Misdirected email containing electronic protected health information
<u>High Risk</u>	Any event or pattern of events (malicious or unintentional) that indicate a significant, current threat to electronic protected health information.	<ul style="list-style-type: none"> • Password sharing • IP address spoofing • Unauthorized physical access to health care provider facility • Intentional or inadvertent destruction of electronic protected health information • Denial of Service attack • Misuse of high-level access accounts • Computer virus exposure/propagation • Lost or stolen workstations or other media (e.g., disks, CD-ROMs) • Escalation of any combination of Low Risk and Moderate Risk security incidents • Improper computer disposal

- Current Classification of Security Incident: Low Risk Moderate Risk High Risk

Explanation of analysis: _____

2. Explain the steps taken to minimize the harmful effect of the security incident: _____

3. Review the possible responses to the security incident using the Security Incident Response Matrix as a guide. Recognize that the response in any particular circumstance must be determined on a case-by-case basis and that the Response Matrix cannot provide guidance on every possible response.

SECURITY INCIDENT RESPONSE MATRIX

INCIDENT LEVEL	INCIDENT RESPONSE
<u>Low Risk</u>	<ol style="list-style-type: none"> 1. Incident reported to Security Official on non-expedited basis (e.g., weekly reports or interoffice routing). 2. Logging and monitoring shall be intensified when deemed reasonable and appropriate by the Security Official. 3. Consider whether it is appropriate to log report of situation.
<u>Moderate Risk</u>	<ol style="list-style-type: none"> 1. Incident shall be immediately reported to Security Official. 2. Security Official shall immediately review the incident to determine if action needs to be taken. 3. The party (or parties) involved with and/or responsible for the threat shall be contacted to obtain details of the potential security threat. 4. If immediate action is not necessary, logging and monitoring of the potential security threat shall be intensified when deemed reasonable and appropriate by the Security Official. 5. If workforce member is involved, contact member and discuss situation. 6. Incident and incident resolution details shall be documented and logged.
<u>High Risk</u>	<ol style="list-style-type: none"> 1. Incident shall be immediately reported to Security Official. 2. Security Official shall immediately review the incident to determine what action will be taken. 3. Incident shall be noted and logged separately from the initial security incident logs and reported directly to other management, if deemed reasonable and appropriate by the Security Official. 4. The party (or parties) involved with and/or responsible for the threat shall be notified and advised about the details of the security threat. 5. If workforce member is involved, contact member and discuss situation. Involve Human Resources Department, for potential disciplinary action, as Security Official deems reasonable and appropriate. 6. Consider whether to contact law enforcement authorities if criminal activity is suspected.

- Based on the above Security Incident Response Matrix, describe the actions taken: _____

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0960444.1

ONEIDA COMMUNITY HEALTH CENTER

CONTINGENCY PLAN

Purpose: This Form is used to document the health care provider's contingency plans to help secure electronic protected health information. This Form also establishes the plan's policies and procedures regarding the contingency plan.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Data Backup Plan Policy

It is the policy of the health care provider to have a data backup plan to help secure electronic protected health information. The backup plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The backup plan will be designed to create and maintain retrievable exact copies of electronic protected health information.

SECTION B: Data Backup Plan Procedures

The following backup procedures, if chosen, shall be followed:

1. **Data Included in Backup Plan.** The following data will be subject to the backup plan:

All electronic protected health information held by the provider's workforce on servers or AS 400

2. **Frequency of Backup.** Data will be backed up daily.

3. **Storage of Backup Data.** Data that has been backed up will be stored by a third party vendor: (1) on a daily basis for AS 400 and (2) on a weekly basis for the server.

4. **Performing of Backup.** Data will be backed up by Oneida MIS via software.

5. **Integrity of Backups.** The backups will be examined and audited every day by Oneida MIS to verify the integrity of the backed up data.

SECTION C: Disaster Recovery Plan Policy

It is the policy of the health care provider to have a disaster recovery plan. The disaster recovery plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The disaster recovery plan will be designed to restore any loss of relevant electronic protected health information.

SECTION D: Disaster Recovery Plan Procedures

1. **Assessment of Damage and Loss of Data.** The Security Official, in conjunction with MIS management, will gather as much information as possible to determine how much electronic protected health information was lost in a disaster. The Security Official, in conjunction with MIS management will gather information about each potentially affected area where electronic protected health information was stored.

— 2. **Designee of Security Official.** In the event the Security Official is unavailable, the Security Official designates Oneida MIS Manager to act in place of the Security Official. The Security Official will communicate this designation to the designated individual.

3. **List of Third Party Vendors.** The Security Official will determine, prior to any disaster, which third party vendors are likely to be available to assist in recovering the data (e.g., a vendor who holds backup data or a vendor who specializes in recovering data from damaged computers) or providing additional equipment. Vendors and their anticipated roles are as follows :

Vendor	Role
HP/Bedrock	Replacement of server hardware
Computech	Equipment for restoration of AS-400

4. **General Procedures for Restoring Information System.** MIS Network Team will rebuild server with operating system and restore server data from tape.

SECTION E: Emergency Mode Operation Plan Policy

It is the policy of the health care provider to establish and implement an emergency mode operation plan. The emergency mode operation plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The emergency mode operation plan will be designed to enable the provider to continue critical business processes for protecting the security of electronic protected health information while operating in emergency mode.

SECTION F: Emergency Mode Operation Plan Procedures

1. **Reassignment of Duties.** The Security Official will consider which operations are most critical based on the particular emergency encountered by the plan. The Security Official should reassign duties if necessary (e.g., critical functions may take priority over long-term projects). The Security Official should promptly discuss any reassignments with affected workforce members.

2. **Physical Security.** The Security Official will consider whether additional physical security (e.g., a locking file cabinet to hold disks or CD-ROMs) is necessary due to the emergency situation. If so, the Security Official will obtain necessary items as soon as reasonably possible. If it is reasonably possible to anticipate what physical security items will be required, the Security Official should list those items here: secured site will be designated by director of MIS on a case by case basis. Backup tapes and data will be collected and brought to that area.

3. **Technical Security.** The Security Official will work with the workforce and appropriate third party vendors to implement any technical security mechanisms required due to the emergency situation.

SECTION G: Testing and Revision Procedures and Applications and Data Criticality Analysis

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Testing and Revision Procedures—Implement procedures for periodic testing and revision of contingency plans.
- Applications and Data Criticality Analysis—Assess the relative criticality of specific applications and data in support of other contingency plan components.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and

appropriate, or has already implemented both Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. **Risk.** Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- Testing and Revision Procedures Low Medium High
- Applications and Data Criticality Analysis Low Medium High

Explanation of analysis

2. **Cost.** Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Testing and Revision Procedures Low Medium High
- Applications and Data Criticality Analysis Low Medium High

Explanation of analysis

3. **Benefit.** Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Testing and Revision Procedures Low Medium High
- Applications and Data Criticality Analysis Low Medium High

Explanation of analysis:

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Testing and Revision Procedures Feasible and Not Difficult Feasible but Difficult Not Feasible
- Applications and Data Criticality Analysis Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: Contingency testing is not a feasible option for programs residing on the AS/400. To test the contingency plan would involve an expenditure of \$1 million or more to get a second AS/400. This option is neither practical nor feasible.

5. **Policy.** Based on the above, the health care provider **will not** adopt a policy and procedure regarding the *Testing and Revision Procedures Implementation Specification*. The health care provider **will** adopt a policy and procedure regarding the *Applications and Data Criticality Analysis Implementation Specification*.

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

• **Applications and Data Criticality Analysis**

It is the policy of the health plan to conduct an applications and data criticality analysis. The analysis will include the following:

- X Identification of systems which are the most important parts of the contingency plan;
- X Identification of how the systems interact in order to recognize potential failures if one or several systems are not available;
- X Identification of reasonable and appropriate modifications that can be made to address potential failures

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

See G(4) above. Alternatives include restoring server from off-site tape back-up. _____

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: The alternative selection is the current procedure.

3. Policy. Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: See B(1) above.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria A. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0921186.1

ONEIDA COMMUNITY HEALTH CENTER EVALUATION

Purpose: This Form is used to document how the health care provider will evaluate its security policies and procedures to ensure they comply with the Security Rule.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Evaluation Policy

It is the policy of the health care provider to conduct a periodic technical and nontechnical evaluation of its security policies and procedures to determine if those policies and procedures, and the implementation of those policies and procedures, complies with the Security Rule. The Security Official, in conjunction with the Security Committee will decide the proper way to conduct this evaluation and how often to conduct the evaluation.

SECTION B: Evaluation Procedures

1. Entity to Conduct Evaluation. The Security Official, in conjunction with the Security Committee must determine who will conduct the evaluation. The Security Official first must determine whether the evaluation will be performed by a workforce member (such as the Security Official) or a third party (such as a consultant or attorney). The Security Official will consider the following factors:

- Cost of evaluation;
- Expected thoroughness of evaluation;
- Understanding of the health care provider and its operations;
- Understanding of security policies and procedures;
- Whether a technical evaluation could be conducted by one entity, while a nontechnical evaluation could be conducted by another entity;
- Consideration of advantages and disadvantages of having a third party conduct the evaluation. Advantages include separating the responsibility of creation and oversight (e.g., so the Security Official is not evaluating the Security Official's own work) and perhaps being able to hire an expert with additional technical and nontechnical experience in the area. Disadvantages include the potential additional time to conduct the analysis and cost.

Based on the above considerations, **Oneida MIS** will conduct the technical evaluation. Based on the above considerations, **Deloitte and Touche or other reputable third party auditor** will conduct the nontechnical evaluation.

2. Frequency of Evaluation. The evaluation initially will occur every year. The Security Official will reconsider every year whether the evaluation period should be modified.

3. Use of Evaluations. The Security Official will consider the results of the evaluations and make all reasonable and appropriate modifications to the provider's security policies and procedures.

4. Retention of Evaluation Results. The Security Official will retain the results of the evaluation for at least six (6) years after the completion of the evaluation.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0960450.1

SECTION 1. Evaluation Policy

It is the policy of the health care provider to conduct a periodic technical and non-technical evaluation of its security posture and processes to determine if there are changes and the implementation of those changes and procedures to ensure they comply with the security risks. The Security Official, in consultation with the Security Committee, will develop the paper work to conduct the evaluation and how often to conduct the evaluation.

SECTION 2. Frequency of Evaluation

1. Entry to Conduct Evaluation. The Security Official, in consultation with the Security Committee, will determine who will conduct the evaluation. The Security Official may determine whether the evaluation will be conducted by a workforce member (such as the Security Official) or a third party (such as a consultant or attorney). The Security Official will consider the following factors:

- Cost of evaluation
- Impact to operations of evaluation
- Understanding of the health care provider and its operations
- Understanding of security posture and procedures
- Whether a consultant - evaluation would be conducted by one entity, with a consultant evaluation could be conducted by another entity

• Identification of strengths and weaknesses of having a third party conduct the evaluation. Advantages include separating the responsibility of control and oversight (e.g., the Security Official) from the responsibility of execution (e.g., the third party). Disadvantages include the potential additional time to conduct the evaluation and cost.

Based on the above considerations, the Security Official will conduct the technical evaluation. Based on the above considerations, the Security Official will conduct the non-technical evaluation.

2. Frequency of Evaluation. The evaluation generally will occur every year. The Security Official will determine every year whether the evaluation period should be modified.

3. Use of Evaluation. The Security Official will consider the results of the evaluation and make all necessary and appropriate modifications to the provider's security policies and procedures.

4. Retention of Evaluation Results. The Security Official will retain the results of the evaluation for a least six (6) years after the completion of the evaluation.

ONEIDA COMMUNITY HEALTH CENTER
FACILITY ACCESS CONTROLS

Purpose: This Form is used to document the health care provider's decision whether to implement policies and procedures regarding the Facility Access Controls Standard. The Form also establishes any selected policies and procedures related to the Standard.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Facility Access Controls

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement none, some or all of the Implementation Specifications:

- Contingency Operations—Procedures to allow access to the provider's facility to help restore data lost in an emergency, considering the disaster recovery plan and emergency mode operations plan.
- Facility Security Plan—Policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering and theft.
- Access Control and Validation Procedures—Procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.
- Maintenance Records—Policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented all these Specifications, skip (1) – (4) and proceed directly to (5).)

1. **Risk.** Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- Contingency Operations Low Medium High
- Facility Security Plan Low Medium High
- Access Control and Validation Procedures Low Medium High
- Maintenance Records Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Contingency Operations Low Medium High
- Facility Security Plan Low Medium High

- Access Control and Validation Procedures Low Medium High
- Maintenance Records Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Contingency Operations Low Medium High
- Facility Security Plan Low Medium High
- Access Control and Validation Procedures Low Medium High
- Maintenance Records Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Contingency Operations Feasible and Not Difficult Feasible but Difficult Not Feasible
- Facility Security Plan Feasible and Not Difficult Feasible but Difficult Not Feasible
- Access Control and Validation Procedures Feasible and Not Difficult Feasible but Difficult Not Feasible
- Maintenance Records Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider **will** adopt a policy and procedure regarding the following Implementation Specifications:

- X Contingency Operations.
- X Facility Security Plan.
- X Access Control and Validation Procedures.
- X Maintenance Records.

_____ The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Contingency Operations.** The health care provider's policy is to have a policy allowing reasonable facility access to authorized personnel to restore data lost (or perhaps lost) due to an emergency. This policy will work in conjunction with any disaster recovery plan and emergency mode operations plan. The Security Official will first determine the risk of accessing the provider's physical structure (e.g., if the building was damaged due to a tornado, whether it is safe to enter the building). The Security Official will work with local authorities to help make this determination.

The Security Official will, if reasonable and appropriate, accompany the workforce member or third party vendor when they work to recover the lost data. The Security Official will consider whether any third parties will be considered business associates. If so, the Security Official will enter into a business associate agreement with the third party vendor prior to any emergency.

- **Facility Security Plan.** The health care provider's policy is to have procedures to safeguard the provider's facility and equipment therein from unauthorized physical access, tampering and theft. The health care provider will:

- X Provide identification badges to all workforce members and require that the badges be worn at all times while at work;

- X Require visitors and vendors to sign in and out when visiting the provider's facilities, and maintaining that log for at least 6 months.

- X Identify areas which, due to the sensitivity of the electronic protected health information stored at the area, may not be accessed by certain classes of workforce members, visitors or vendors. These areas include:

All electronic EPHI is stored on the Casino Server, the Health Center Server, the Social Services Server and AS-400. Only authorized individuals may access these areas.

The Security Official will ensure that workforce members, visitors or vendors are not allowed access to this area by:

- x Physical security measures (e.g., locked doors or electronic key card access required);

- x Stationing of Personnel (e.g., having a receptionist placed near the site to verify that no access occurs); and / or

- x Requiring key or proximity card to access

- X Examining physical structures (e.g., doors and windows) to assess vulnerability to intrusion;

- **Access Control and Validation Procedures.** The health care provider's policy is to establish a procedure to control and validate a person's access to the provider's facilities, based on the person's role or function. This includes visitor control, and control of access to software programs for testing and revision. The health care provider will (note: some items duplicative of Facility Security Plan procedure, above):

- X Provide identification badges to all workforce members and require that the badges be worn at all times while at work;

- X Require visitors and vendors to sign in and out when visiting the provider's facilities, and maintaining that log for at least 6 months.

- X Identify areas which, due to the sensitivity of the electronic protected health information stored at the area, may not be accessed by certain classes of workforce members, visitors or vendors. These areas

include: *All electronic EPHI is stored on the Casino server, Health Center Server, and AS-400. Only authorized workforce members may access these areas.*

The Security Official will ensure that workforce members, visitors or vendors are not allowed access to this area by:

- X Physical security measures (e.g., locked doors or electronic key card access required);
- X Stationing of Personnel (e.g., having a receptionist placed near the site to verify that no access occurs); and / or
- X Requiring that only a select group of authorized information technology workforce members are able to access software programs for testing and revision, with the select group specified by the Security Official. To ensure that only the select group has such access, the provider will:
 - X Design its computer specifications so that only authorized users are able to access software programs for testing and revision purposes;
 - X Not leave software in an unsecured location; and / or
 - X Provide for discreet testing environments;

• **Maintenance Records.** The health care provider's policy is that it will establish a procedure to document repairs and modifications to the physical components of a facility which are related to security (including but not limited to hardware, walls, doors and locks). All actions are to be taken by the Security Official, acting through Oneida MIS, as promptly as reasonably possible. The health care provider establishes this procedure by adopting the following components:

- X The Security Official will consider all proposed maintenance to the facility to determine the security issues, if any, raised by the maintenance;
- X If the provider's facilities are shared with another entity, the Security Official will discuss the provider's need to be apprised, in advance when possible, of maintenance that could impact the provider's physical security;
- X Records describing the maintenance work and who performed the work shall be retained for at least one year.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: [*Describe policy and procedure; may want to base language off Section A(5), above.*]

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0960452.1

ONEIDA COMMUNITY HEALTH CENTER
WORKSTATION USE

Purpose: This Form is used to develop a policy and procedure for the health care provider regarding the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will have a procedure governing its workforce's use of computer workstations. This policy will specify: (1) the proper functions to be performed; (2) the manner in which those functions are to be performed; and (3) the physical attributes of the surroundings of a specific workstation or class of workstation, if that workstation can access electronic protected health information.

SECTION B: Procedure.

1. Proper Functions to be Performed. The Security Official will determine which functions are appropriate for particular workstations. For example, the Security Official may determine that it is not proper to access electronic protected health information at a workstation that cannot be reasonably secured (e.g., a receptionist's workstation where many visitors could view the screen). The Security Official may also determine that some workstations should not be used for some purposes. For example, if a computer's hard drive contains significant electronic protected health information that is not stored elsewhere, and there is concern about malicious software for which no effective remedy is available, the Security Official may direct that that particular computer not be used to open email or download files from the Internet due to concerns about the malicious software.

Considering these factors, the Security Official implements the following procedure: *Employees with access to EPHI shall only access such EPHI from appropriate workstations as designated by provider. Existing policies restrict what users may or may not do at Windows workstations.*

2. Manner in Which Functions are to be Performed. All provider workforce functions involving electronic protected health information are to be performed in a manner that, in the opinion of the Security Official, reasonably protects the integrity and availability of electronic protected health information. In order to achieve this, the health care provider requires that:

- All workstations have password-protected screen savers whose password feature applies after two minutes (or as deemed appropriate by department) of inactivity;
- When a workforce member logged on to AS-400 intends to leave his or her workstation for longer than 30 minutes the member will log off the workstation;
- When a workforce member has completed work for the day the member will log off the workstation;
- Vendors using health care provider workstations shall follow the same rules as workforce members. These rules will be communicated to the vendors by the Security Official;

3. Physical Attributes of Surroundings. The HIPAA Security Committee shall analyze the physical attributes of the surroundings of every workstation within the control of the provider that can access electronic protected health information. The Security Official shall consider all relevant criteria in determining the security of such a workstation, including:

X Whether monitors are positioned in a way to minimize the risk that electronic protected health information can be viewed by non-authorized individuals;

X Whether individuals authorized to access electronic protected health information should be grouped in one or more separate areas to minimize the risk of accidental disclosures of electronic protected health information;

X Whether individuals authorized to access electronic protected health information have been trained on the importance of these workstation use rules and instructed to not alter the workstation surroundings in a way that could jeopardize electronic protected health information;

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\client\045146\0001\A0960471.1

ONEIDA COMMUNITY HEALTH CENTER
WORKSTATION SECURITY

Purpose: This Form is used to develop a policy and procedure for the health care provider regarding physical safeguards for all workstations under the control of the provider. The policy and procedure will help ensure that access to electronic protected health information is restricted to authorized users.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will have a procedure to implement physical safeguards for all workstations under the control of the provider if those workstations have access to electronic protected health information. The procedure will be designed to restrict access to authorized users.

SECTION B: Procedure.

1. Identification of Workstations. The Security Official will identify which workstations can access electronic protected health information. As of the date noted below, these include (See Form 3).

2. Physical Security. The following security provisions are adopted to help ensure compliance with the Workstation Security Standard:

The workstation will be logged and inventoried;

Each workforce member will be trained to not type in his or her password if the password (or typing of the password) could be viewed by an unauthorized individual;

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960554.1

ONEIDA COMMUNITY HEALTH CENTER
DISPOSAL AND MEDIA RE-USE

Purpose: This Form is used to develop a policy and procedure for (1) the disposal of hardware and / or electronic media containing electronic protected health information; and (2) removing electronic protected health information from electronic media before the media is made available for re-use.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will have a procedure governing the (1) disposal of hardware and / or electronic media containing electronic protected health information; and (2) removing electronic protected health information from electronic media before the media is made available for re-use.

SECTION B: Procedure for Disposal of Hardware and / or Electronic Media.

1. Notification to Workforce Members. In *Form 5, Information System Activity Review*, the Security Official determined where electronic protected health information was stored or maintained, either in physical form (e.g., a disk or CD-ROM) or electronic form (e.g., a computer's hard drive). The Security Official shall train all workforce members that hardware and other electronic media containing electronic protected health information must be (a) sanitized so no electronic protected health information is accessible; or (b) destroyed or altered so that no electronic protected health information is accessible.

2. Additional Steps. The Security Official shall take the following additional steps to help ensure that electronic protected health information is not accessible when hardware and / or electronic media is disposed:

- Place a notification (e.g., a small sticker) on the hardware or media that the hardware or media contains or likely contains electronic protected health information that must be sanitized prior to disposal;
- Require that all disposals of hardware or media containing or likely containing electronic protected health information must be approved by the Security Official;
- Require that the following general types of hardware and media be sanitized in the following ways prior to disposal, or be destroyed in a manner so that electronic protected health information will no longer be accessible:

Disks Reformatted

CD-ROMs Destroyed

Personal Computers, laptops Hard drives are reformatted

Servers Reformatted

The Security Official will audit and update *Form 5, Information System Activity Review*, every 6 months to verify whether any hardware or media has been added and to verify that previously reported hardware and media remain; and / or

SECTION C: Procedure for Re-Use.

1. **Identify Re-Useable Devices.** In *Form 5, Information System Activity Review*, the Security Official determined where electronic protected health information was stored or maintained, either in physical form (e.g., a disk or CD-ROM) or electronic form (e.g., a computer's hard drive). The Security Official should identify whether all or some of the hardware and media may be re-used:

All hardware and media may be re-used;

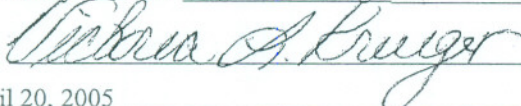
Only the following hardware and media may be re-used: _____

2. **Notification to Workforce Members.** All provider workforce members will be notified that the devices described above may be re-used to store electronic protected health information subject to these procedures.

3. **Proper Method of Sanitizing Hardware and Media.** The method for sanitizing electronic protected health information from the hardware and media described above is:

See #2 above. _____

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0960563.1

ONEIDA COMMUNITY HEALTH CENTER
ACCOUNTABILITY AND DATA BACKUP AND STORAGE

Purpose: This Form is used to document the health care provider's decision whether to implement policies and procedures regarding the Accountability and Data Backup and Storage Implementation Specifications. The Form also establishes any selected policies and procedures related to each chosen Specification.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Accountability and Data Backup and Storage

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- **Accountability**—Consider whether to maintain a record of hardware and electronic media and any person responsible for those items.
- **Data Backup and Storage**—Consider whether the provider should be able to create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Accountability and Data Backup and Storage Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- **Accountability** Low Medium High
- **Data Backup and Storage** Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- **Accountability** Low Medium High
- **Data Backup and Storage** Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- **Accountability** Low Medium High

- Data Backup and Storage Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Accountability Feasible and Not Difficult Feasible but Difficult Not Feasible
- Data Backup and Storage Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider *will* adopt a policy and procedure regarding the following Implementation Specifications:

- X Accountability
- X Data Backup and Storage

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Accountability.** The health care provider's policy is to maintain a record of hardware and electronic media and any person responsible for those items. The Security Official will create and maintain this list. The Security Official will use Attachment A to this Form 19, or an equivalent form, as the basis for creating and maintaining the list. The Security Official will update Attachment A as necessary.

- **Data Backup and Storage.** The health care provider's policy is to take the necessary steps to be able to create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. This will apply to the following equipment:

- All equipment;
- X Servers and other large hardware;
- Desktop computers;
- Laptop computers;
- Other portable devices including _____ [Describe portable device, e.g., personal digital assistant ("PDA")]; and / or

This will occur by the following methods:

- X Automatically: Veritas "Back up Exec" for Intel Servers and OS-400 for the AS-400 system;

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: *[Describe policy and procedure; may want to base language off Section A(5), above.]*

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

ATTACHMENT A

Description of Hardware and / or Electronic Media	Responsible Person	Date Responsibility Assigned
Intel Server (QSI, Indian Health Service)	MIS	
AS-400	MIS	

T:\client\045146\0001\A0960571.1

ONEIDA COMMUNITY HEALTH CENTER
UNIQUE USER IDENTIFICATION AND EMERGENCY ACCESS PROCEDURE

Purpose: This Form is used to develop a policy and procedure for (1) assigning a unique name and / or number for identifying and tracking user identity; and (2) establishing (and implementing as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will have a procedure for (1) assigning a unique name and / or number for identifying and tracking user identity; and (2) obtaining necessary electronic protected health information during an emergency.

SECTION B: Procedure for Assigning Unique Name and / or Number

1. Review of Current Software. The Security Official will determine whether the health care provider's current software automatically assigns a unique name and / or number for identifying and tracking user identity.

2. Action Based on Review. The Security Official believes that the health care provider's current software *is* adequate and satisfies this requirement

SECTION C: Obtaining Necessary Electronic Protected Health Information During Emergency.

1. Providing Temporary, Emergency Access. The Security Official implements the following technical procedures for allowing temporary access to electronic protected health information to an approved user during an emergency:

Relying on current software capabilities to allow temporary, emergency access (e.g., have a current procedure providing for a temporary password);

2. Termination of Temporary Access. Temporary, emergency access provided pursuant to Section C(1) shall be terminated immediately if the Security Official determines that the access has resulted in misuse of electronic protected health information. Temporary, emergency access provided pursuant to Section C(1) shall be terminated as soon as the emergency access is no longer needed. This is determined and occurs:

Automatically by software (e.g., terminates after one day) {Note: automatic termination must occur quickly, or there is a risk that user will have access that is not "temporary" or not related to the "emergency"};

By software upon direction from Security Official.

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0960598.1

ONEIDA COMMUNITY HEALTH CENTER
AUTOMATIC LOGOFF AND ENCRYPTION AND DECRYPTION

Purpose: This Form is used to document the health care provider's decision whether to implement policies and procedures regarding the Automatic Logoff and Encryption and Decryption Implementation Specifications. The Form also establishes any selected policies and procedures related to each chosen Specification.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Automatic Logoff and Encryption and Decryption

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Automatic Logoff—Consider whether to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- Encryption and Decryption—Consider whether to implement a mechanism to encrypt and decrypt electronic protected health information.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Automatic Logoff and Encryption and Decryption Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- Automatic Logoff Low Medium High
- Encryption and Decryption Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Automatic Logoff Low Medium High
- Encryption and Decryption Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Automatic Logoff Low Medium High

- Encryption and Decryption Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Automatic Logoff Feasible and Not Difficult Feasible but Difficult Not Feasible
- Encryption and Decryption Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider X will will not adopt a policy and procedure regarding the following Implementation Specifications:

- X Automatic Logoff
- X Encryption and Decryption

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Automatic Logoff.** The health care provider's policy is to implement electronic procedures that terminate an electronic session after *2 minutes on PC, 5 minutes on AS-400*. This will be accomplished by:

- X Using the following, existing software: Windows password protected screen savers _____;
- Purchasing and using the following software: _____;
- Designing custom software to accomplish the purpose; and / or
- _____.

The software will be tested when it is initially installed to ensure it functions properly. The software will be tested on an as-needed basis thereafter.

- **Encryption and Decryption.** The health care provider's policy is to implement a mechanism to encrypt and decrypt electronic protected health information. This will be accomplished by:

- X Using the following existing software: Groupwise _____;
- Purchasing and using the following software: _____;
- Designing custom software to accomplish the purpose; and / or
- _____.

The software will be tested when it is initially installed to ensure it functions properly. The software will be tested on an as-needed basis thereafter.

The health care provider will encrypt electronic protected health information:

When transmitted electronically (e.g., email); and / or

When stored electronically (e.g., on a computer's hard drive) at all locations or at the following locations: _____

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

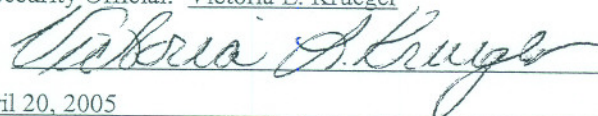
Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows:

Name of Security Official: Victoria L. Krueger

Signature: _____



Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0960609.1

ONEIDA COMMUNITY HEALTH CENTER
AUDIT CONTROLS

Purpose: This Form is used to develop a policy and procedure for the health care provider to implement hardware, software and / or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will implement hardware, software and / or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

SECTION B: Procedure.

1. Identification of Audit Control Features. The Security Official will identify audit control features of the health care provider's existing software that can help determine which users have accessed electronic protected health information. This is as follows: Access is controlled by menu options, application controls for authorization levels, identity of last user to update file in Encore , and lab has full audit trail.

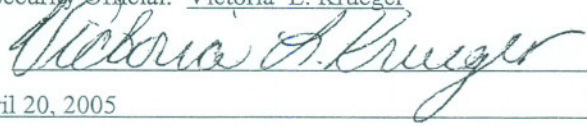
2. Determination of Needed Audit Controls. The Security Official has determined that:

- The audit controls identified above are sufficient; or
- The audit controls identified above are not sufficient. Additional audit controls will be implemented: _____

3. Implementation of Audit Controls. The Security Official will implement the audit controls identified above.

4. Testing of Audit Controls. The Security Official will test the audit controls when initially implemented to determine their functionality. The Security Official will re-test the audit controls on an as-needed basis.

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

T:\cienta\045146\0001\A0960614.1

ONEIDA COMMUNITY HEALTH CENTER
MECHANISM TO AUTHENTICATE ELECTRONIC
PROTECTED HEALTH INFORMATION

Purpose: This Form is used to document the health care provider's decision whether to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Mechanisms to Authenticate Electronic Protected Health Information

The Security Official must determine whether it is reasonable and appropriate to implement the Mechanisms to Authenticate Electronic Protected Health Information Implementation Specification. This Specification requires the health care provider to decide whether to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

The Security Official will determine whether this Implementation Specification is reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Implementation Specification, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing the Implementation Specification:

Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for the Implementation Specification:

Low Medium High

Explanation of analysis: _____

4. Feasibility. Determine the feasibility of implementing a procedure for the Implementation Specification:

Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider will will not adopt a policy and procedure regarding the Mechanism to Authenticate Electronic Protected Health Information Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible.

The health care provider's policy is to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. The health care provider will do this by: _____

Using existing mechanisms: Access is controlled by available menu options, application controls for authorization levels, identification of last user to update file and lab package offers full audit trail.

Obtaining additional mechanisms: _____

The Security Official will monitor these mechanisms, and new mechanisms that become available, on an as-needed basis to ensure that the provider continues to maintain appropriate electronic mechanisms.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding the Implementation Specification.

1. **Description of Alternatives.** If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows:

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

**ONEIDA COMMUNITY HEALTH CENTER
PERSON OR ENTITY AUTHENTICATION**

Purpose: This Form is used to develop a policy and procedure for the health care provider to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health care provider that the provider will verify that a person or entity seeking access to electronic protected health information is the one claimed.

SECTION B: Procedure.

1. Identification of Ways of Accessing Electronic Protected Health Information. In *Form 5, Information System Activity Review*, the health care provider previously identified where electronic protected health information is stored in physical form (e.g., disks and CD-ROMs) and in electronic form (e.g., on servers' hard drives). The Security Official will review *Form 5, Information System Activity Review*, when completing this form.

2. Methods of Ensuring Person or Entity Authentication. The health care provider adopts the following methods of ensuring that the person or entity accessing or requesting access to electronic protected health information is the one claimed:

X Physical Form:

Passwords;

Tokens;

Biometric methods: _____
[Describe; e.g., fingerprint recognition];

Personal identification number ("PIN"); and / or

X Identification cards _____

X Electronic Form:

X Passwords;

Tokens;

Biometric methods: _____
[Describe; e.g., fingerprint recognition];

Personal identification number ("PIN"); and / or

3. Different Methods Depending on Access. If different methods of authentication exist depending on the method of access (e.g., password is used for remote access when person connects through computer at home; fingerprint

recognition used when accessing electronic protected health information at health care provider's facilities) describe the different methods: _____

Name of Security Official: Victoria L. Krueger

Signature: _____

Victoria L. Krueger

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0960628.1

ONEIDA COMMUNITY HEALTH CENTER
INTEGRITY CONTROLS AND ENCRYPTION

Purpose: This Form is used to document the health care provider's decision whether to implement policies and procedures regarding the Integrity Controls and Encryption Implementation Specifications. The Form also establishes any selected policies and procedures related to each chosen Specification.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Integrity Controls and Encryption

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Integrity Controls—Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
- Encryption—Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Integrity Controls and Encryption Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health care provider does not have a procedure in place regarding the Implementation Specification:

- Integrity Controls Low Medium High
- Encryption Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Integrity Controls Low Medium High
- Encryption Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Integrity Controls Low Medium High
- Encryption Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Integrity Controls Feasible and Not Difficult Feasible but Difficult Not Feasible
- Encryption Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health care provider will will not adopt a policy and procedure regarding the following Implementation Specifications:

- X Integrity Controls
- X Encryption

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Integrity Controls.** The health care provider's policy is to implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. This will be accomplished by: Using existing software and possibly digital signatures.

- **Encryption.** The health care provider's policy is to implement a mechanism to encrypt electronic protected health information when appropriate. The following situations are always deemed appropriate for encryption of electronic protected health information:

- X Transmissions to other health care providers;
- X Transmissions to business associates (e.g., peer review consultant or attorney);

This will occur by the following methods:

- X Automatically: Groupwise has proprietary encryption;
- X Case-by-Case Basis: Use PGP for e-mail correspondence as required; and / or
- X Data from most EPHI systems is a point to point transmission with user ID's and passwords required to create a private "tunnel." If such transmissions are internet based in the future, PKI certs. will be used.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: [*Describe policy and procedure; may want to base language off Section A(5), above.*]

Name of Security Official: Victoria L. Krueger

Signature: _____

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0960636.1

ONEIDA HEALTH CARE BENEFIT PLAN
· SECURITY OFFICIAL DESIGNATION

COPY

Purpose: This Form is used to designate the health plan's Security Official.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

After careful consideration, the Oneida Health Care Benefit Plan determined that it would be prudent to select **Victoria L. Krueger** as the interim Security Official of the Oneida Health Care Benefit Plan (the "Plan"). The Security Official, working in conjunction with the Oneida HIPAA Security Committee, will be responsible for developing and implementing policies and procedures to ensure the confidentiality, integrity and availability of all electronic protected health information created, received, maintained or transmitted by the Plan. This designation is effective April 20, 2005 and shall continue indefinitely until modified by the fiduciaries of the Plan.

Unless otherwise specified in any policy and procedure, the Security Official shall: (1) take all actions required of the Plan to comply with the Security Rule of the Health Insurance Portability and Accountability Act of 1996; (2) have authority and responsibility to adopt a policy and / or procedure and complete any related forms; (3) have authority to modify a policy and / or procedure and any related forms; (4) have responsibility to retain all policies, procedures, forms, documents and training materials as required by the Security Rule; and (5) periodically review and update all relevant policies, procedures, forms, documents and training materials as needed, in response to environmental or operational changes affecting the security of electronic protected health information.

The Security Official is authorized to create and supervise a Security Committee to assist in carrying out these responsibilities.

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0918605.1

ONEIDA HEALTH CARE BENEFIT PLAN
RISK ANALYSIS

Purpose: This Form is used to help conduct a risk analysis of the confidentiality, integrity and availability of the health plan's electronic protected health information. The risk analysis includes electronic protected health information both when it is in transit (for example, sent via email from one entity to another) and at rest (for example, stored on a computer disk).

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Identifying Individuals Involved in Routine Transmissions and Routine Storage.

The following is a list of the health plan's workforce members who routinely transmit or store electronic protected health information. The list includes employees of the plan sponsor who are allowed access to electronic protected health information pursuant to HIPAA's plan amendment requirements.

1. Name / Position. **Computer Operations and Programming**
2. Name / Position. **PC Support, Network Administration**
3. Name / Position. **Benefit Director**
4. Name / Position. **Insurance Specialist/Clerk 1, Clerk 2, Clerk 3.**
5. Name / Position. **Risk Manager**
6. Name / Position. **Risk Management Analyst**
7. Name / Position. **Chief Financial Officer**

Note: Attach additional pages as necessary.

SECTION B: Identifying Routine Transmissions of Electronic Protected Health Information.

The individuals identified in Section A routinely transmit electronic protected health information to the following individuals or entities, as applicable. The risk associated with each transmission is also considered. The risk consists of :

(1) Confidentiality Risk – Whether the information is made available or disclosed to unauthorized persons or processes;

(2) Integrity Risk – Whether the information has been altered or destroyed in an unauthorized manner;

(3) Availability Risk – Whether the information is not accessible and not useable upon demand by an authorized person.

1. **Wausau Benefits – Enrollment Representative, Group Manager, Flex Manager**

Confidentiality Risk X Low Medium High

Explanation of analysis: Transmission is sent to specific individuals, not entire staff. HIPAA Business Associate Agreements.

Integrity Risk Low Medium High

Explanation of analysis: Transmitting to secure site. We receive confirmation of successful transmission.

Availability Risk Low Medium High

Explanation of analysis: _____

2. **Metlife- Short Term Disability Claim Representative**

Confidentiality Risk Low Medium High

Explanation of analysis: Claim numbers are used rather than social security numbers. Emails are sent are secured.

Integrity Risk Low Medium High

Explanation of analysis: Transmission is made to a secure site.

Availability Risk Low Medium High

Explanation of analysis: _____

3. **Mortenson, Matzelle and Meldrum, Broker**

Confidentiality Risk Low Medium High

Explanation of analysis: Data sent or received is via secured e-mail.

Integrity Risk Low Medium High

Explanation of analysis: Passwords and access are restricted.

Availability Risk Low Medium High

Explanation of analysis: _____

4. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

5. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

6. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

7. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

Note: Attach additional pages as necessary.

SECTION C: Identify Routine Storage of Electronic Protected Health Information.

Electronic protected health information is routinely stored in the following manner and locations:

1. AS/400 databases and Norbert Hill Center.

Confidentiality Risk Low Medium High

Explanation of analysis: Secured area at NHC. Off site storage and ARMS.

Integrity Risk Low Medium High

Explanation of analysis: Daily backup with proven backup technology.

Availability Risk Low Medium High

Explanation of analysis: Access to backup data available on 24 hour basis.

2. Backup Tapes

Confidentiality Risk Low Medium High

Explanation of analysis: Data cannot be altered.

Integrity Risk Low Medium High

Explanation of analysis: Tapes are stored in a secure location.

Availability Risk Low Medium High

Explanation of analysis: Tapes are available 24 hours a day, seven days a week.

3. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

4. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

5. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

6. _____

Confidentiality Risk Low Medium High

Explanation of analysis: _____

Integrity Risk Low Medium High

Explanation of analysis: _____

Availability Risk Low Medium High

Explanation of analysis: _____

Note: Attach additional pages as necessary.

SECTION D: Policy Regarding Non-Routine Transmission and Storage of Electronic Protected Health Information.

It is the policy of the health plan that transmission and storage of electronic protected health information in a manner other than that identified above will be considered on a case-by-case basis by the Security Official. The Security Official will consider, in each situation, the confidentiality risk, integrity risk and availability risk for each non-routine transmission and storage.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0918858.1

ONEIDA HEALTH CARE BENEFIT PLAN
SANCTION POLICY

Purpose: This Form is used to develop a sanction policy for the health plan's workforce, in the event the workforce violates the plan's policies and procedures regarding the security of electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan's workforce, shall comply with the plan's policies and procedures relating to the security of electronic protected health information. Appropriate disciplinary procedures, up to and including termination of employment, will be imposed upon workforce members violating this policy.

SECTION B: Procedure.

1. The Security Official will work with the appropriate Supervisor and the Human Resources Department to determine an appropriate sanction consistent with the requirements of the Oneida Personnel Policies and Procedures. Sanctions can include verbal warnings, written warnings, suspension of employment, termination of employment or other appropriate actions.
2. The Security Official shall review and update this Sanction Policy as needed.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0919992.1

**ONEIDA HEALTH CARE BENEFIT PLAN
INFORMATION SYSTEM ACTIVITY REVIEW**

Purpose: This Form is used to develop a policy for the health plan to help ensure that the health plan regularly reviews information system activity relating to electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will regularly review records of information system activity. The health plan will do so in order to determine "internal" access from within the health plan's workforce relating to: (1) what electronic protected health information is accessed; (2) who accessed the electronic protected health information; and (3) whether the access was proper.

SECTION B: Procedure.

1. Physical Access. The Security Official has determined that electronic protected health information in physical form (such as storage on a disk, CD-ROM or DVD) is located at the following locations:

- i. Norbert Hill Center (Secured area with proximity cards).
- ii. Oneida Community Health Center (Servers in locked room).
- iii. Social Services (Servers in locked room).
- iv. ARMS (Off site storage vault).
- v. Casino (Server in secured area).

The health plan establishes the following procedure for determining whether an individual has accessed this electronic protected health information stored in physical form: *Access to these areas is restricted and tracked by electronic access badge or manual sign in.*

2. Electronic Access. The Security Official has determined that electronic protected health information in electronic form (such as storage on a computer's hard drive) is located at the following locations:

- i. *Data is stored on Central AS/400 Server or Intel Server. All access to these servers requires authentication to the Network and authorization to any application data base.*

The health plan establishes the following procedure for determining whether an individual has accessed this electronic protected health information stored in electronic form:

The application software tracks who has modified the data. Access to the data is only provided to those individuals requiring access to perform their job duties.

Note: Attach additional pages as necessary.

3. Frequency of Review. The Security Official will conduct an information system activity review every *6 months.*

4. **Use of Information.** The Security Official shall use the information gathered in the review to determine whether electronic protected health information was accessed by an internal user, who accessed the information and whether the access was proper.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0920042.1

ONEIDA HEALTH CARE BENEFIT PLAN AUTHORIZATION AND/OR SUPERVISION

Purpose: This Form is used to develop a policy for the health plan to document whether the plan must have a procedure regarding the authorization and/or supervision of workforce members who will access electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Authorization and Policy Regarding Authorization.

In *Form 3, Risk Analysis*, the health plan determined which workforce members typically would need access to electronic protected health information. The Security Official now needs to determine whether it is reasonable and appropriate to pre-authorize or pre-screen workforce members before allowing them access to electronic protected health information. In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk if the health plan does not pre-authorize or pre-screen a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the plan's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of the health plan pre-authorizing or pre-screening a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the plan's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Background checks are a part of the standard hiring process.*

3. **Benefit.** Determine or estimate the benefit of the health plan pre-authorizing or pre-screening a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the plan's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Background checks will detect prior criminal activity.*

4. **Feasibility.** Determine the feasibility of the health plan pre-authorizing or pre-screening a workforce member as being trustworthy to obtain electronic protected health information and being able to follow the plan's policies and procedures regarding electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: *See 2 above.*

5. **Policy.** Based on the above, it is the policy of the health plan that the Security Official acting through the Human Resources Department *will* pre-authorize or pre-screen workforce members as being trustworthy to obtain electronic protected health information and being able to follow the plan's policies and procedures regarding electronic protected health information. This is part of the background check process.

SECTION B: Determination of Need for Supervision and Policy Regarding Supervision.

The Security Official now needs to determine whether it is reasonable and appropriate to supervise workforce members who access electronic protected health information. In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk that if the health plan does not supervise a workforce member, the workforce member will violate the plan's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Risk is medium. Background checks should screen out those individuals who would maliciously violate security policies and procedures.*

2. **Cost.** Determine or estimate the cost of supervising all workforce members to ensure that the member will follow the plan's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Such supervision falls within established chain of command.*

3. **Benefit.** Determine or estimate the benefit of supervising all workforce members to ensure that the member will follow the plan's policies and procedures regarding electronic protected health information: Low Medium High

Explanation of analysis: *Supervision will ensure compliance with security policies and procedures.*

4. **Feasibility.** Determine the feasibility of supervising all workforce members to ensure that the members follow the plan's policies and procedures regarding electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: *See (2) above.*

5. **Policy.** Based on the above, it is the policy of the health plan that the applicable Supervisor *will* supervise all workforce members to ensure that the members follow the plan's policies and procedures regarding electronic protected health information.

SECTION C: Alternatives if No Authorization or Supervision is Selected

Complete this Section C only if, pursuant to Sections A or B, the health plan chose not to enact a policy regarding authorization and/or supervision. If a policy was enacted regarding one or the other (for example, a policy was enacted regarding authorization but not supervision) complete this Section C only for the item not enacted (in this example, supervision).

1. **Description of Alternatives.** If the health plan determined under Sections A and/or B that no authorization and/or supervision was reasonable and appropriate, describe alternative measures the health plan considered to achieve the same goals of the Authorization and/or Supervision Implementation Standard:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. If more than one alternative measure was proposed attach additional pages as necessary and indicate which alternative measure(s) were selected:

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, it is the policy of the health plan that the Security Official will will not enact the alternative measures discussed and selected above.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\client\045146\0001\A0920138.1

**ONEIDA HEALTH CARE BENEFIT PLAN
WORKFORCE CLEARANCE PROCEDURE**

Purpose: This Form is used to document whether the plan must have a procedure regarding the appropriateness of a workforce member's access to electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Workforce Clearance Procedure.

In *Form 3, Risk Analysis*, the health plan determined which workforce members typically would need access to electronic protected health information. The Security Official now needs to determine whether it is reasonable and appropriate to have a procedure in place to verify whether it is appropriate for a workforce member to access all or some electronic protected health information. (If the Security Official already knows it is reasonable and appropriate, or has already implemented a Workforce Clearance Procedure, skip (1) – (4) and proceed directly to (5).) In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk if the health plan does not have a procedure in place to determine whether the workforce member may access all or some electronic protected health information: Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of implementing a procedure to determine whether a particular workforce member may access all or some electronic protected health information: Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of the health plan establishing a procedure to determine whether a particular workforce member may access all or some electronic protected health information: Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of the health plan implementing a procedure to determine whether a particular workforce member may access all or some electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, it is the policy of the health plan that the Security Official will determine whether a particular workforce member may access all or some electronic protected health information.

Attached is the procedure and RFS forms for requesting access.

SECTION B: Alternatives if No Workforce Clearance Procedure is Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy to determine whether a particular workforce member may access all or some electronic protected health information.

1. Description of Alternatives. If the health plan determined under Section A that no policy was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Workforce Clearance Implementation Specification:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. If more than one alternative measure was proposed attach additional pages as necessary and indicate which alternative measure(s) were selected:

Cost Low Medium High

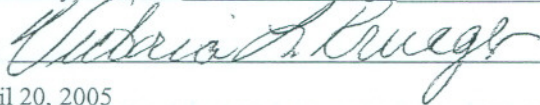
Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, it is the policy of the health plan that the Security Official will will not enact the alternative measures discussed relating to whether a particular workforce member may have access to electronic protected health information.

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0920341.1

January 25, 2001

STANDARD OPERATING PROCEDURE TO REQUEST USER ID's

Assigning User ID's for training and production purposes for the ENCORE System will be run through the HIS Trainer for the component to be trained in.

HIS Trainer will fill out RFS and forward to appropriate MIS Staff, approximately 3-4 days prior to training session for assignment of User ID's.

These User ID's will be given to the employee at their scheduled training session. At this training, the employee will learn to sign-on to both training and production modules.

If employee does not attend a formal training session, employee will not have access to ENCORE System and no User ID will be assigned.

Approved by Steering Committee
April 5, 2001

- c OCHC Supervisors/Directors
- SSB Supervisors/Directors

Oneida Tribe of Indians of Wisconsin

Project No.
Assigned

MIS Request for Services

Request Date: March 3, 2005

Requester: Supervisor's Name

Dept: Department

Bldg: OCHC

Phone / Ext#: 869-2711

MIS Category (type an "X" to the left of all that apply)

PC / LAN / WAN AS / 400 RS / 6000 Telecommunications

Request Type (type an "X" to the left of all that apply)

Modification New Software Relocation Acquisition
 Installation Problem Computer Account Information
 User Setup/System Access * Other: **Disconnection and Disablement of User**

Full Time
 Temporary (LTE, ET, Intern) ** Termination Date (MM/DD/YY)
 Other (Please Explain)

Request:

Please disable (**employees name**), (**job title of employee**) @ OCHC from the network, groupwise, internet, and from the AS400 sessions.

Why Required / Expected Benefit:

Will no longer be working at OCHC as of (**termination/leave date**).

Impact on other areas (if any):

Protect Data Integrity and for Tribal Security and Confidentiality Controls

Requested Completion Date (MUST HAVE A DATE HERE FOR MIS TO ROUTE YOUR REQUEST):

GIVE AT LEAST A WEEK'S NOTICE IF POSSIBLE

* User Setup/System Access requires user has read Computer Resources Ordinance and has a signed acknowledgment form on file at HRD.

Supervisor initial this is completed. Date Signed (MM/DD/YY)

** Supervisors must complete an RFS to terminate system access rights.

MIS Request for Services

Request Date: March 3, 2005

Requester: Supervisor's Name

Dept: Department

Bldg: OCHC

Phone / Ext#: 869-2711

MIS Category (type an "X" to the left of all that apply)

X PC / LAN / WAN X AS / 400 X RS / 6000 X Telecommunications

Request Type (type an "X" to the left of all that apply)

Modification Installation X User Setup/System Access * X Full Time Temporary (LTE, ET, Intern) ** Other (Please Explain) New Software Problem Relocation Acquisition Computer Account Information Other: Termination Date (MM/DD/YY)

Request:

- 1. Please set up new (employee name) on the computer station next to along the windows outside office CH-461 with the same access as (current user name of for profile set-up by operations).
2. Please include all G drive access to match that of (current user name of for profile set-up by operations).
3. Please set up AS400/PASS access for (employee name) to match the other Community Health Nurses.
4. Please set up (employee name) the phone with extension 4940 as and set up access to voice mail for her/him.
5. Please set up cell phone number 713-8310 for (employee name). Re-establish voice mail access and new security code.
6. Set up as provider in the IHS system for data entry purposes.

Why Required / Expected Benefit:

Needed in order to complete job duties.

Impact on other areas (if any):

New employee

Requested Completion Date (MUST HAVE A DATE HERE FOR MIS TO ROUTE YOUR REQUEST):

GIVE AT LEAST A WEEK'S NOTICE

* User Setup/System Access requires user has read Computer Resources Ordinance and has a signed acknowledgment form on file at HRD.

J Supervisor initial this is completed.

3-3-2005 Date Signed (MM/DD/YY)

** Supervisors must complete an RFS to terminate system access rights.

ONEIDA HEALTH CARE BENEFIT PLAN

TERMINATION PROCEDURES

Purpose: This Form is used to document whether the plan must have a procedure regarding the termination of a workforce member who had access to electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Termination Procedure.

In *Form 3, Risk Analysis*, the health plan determined which workforce members typically would need access to electronic protected health information. The Security Official now needs to determine whether it is reasonable and appropriate to establish an access termination procedure for when a workforce member terminates employment or when it is reasonably required under the Workforce Clearance Procedure Implementation Specification. (If the Security Official already knows it is reasonable and appropriate, or has already implemented a Termination Procedure, skip (1) – (4) and proceed directly to (5).) In order to do so, the Security Official considers the following:

1. **Risk.** Rate the risk if the health plan does not have a procedure in place regarding the termination of employment of a workforce member who had access to electronic protected health information: Low Medium High

Explanation of analysis: _____

2. **Cost.** Determine or estimate the cost of implementing a procedure regarding the termination of employment of a workforce member who had access to electronic protected health information: Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of implementing a procedure regarding the termination of employment of a workforce member who had access to electronic protected health information: Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure regarding the termination of employment of a workforce member who had access to electronic protected health information: Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan will will not adopt a policy and procedure regarding the termination of employment of a workforce member who had access to electronic protected health information. If selected, the policy and procedure is as follows:

It is the policy of the health plan that the health plan will take reasonable and appropriate steps to ensure that electronic protected health information is not accessed by workforce members who have terminated employment. The Security Official shall take all necessary steps to ensure this policy is implemented. These steps include the following, all to be taken as soon as reasonably possible [*Select applicable steps and/or add additional steps*]:

- Determining what electronic protected health information the person had access to, in order to determine what the person may have retained or may still be able to access;
- Requiring the return of all keys that can lead to access of electronic protected health information;
- Turning off card keys or other electronic equivalents;
- Requiring the return of laptops and other electronic media, such as computer disks, CD-ROMs and DVDs;
- Removing the person as an authorized user; and/or
- Contact applicable insurance companies to remove terminated employees access to secure websites.

SECTION B: Alternatives if No Termination Procedure is Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding the termination of employment of a workforce member who had access to electronic protected health information.

1. Description of Alternatives. If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Termination Procedure Implementation Specification:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. If more than one alternative measure was proposed attach additional pages as necessary and indicate which alternative measure(s) were selected:

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: [*Describe policy and procedure; may want to base language off Section A(5), above.*]

Name of Security Official: Victoria L. Krueger

Signature: _____

Victoria L. Krueger

Date: April 20, 2005

Version 1, 10/04

T:\client\045146\0001\A0920482.1

Hiring Department; Employee Separations

When an employee separates employment, it is extremely important that the Separation Report is sent by the supervisor to the Human Resource Department Representative immediately.

The Document has several purposes which benefit the employee, supervisor, and the organization:

- It immediately stops the employee's benefits at Midnight of the date of separation.
- Employee Insurance Department will send information regarding COBRA to offer continuing employee medical coverage.
- It immediately stops all Payroll Deductions.
- Payroll, upon receiving the separation date, will payout all vacation and personal time to the employee.
- HRD will have the correct Workforce Levels for Reporting Purposes to Department Managers and external agencies as required by law.

As a supervisor, you need to do more than just send the Separation Form to HRD, here's a checklist to help you remember to:

- Notify MIS to revoke all PC access.
- Collect Tribal property, such as; keys, Kronos badge, cell phone, laptop, PDA, etc....
-

Please send Separations to Your HR Representatives by Division:

Gaming Division: Terry Skenandore or Marilyn Jourdan

Governmental Services, Development Division, Enterprise Division and Compliance Division: Lisa Hock or Wanita DeCorah

Internal Services Division, Land Management Division, Transit, Oneida Police Department, Non-Divisional Departments, Boards, Committees, Commissions: Lisa Duff

HRD Telephone Number: 496-7900

SEPARATION SECURITY FORM

Form #HRD203

Employee's Name: _____ Employee Number: _____

Employee's Department: _____ Employee's Division: _____

Employee's Separation Date: _____ Employee's Title: _____

Supervisor's Name: _____ Supervisor's Title: _____

Listed below are Tribal items which must be returned prior to the employee separating from employment. If the employee does not have the particular item, please write N/A for not applicable.

<u>ITEM</u>	<u>DATE RETURNED</u>
a. Employee Badge	a. _____
b. Desk Keys	b. _____
c. Door Keys	c. _____
d. Security Access/Code	d. _____
e. Beeper	e. _____
f. Cell Phone	f. _____
g. Lap Top Computer	g. _____
h. Tribal Documents taken Home	h. _____
i. Uniforms	i. _____

Supervisor must follow through with the items listed below, as applicable:

<u>ITEM</u>	<u>DATE COMPLETED</u>
1. Contact the Kronos Administrator to have employee removed from Kronos	1. _____
2. Contact MIS to have the employee removed from GroupWise, Infinium, and computer access.	2. _____
3. Schedule appointment for return of items listed as Employee Property.	3. _____

SEPARATION SECURITY FORM



ITEM

DATE COMPLETED

4. Complete the Separation Report and/or the Disciplinary Form and send to HRD for the Employee to be paid our vacation/personal time.

3. _____

5. Contact Accounting to remove all sign-off Authority.

4. _____

6. Contact Building Administrator to remove Building Security codes, eye dots, etc.

5. _____

7. Assess whether work area locks and security codes need to be changed

6. _____

EMPLOYEE SEPARATION REPORT

(Print)

Name: _____ Empl #: _____
Last First M.I.

Job Title: _____ Separation Date: _____

Department: _____ Division: _____

TYPE OF SEPARATION:

- Resignation (attach letter) Termination Deceased Denial of LOA
 Transfer/Reassignment Retirement Lay-Off (26 wk)
 Other _____

REASON FOR SEPARATION:

- Working Conditions Reduction in Force
 Job Change within Oneida Tribe Where: _____
 Policy Violation _____
 Other _____

INVESTIGATION PENDING AT TIME OF SEPARATION: Yes No

EMPLOYEE EVALUATION (please check appropriate boxes):

	Unsatisfactory	Satisfactory	Excellent
Attendance			
Cooperation			
Initiative			
Job knowledge			
Quality of work			

REHIRE: Yes No (See attached documentation)

Additional Comments: _____

Supervisor Signature

Date

Supervisor Name (Print)

ONEIDA HEALTH CARE BENEFIT PLAN
INFORMATION ACCESS MANAGEMENT

Purpose: This Form is used to document the health plan's decision whether to implement policies and procedures regarding the Access Authorization and Access Establishment and Modification Implementation Specifications. If either Specification is selected, this Form establishes the plan's policies and procedures regarding the selected Specification(s).

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Access Authorization and Access Establishment and Modification.

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Access Authorization—Implement policies and procedures for granting access to electronic protected health information.
- Access Establishment and Modification—Implement policies and procedures that, based upon the health plan's Access Authorization policies, establishes, documents, reviews and modifies a user's right of access to a workstation, transaction, program or process.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Access Authorization and Access Establishment and Modification Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- Access Authorization Low Medium High
- Access Establishment and Modification Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Access Authorization Low Medium High
- Access Establishment and Modification Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Access Authorization Low Medium High
- Access Establishment and Modification Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Access Authorization Feasible and Not Difficult Feasible but Difficult Not Feasible
- Access Establishment and Modification Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan will adopt a policy and procedure regarding the following Implementation Specifications:

- X Access Authorization
- X Access Establishment and Modification

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

It is the policy of the health plan that the health plan will take reasonable and appropriate steps to ensure that only approved workforce members or others may have access to electronic protected health information. It is the policy of the health plan that the granting of such access may be modified by the Security Official when the Security Official deems reasonable and appropriate. The Security Official shall take all necessary steps to ensure this policy is implemented. These steps include the following:

- X Ensuring that access is granted only on a case-by-case basis and is not automatic for every workforce member;
- X Establishing passwords on computer systems and providing passwords only to approved workforce members and others;
- X Establishing screen savers on computers with passwords required in order to access the computer after a certain period of inactivity;
- X Communicating passwords to workforce members in a secure manner (e.g., not using interoffice routing in a non-secure envelope);
- X Working with the Human Resources Department and MIS so that the Security Official is notified promptly of any new members added to the plan's workforce and of any termination of a workforce member or change in that member's job functions that could affect the member's ability or authority to access electronic protected health information;
- X Documenting any granting of access or modification of access and notifying the following departments or areas of the granting of such access or modification of such access: [*Modify as appropriate; for example, may need to notify Information Technology and Employee Benefits Departments*]:

Oneida MIS

Oneida Benefits Department

X Establishing different categories of electronic protected health information and establishing passwords to ensure that workforce members have access only to the category of electronic protected health information appropriate to the particular member; and/or

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows:

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0920604.1

**ONEIDA HEALTH CARE BENEFIT PLAN
SECURITY AWARENESS AND TRAINING**

Purpose: This Form is used to document the health plan's decision whether to implement policies and procedures regarding the Security Awareness and Training Standard. The Form also establishes any selected policies and procedures related to the Standard.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Security Awareness and Training

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement none, some or all of the Implementation Specifications:

- Security Reminders—Periodic security updates.
- Protection From Malicious Software—Guarding against, detecting and reporting malicious software.
- Log-in Monitoring—Monitoring log-in attempts and reporting discrepancies.
- Password Management—Creating, changing and safeguarding passwords.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented a particular Specification, skip (1) – (4) for that Specification and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- Security Reminders Low Medium High
- Protection From Malicious Software Low Medium High
- Log-in Monitoring Low Medium High
- Password Management Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Security Reminders Low Medium High
- Protection From Malicious Software Low Medium High
- Log-in Monitoring Low Medium High
- Password Management Low Medium High

Explanation of analysis: _____

3. **Benefit.** Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Security Reminders Low Medium High
- Protection From Malicious Software Low Medium High
- Log-in Monitoring Low Medium High
- Password Management Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Security Reminders Feasible and Not Difficult Feasible but Difficult Not Feasible
- Protection From Malicious Software Feasible and Not Difficult Feasible but Difficult Not Feasible
- Log-in Monitoring Feasible and Not Difficult Feasible but Difficult Not Feasible
- Password Management Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan X will will not adopt a policy and procedure regarding the following Implementation Specifications:

- X Security Reminders.
- X Protection From Malicious Software.
- X Log-in Monitoring.
- X Password Management.

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Security Reminders.** The health plan's policy is to issue security reminders to relevant workforce members as reasonable and appropriate. The health plan will determine the topics for the reminder and the method of distributing the reminder. The health plan will document, and retain for six (6) years, proof of the reminder. The reminder will be distributed on an as needed basis.

• **Protection From Malicious Software.** The health plan's policy is to have protection from malicious software. The health plan will examine its vulnerability to particular, known malicious software. The health plan will:

X License or purchase software designed to combat malicious software; and / or

The health plan will take steps to ensure that it maintains current knowledge about malicious software. These steps include:

X Updating the software used to combat malicious software;

X Subscribing to trade publications, newsletters and other periodic resources that provide information on current developments; and / or

The health plan will take steps to ensure that appropriate, current software (if selected above) is placed on each computer or server that could be affected by malicious software, including portable computers such as laptop computers.

All incoming email messages will be scanned for malicious software. If a workforce member has security concerns about an attachment to an email message the member shall contact the Security Official prior to opening the attachment. Workforce members are not allowed to download software onto their computers unless the Security Official has approved the software. The Security Official shall, if appropriate, use Form 11, Workforce Member Training, to train all workforce members on these policies and procedures regarding Protection From Malicious Software.

• **Log-in Monitoring.** The health plan's policy is to monitor log-in attempts of users. If the log-in is successful on the first attempt no log-in report will be generated. If the log-in is unsuccessful after 3 (three) consecutive attempts, the user will be locked out of the system. The user will be required to contact MIS operations to access the network after being locked out.

• **Password Management.** The health plan's policy is that passwords are an important security provision and appropriate steps will be taken to ensure the use and confidentiality of passwords. The health plan implements the following requirements regarding passwords:

X Passwords will have a minimum length of 8 characters;

Passwords will include both numeric and alphabetic characters;

Passwords should contain both upper and lower case characters (e.g., a-z, A-Z);

Passwords should not be based on personal information (e.g., spouse's name, street address);

Passwords shall not be composed of only one character (e.g., aaaaaa);

X Publishing or sharing of passwords is not allowed;

X Passwords should not be written down but, if they are written down, shall be stored in a secure (preferably locked) location;

X Passwords will be changed every 90 days;

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows:

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\client\045146\0001\A0920701.1

ONEIDA HEALTH CARE BENEFIT PLAN
WORKFORCE MEMBER TRAINING

Purpose: This Form is used to determine which components of the Security Rule, if any, should be explained to the health care plan's workforce as part of the plan's training under the Security Rule.

Retention: This Form should be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Identification of Potential Components Requiring Training.

The Security Official should review the following list of Security Rule components. The Security Official should determine which, if any, components should be explained to the plan's workforce. For example, the Security Official may determine that only a few components (such as changing passwords and informing workforce members about proper workstation use) should be explained to the plan's workforce. The Security Official should document the selected components.

ADMINISTRATIVE SAFEGUARDS

Standards	Implementation Specifications	Workforce Training/Explanation Required?	
Security Management Process	Risk Analysis	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Risk Management	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Sanction Policy	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Information System Activity Review	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Assigned Security Responsibility		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Workforce Security	Authorization and/or Supervisions	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Workforce Clearance Procedure	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Termination Procedures	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Information Access Management	Isolating Health Care Clearinghouse Function	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Access Authorization	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Access Establishment and Modification	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Security Awareness and Training	Security Reminders	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Protection from Malicious Software	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Log-in Monitoring	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Password Management	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Security Incident Procedures	Response and Reporting	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Contingency Plan	Data Backup Plan	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Disaster Recovery Plan	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Emergency Mode Operation Plan	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Testing and Revision Procedure	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Applications and Data Criticality Analysis	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Evaluation		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Business Associate Contracts and Other Arrangement	Written Contract or other Arrangement	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

PHYSICAL SAFEGUARDS

Standards	Implementation Specifications	Workforce Training/Explanation Required?	
Facility Access Controls	Contingency Operations	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Facility Security Plan	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Access Control and Validation Procedures	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Maintenance Records	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Workstation Use		<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

Workstation Security		<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Device and Media Controls	Disposal	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Media Re-use	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Accountability	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Data Backup and Storage	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

TECHNICAL SAFEGUARDS

Standards	Implementation Specifications	Workforce Training/ Explanation Required?	
		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Access Control	Unique User Identification	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Emergency Access Procedure	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Automatic Logoff	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Encryption and Decryption	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Audit Controls		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Integrity	Mechanism to Authenticate Electronic Protected Health Information	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Person or Entity Authentication		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Transmission Security	Integrity Controls	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	Encryption	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

SECTION B: Preparation of Training Materials.

The Security Official should prepare appropriate training materials that will inform the workforce members of the items specified above. These training materials can include any appropriate items, such as an electronic presentation or written materials.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\client\045146\0001\A0953232.1

{COVERED ENTITY NAME}
RESPONSE AND REPORTING

Purpose: This Form is used to develop a policy for the health plan to: identify and respond to suspected or known security incidents involving electronic protected health information; mitigate, to the extent practicable, harmful effects of security incidents known to the health plan; and document security incidents and their outcomes.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will:

- Identify and respond to suspected or known security incidents involving electronic protected health information;
- Mitigate, to the extent practicable, harmful effects of security incidents known to the plan; and
- Document security incidents and their outcomes.

All such actions shall be taken by the Security Official as promptly as possible after learning of a security incident or suspected security incident.

SECTION B: Procedure.

1. Once the health plan becomes aware of a security incident or potential security incident, the Security Official will use the Security Incident Type Matrix, below, to verify that a security incident occurred and determine the level of severity of the security incident.

- Description of Security Incident or Potential Security Incident, including workforce members and equipment involved: _____

SECURITY INCIDENT TYPE MATRIX

INCIDENT TYPE	INCIDENT DESCRIPTION	EXAMPLES
<u>Low Risk</u>	Isolated incidents attributable to common non-malicious behavior that are determined to be non-threatening.	<ul style="list-style-type: none"> • Typographical errors • Forgotten passwords
<u>Moderate Risk</u>	Any event or pattern of events (malicious or unintentional) that indicate a potential threat to electronic protected health information.	<ul style="list-style-type: none"> • Patterns of repeated Low Risk incidents • Suspicious patterns of incoming data from external sources • Information that email attachments are being opened without proper consideration of risks • Unattended workstation • Backup failure • Misdirected email containing electronic protected health information
<u>High Risk</u>	Any event or pattern of events (malicious or unintentional) that indicate a significant, current threat to electronic protected health information.	<ul style="list-style-type: none"> • Password sharing • IP address spoofing • Unauthorized physical access to health plan facility • Intentional or inadvertent destruction of electronic protected health information • Denial of Service attack • Misuse of high-level access accounts • Computer virus exposure/propagation • Lost or stolen workstations or other media (e.g., disks, CD-ROMs) • Escalation of any combination of Low Risk and Moderate Risk security incidents • Improper computer disposal

- Current Classification of Security Incident: Low Risk Moderate Risk High Risk

Explanation of analysis: _____

2. Explain the steps taken to minimize the harmful effect of the security incident: _____

3. Review the possible responses to the security incident using the Security Incident Response Matrix as a guide. Recognize that the response in any particular circumstance must be determined on a case-by-case basis and that the Response Matrix cannot provide guidance on every possible response.

SECURITY INCIDENT RESPONSE MATRIX

INCIDENT LEVEL	INCIDENT RESPONSE
<u>Low Risk</u>	<ol style="list-style-type: none"> 1. Incident reported to Security Official on non-expedited basis (e.g., weekly reports or interoffice routing). 2. Logging and monitoring shall be intensified when deemed reasonable and appropriate by the Security Official. 3. Consider whether it is appropriate to log report of situation.
<u>Moderate Risk</u>	<ol style="list-style-type: none"> 1. Incident shall be immediately reported to Security Official. 2. Security Official shall immediately review the incident to determine if action needs to be taken. 3. The party (or parties) involved with and/or responsible for the threat shall be contacted to obtain details of the potential security threat. 4. If immediate action is not necessary, logging and monitoring of the potential security threat shall be intensified when deemed reasonable and appropriate by the Security Official. 5. If workforce member is involved, contact member and discuss situation. 6. Incident and incident resolution details shall be documented and logged.
<u>High Risk</u>	<ol style="list-style-type: none"> 1. Incident shall be immediately reported to Security Official. 2. Security Official shall immediately review the incident to determine what action will be taken. 3. Incident shall be noted and logged separately from the initial security incident logs and reported directly to other management, if deemed reasonable and appropriate by the Security Official. 4. The party (or parties) involved with and/or responsible for the threat shall be notified and advised about the details of the security threat. 5. If workforce member is involved, contact member and discuss situation. Involve Human Resources Department, for potential disciplinary action, as Security Official deems reasonable and appropriate. 6. Consider whether to contact law enforcement authorities if criminal activity is suspected.

- Based on the above Security Incident Response Matrix, describe the actions taken: _____

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: 4/20/05

Version 1, 09/04

T:\clienta\045146\0001\A0920999.1

ONEIDA HEALTH CARE BENEFIT PLAN

CONTINGENCY PLAN

Purpose: This Form is used to document the health plan's contingency plans to help secure electronic protected health information. This Form also establishes the plan's policies and procedures regarding the contingency plan.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Data Backup Plan Policy

It is the policy of the health plan to have a data backup plan to help secure electronic protected health information. The backup plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The backup plan will be designed to create and maintain retrievable exact copies of electronic protected health information.

SECTION B: Data Backup Plan Procedures

The following backup procedures, if chosen, shall be followed:

1. Data Included in Backup Plan. The following data will be subject to the backup plan:

All electronic protected health information held by the plan's workforce on servers or AS 400

2. Frequency of Backup. Data will be backed up daily.

3. Storage of Backup Data. Data that has been backed up will be stored by a third party vendor: (1) on a daily basis for AS 400 and (2) on a weekly basis for the server.

4. Performing of Backup. Data will be backed up by Oneida MIS via software.

5. Integrity of Backups. The backups will be examined and audited every day by Oneida MIS to verify the integrity of the backed up data.

SECTION C: Disaster Recovery Plan Policy

It is the policy of the health plan to have a disaster recovery plan. The disaster recovery plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The disaster recovery plan will be designed to restore any loss of relevant electronic protected health information.

SECTION D: Disaster Recovery Plan Procedures

1. Assessment of Damage and Loss of Data. The Security Official, in conjunction with MIS management, will gather as much information as possible to determine how much electronic protected health information was lost in a disaster. The Security Official, in conjunction with MIS management will gather information about each potentially affected area where electronic protected health information was stored.

2. Designee of Security Official. In the event the Security Official is unavailable, the Security Official designates Oneida MIS Manager to act in place of the Security Official. The Security Official will communicate this designation to the designated individual.

3. List of Third Party Vendors. The Security Official will determine, prior to any disaster, which third party vendors are likely to be available to assist in recovering the data (e.g., a vendor who holds backup data or a vendor

who specializes in recovering data from damaged computers) or providing additional equipment. Vendors and their anticipated roles are as follows :

Vendor	Role
HP/Bedrock	Replacement of server hardware
Computech	Equipment for restoration of AS-400

4. **General Procedures for Restoring Information System.** MIS Network Team will rebuild server with operating system and restore server data from tape.

SECTION E: Emergency Mode Operation Plan Policy

It is the policy of the health plan to establish and implement an emergency mode operation plan. The emergency mode operation plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The emergency mode operation plan will be designed to enable the plan to continue critical business processes for protecting the security of electronic protected health information while operating in emergency mode.

SECTION F: Emergency Mode Operation Plan Procedures

1. **Reassignment of Duties.** The Security Official will consider which operations are most critical based on the particular emergency encountered by the plan. The Security Official should reassign duties if necessary (e.g., critical functions may take priority over long-term projects). The Security Official should promptly discuss any reassignments with affected workforce members.

2. **Physical Security.** The Security Official will consider whether additional physical security (e.g., a locking file cabinet to hold disks or CD-ROMs) is necessary due to the emergency situation. If so, the Security Official will obtain necessary items as soon as reasonably possible. If it is reasonably possible to anticipate what physical security items will be required, the Security Official should list those items here: secured site will be designated by director of MIS on a case by case basis. Backup tapes and data will be collected and brought to that area.

3. **Technical Security.** The Security Official will work with the workforce and appropriate third party vendors to implement any technical security mechanisms required due to the emergency situation.

SECTION G: Testing and Revision Procedures and Applications and Data Criticality Analysis

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Testing and Revision Procedures—Implement procedures for periodic testing and revision of contingency plans.
- Applications and Data Criticality Analysis—Assess the relative criticality of specific applications and data in support of other contingency plan components.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented both Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. **Risk.** Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- Testing and Revision Procedures Low Medium High
- Applications and Data Criticality Analysis Low Medium High

Explanation of analysis

2. **Cost.** Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Testing and Revision Procedures Low Medium High
- Applications and Data Criticality Analysis Low Medium High

Explanation of analysis

3. **Benefit.** Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Testing and Revision Procedures Low Medium High
- Applications and Data Criticality Analysis Low Medium High

Explanation of analysis:

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Testing and Revision Procedures Feasible and Not Difficult Feasible but Difficult Not Feasible
- Applications and Data Criticality Analysis Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: Contingency testing is not a feasible option for programs residing on the AS/400. To test the contingency plan would involve an expenditure of \$1 million or more to get a second AS/400 to restore to. This option is neither practical nor feasible.

5. **Policy.** Based on the above, the health plan **will not** adopt a policy and procedure regarding the *Testing and Revision Procedures Implementation Specification*. The health plan **will** adopt a policy and procedure regarding the *Applications and Data Criticality Analysis Implementation Specification*.

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

• **Applications and Data Criticality Analysis**

It is the policy of the health plan to conduct an applications and data criticality analysis. The analysis will include the following:

- X Identification of systems which are the most important parts of the contingency plan;

X Identification of how the systems interact in order to recognize potential failures if one or several systems are not available;

X Identification of reasonable and appropriate modifications that can be made to address potential failures

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

See G(4) above. Alternatives include restoring server from off site tape backup.

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: The alternative selection is the current procedure.

3. **Policy.** Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows:

See B(1) above.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0921186.1

ONEIDA HEALTH CARE BENEFIT PLAN EVALUATION

Purpose: This Form is used to document how the health plan will evaluate its security policies and procedures to ensure they comply with the Security Rule.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Evaluation Policy

It is the policy of the health plan to conduct a periodic technical and nontechnical evaluation of its security policies and procedures to determine if those policies and procedures, and the implementation of those policies and procedures, complies with the Security Rule. The Security Official, in conjunction with the Security Committee will decide the proper way to conduct this evaluation and how often to conduct the evaluation.

SECTION B: Evaluation Procedures

1. Entity to Conduct Evaluation. The Security Official, in conjunction with the Security Committee must determine who will conduct the evaluation. The Security Official first must determine whether the evaluation will be performed by a workforce member (such as the Security Official) or a third party (such as a consultant or attorney). The Security Official will consider the following factors:

- Cost of evaluation;
- Expected thoroughness of evaluation;
- Understanding of the health plan and its operations;
- Understanding of security policies and procedures;
- Whether a technical evaluation could be conducted by one entity, while a nontechnical evaluation could be conducted by another entity;
- Consideration of advantages and disadvantages of having a third party conduct the evaluation. Advantages include separating the responsibility of creation and oversight (e.g., so the Security Official is not evaluating the Security Official's own work) and perhaps being able to hire an expert with additional technical and nontechnical experience in the area. Disadvantages include the potential additional time to conduct the analysis and cost.

Based on the above considerations, **Oneida MIS** will conduct the technical evaluation. Based on the above considerations, **Deloitte and Touche or other reputable third party auditor** will conduct the nontechnical evaluation.

2. Frequency of Evaluation. The evaluation initially will occur every year. The Security Official will reconsider every year whether the evaluation period should be modified.

3. Use of Evaluations. The Security Official will consider the results of the evaluations and make all reasonable and appropriate modifications to the plan's security policies and procedures.

4. Retention of Evaluation Results. The Security Official will retain the results of the evaluation for at least six (6) years after the completion of the evaluation.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\cienta\045146\0001\A0960450.1

SECTION A: Evaluation Policy

It is the policy of the health plan to conduct a periodic evaluation and assessment of its security policies and procedures to determine if these policies and procedures are effective and in compliance with the Security Officer's report. The Security Officer is responsible for the Security Officer's report. The Security Officer will conduct the evaluation and assessment and will report the results to the Board of Directors.

SECTION B: Evaluation Procedures

1. Entry to Control Evaluation: The Security Officer, in cooperation with the Board of Directors, will determine the scope of the evaluation. The Security Officer will determine whether the evaluation will be performed by a third party vendor (such as the Security Officer) or a third party (such as a consultant or attorney). The Security Officer will coordinate the following items:

- Cost of evaluation
 - Required management of evaluation
 - Dates and scope of the audit plan and its operation
 - Identification of security policies and procedures
 - Whether a technical evaluation could be conducted by the entity, with a consultant evaluation could be conducted by a third party
 - Consideration of advantages and disadvantages of having a third party conduct the evaluation. Advantages include: outside expertise, objectivity, and the Security Officer's report. Disadvantages include: the potential additional time to conduct the analysis and cost.
- Based on the above considerations, the Security Officer will conduct the technical evaluation. Based on the above considerations, the Security Officer will conduct the technical evaluation. Based on the above considerations, the Security Officer will conduct the technical evaluation.

2. Frequency of Evaluation: The evaluation will occur every year. The Security Officer will determine every year whether the evaluation period should be modified.

3. Use of Evaluation: The Security Officer will conduct the results of the evaluation and report the results and appropriate modifications to the plan's security policies and procedures.

4. Retention of Evaluation Results: The Security Officer will retain the results of the evaluation for at least six (6) years after the last date of the evaluation.

ONEIDA HEALTH CARE BENEFIT PLAN

FACILITY ACCESS CONTROLS

Purpose: This Form is used to document the health plan's decision whether to implement policies and procedures regarding the Facility Access Controls Standard. The Form also establishes any selected policies and procedures related to the Standard.

Retention: This Form must be retained in the health care provider's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Facility Access Controls

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement none, some or all of the Implementation Specifications:

- **Contingency Operations**—Procedures to allow access to the plan's facility to help restore data lost in an emergency, considering the disaster recovery plan and emergency mode operations plan.
- **Facility Security Plan**—Policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering and theft.
- **Access Control and Validation Procedures**—Procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.
- **Maintenance Records**—Policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented all these Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- Contingency Operations Low Medium High
- Facility Security Plan Low Medium High
- Access Control and Validation Procedures Low Medium High
- Maintenance Records Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Contingency Operations Low Medium High
- Facility Security Plan Low Medium High

- Access Control and Validation Procedures Low Medium High
- Maintenance Records Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Contingency Operations Low Medium High
- Facility Security Plan Low Medium High
- Access Control and Validation Procedures Low Medium High
- Maintenance Records Low Medium High

Explanation of analysis: _____

4. Feasibility. Determine the feasibility of implementing a procedure for each Implementation Specification:

- Contingency Operations Feasible and Not Difficult Feasible but Difficult Not Feasible
- Facility Security Plan Feasible and Not Difficult Feasible but Difficult Not Feasible
- Access Control and Validation Procedures Feasible and Not Difficult Feasible but Difficult Not Feasible
- Maintenance Records Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. Policy. Based on the above, the health plan **will** adopt a policy and procedure regarding the following Implementation Specifications:

- Contingency Operations.
- Facility Security Plan.
- Access Control and Validation Procedures.
- Maintenance Records.

_____ The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

• **Contingency Operations.** The health plan's policy is to have a policy allowing reasonable facility access to authorized personnel to restore data lost (or perhaps lost) due to an emergency. This policy will work in conjunction with any disaster recovery plan and emergency mode operations plan. The Security Official will first determine the risk of accessing the provider's physical structure (e.g., if the building was damaged due to a tornado, whether it is safe to enter the building). The Security Official will work with local authorities to help make this determination.

The Security Official will, if reasonable and appropriate, accompany the workforce member or third party vendor when they work to recover the lost data. The Security Official will consider whether any third parties will be considered business associates. If so, the Security Official will enter into a business associate agreement with the third party vendor prior to any emergency.

• **Facility Security Plan.** The health plan's policy is to have procedures to safeguard the plan's facility and equipment therein from unauthorized physical access, tampering and theft. The health plan will:

X Provide identification badges to all workforce members and require that the badges be worn at all times while at work;

X Require visitors and vendors to sign in and out when visiting the plan's facilities, and maintaining that log for at least 6 months.

X Identify areas which, due to the sensitivity of the electronic protected health information stored at the area, may not be accessed by certain classes of workforce members, visitors or vendors. These areas include:

All electronic EPHI is stored on the Casino Server, the Health Center Server, the Social Services Server and AS-400. Only authorized individuals may access these areas.

The Security Official will ensure that workforce members, visitors or vendors are not allowed access to this area by:

- x Physical security measures (e.g., locked doors or electronic key card access required);
- x Stationing of Personnel (e.g., having a receptionist placed near the site to verify that no access occurs); and / or
- x Requiring key or proximity card to access

X Examining physical structures (e.g., doors and windows) to assess vulnerability to intrusion;

• **Access Control and Validation Procedures.** The health plan's policy is to establish a procedure to control and validate a person's access to the provider's facilities, based on the person's role or function. This includes visitor control, and control of access to software programs for testing and revision. The health plan will (note: some items duplicative of Facility Security Plan procedure, above):

X Provide identification badges to all workforce members and require that the badges be worn at all times while at work;

X Require visitors and vendors to sign in and out when visiting the provider's facilities, and maintaining that log for at least 6 months.

X Identify areas which, due to the sensitivity of the electronic protected health information stored at the area, may not be accessed by certain classes of workforce members, visitors or vendors. These areas include: *All electronic EPHI is stored on the Casino server, Health Center Server, and AS-400. Only authorized workforce members may access these areas.*

The Security Official will ensure that workforce members, visitors or vendors are not allowed access to this area by:

- X Physical security measures (e.g., locked doors or electronic key card access required);
- X Stationing of Personnel (e.g., having a receptionist placed near the site to verify that no access occurs); and / or

X Requiring that only a select group of authorized information technology workforce members are able to access software programs for testing and revision, with the select group specified by the Security Official. To ensure that only the select group has such access, the provider will:

- X Design its computer specifications so that only authorized users are able to access software programs for testing and revision purposes;
- X Not leave software in an unsecured location; and / or
- X Provide for discreet testing environments;

• **Maintenance Records.** The health plan's policy is that it will establish a procedure to document repairs and modifications to the physical components of a facility which are related to security (including but not limited to hardware, walls, doors and locks). All actions are to be taken by the Security Official, acting through Oneida MIS, as promptly as reasonably possible. The health care provider establishes this procedure by adopting the following components:

- X The Security Official will consider all proposed maintenance to the facility to determine the security issues, if any, raised by the maintenance;
- X If the plan's facilities are shared with another entity, the Security Official will discuss the provider's need to be apprised, in advance when possible, of maintenance that could impact the provider's physical security;
- X Records describing the maintenance work and who performed the work shall be retained for at least one year.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health care provider chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health care provider determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health care provider considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health care provider will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: [*Describe policy and procedure; may want to base language off Section A(5), above.*]

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0960452.1

ONEIDA HEALTH CARE BENEFIT PLAN

WORKSTATION USE

Purpose: This Form is used to develop a policy and procedure for the health plan regarding the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will have a procedure governing its workforce's use of computer workstations. This policy will specify: (1) the proper functions to be performed; (2) the manner in which those functions are to be performed; and (3) the physical attributes of the surroundings of a specific workstation or class of workstation, if that workstation can access electronic protected health information.

SECTION B: Procedure.

1. Proper Functions to be Performed. The Security Official will determine which functions are appropriate for particular workstations. For example, the Security Official may determine that it is not proper to access electronic protected health information at a workstation that cannot be reasonably secured (e.g., a receptionist's workstation where many visitors could view the screen). The Security Official may also determine that some workstations should not be used for some purposes. For example, if a computer's hard drive contains significant electronic protected health information that is not stored elsewhere, and there is concern about malicious software for which no effective remedy is available, the Security Official may direct that that particular computer not be used to open email or download files from the Internet due to concerns about the malicious software.

Considering these factors, the Security Official implements the following procedure: *Employees with access to EPHI shall only access such EPHI from appropriate workstations as designated by plan. Existing policies restrict what users may or may not do at Windows workstations.*

2. Manner in Which Functions are to be Performed. All plan workforce functions involving electronic protected health information are to be performed in a manner that, in the opinion of the Security Official, reasonably protects the integrity and availability of electronic protected health information. In order to achieve this, the health plan requires that:

- All workstations have password-protected screen savers whose password feature applies after two minutes (or as deemed appropriate by department) of inactivity;
- When a workforce member logged on to AS-400 intends to leave his or her workstation for longer than 30 minutes the member will log off the workstation;
- When a workforce member has completed work for the day the member will log off the workstation;
- Vendors using health plan workstations shall follow the same rules as workforce members. These rules will be communicated to the vendors by the Security Official;

3. Physical Attributes of Surroundings. The HIPAA Security Committee shall analyze the physical attributes of the surroundings of every workstation within the control of the plan that can access electronic protected health information. The Security Official shall consider all relevant criteria in determining the security of such a workstation, including:

X Whether monitors are positioned in a way to minimize the risk that electronic protected health information can be viewed by non-authorized individuals;

X Whether individuals authorized to access electronic protected health information should be grouped in one or more separate areas to minimize the risk of accidental disclosures of electronic protected health information;

X Whether individuals authorized to access electronic protected health information have been trained on the importance of these workstation use rules and instructed to not alter the workstation surroundings in a way that could jeopardize electronic protected health information;

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0922167.1

ONEIDA HEALTH CARE BENEFIT PLAN
WORKSTATION SECURITY

Purpose: This Form is used to develop a policy and procedure for the health plan regarding physical safeguards for all workstations under the control of the provider. The policy and procedure will help ensure that access to electronic protected health information is restricted to authorized users.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will have a procedure to implement physical safeguards for all workstations under the control of the plan if those workstations have access to electronic protected health information. The procedure will be designed to restrict access to authorized users.

SECTION B: Procedure.

1. Identification of Workstations. The Security Official will identify which workstations can access electronic protected health information. As of the date noted below, these include (See Form 3).

2. Physical Security. The following security provisions are adopted to help ensure compliance with the Workstation Security Standard:

- X The workstation will be logged and inventoried;
- X Each workforce member will be trained to not type in his or her password if the password (or typing of the password) could be viewed by an unauthorized individual;

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 10/04

T:\clienta\045146\0001\A0960554.1

ONEIDA HEALTH CARE BENEFIT PLAN
DISPOSAL AND MEDIA RE-USE

Purpose: This Form is used to develop a policy and procedure for (1) the disposal of hardware and / or electronic media containing electronic protected health information; and (2) removing electronic protected health information from electronic media before the media is made available for re-use.

Retention: This Form must be retained in the health care plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will have a procedure governing the (1) disposal of hardware and / or electronic media containing electronic protected health information; and (2) removing electronic protected health information from electronic media before the media is made available for re-use.

SECTION B: Procedure for Disposal of Hardware and / or Electronic Media.

1. Notification to Workforce Members. In *Form 5, Information System Activity Review*, the Security Official determined where electronic protected health information was stored or maintained, either in physical form (e.g., a disk or CD-ROM) or electronic form (e.g., a computer's hard drive). The Security Official shall train all workforce members that hardware and other electronic media containing electronic protected health information must be (a) sanitized so no electronic protected health information is accessible; or (b) destroyed or altered so that no electronic protected health information is accessible.

2. Additional Steps. The Security Official shall take the following additional steps to help ensure that electronic protected health information is not accessible when hardware and / or electronic media is disposed:

- Place a notification (e.g., a small sticker) on the hardware or media that the hardware or media contains or likely contains electronic protected health information that must be sanitized prior to disposal;
- Require that all disposals of hardware or media containing or likely containing electronic protected health information must be approved by the Security Official;
- Require that the following general types of hardware and media be sanitized in the following ways prior to disposal, or be destroyed in a manner so that electronic protected health information will no longer be accessible:

Disks Reformatted

CD-ROMs Destroyed

Personal Computers, laptops Hard drives are reformatted

Servers Reformatted

The Security Official will audit and update *Form 5, Information System Activity Review*, every 6 months to verify whether any hardware or media has been added and to verify that previously reported hardware and media remain; and / or

SECTION C: Procedure for Re-Use.

1. Identify Re-Useable Devices. In *Form 5, Information System Activity Review*, the Security Official determined where electronic protected health information was stored or maintained, either in physical form (e.g., a disk or CD-ROM) or electronic form (e.g., a computer's hard drive). The Security Official should identify whether all or some of the hardware and media may be re-used:

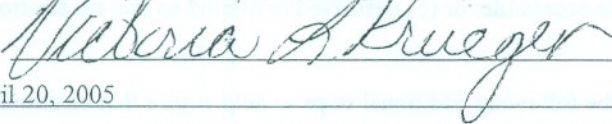
- All hardware and media may be re-used;
- Only the following hardware and media may be re-used: _____

2. Notification to Workforce Members. All provider workforce members will be notified that the devices described above may be re-used to store electronic protected health information subject to these procedures.

3. Proper Method of Sanitizing Hardware and Media. The method for sanitizing electronic protected health information from the hardware and media described above is:

- See #2 above. _____

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

T:\client\045146\0001\A0960563.1

ONEIDA HEALTH CARE BENEFIT PLAN
ACCOUNTABILITY AND DATA BACKUP AND STORAGE

Purpose: This Form is used to document the health plan's decision whether to implement policies and procedures regarding the Accountability and Data Backup and Storage Implementation Specifications. The Form also establishes any selected policies and procedures related to each chosen Specification.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Accountability and Data Backup and Storage

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- **Accountability**—Consider whether to maintain a record of hardware and electronic media and any person responsible for those items.
- **Data Backup and Storage**—Consider whether the plan should be able to create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Accountability and Data Backup and Storage Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- **Accountability** Low Medium High
- **Data Backup and Storage** Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- **Accountability** Low Medium High
- **Data Backup and Storage** Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- **Accountability** Low Medium High
- **Data Backup and Storage** Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Accountability Feasible and Not Difficult Feasible but Difficult Not Feasible
- Data Backup and Storage Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan *will* adopt a policy and procedure regarding the following Implementation Specifications:

- X Accountability
- X Data Backup and Storage

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Accountability.** The health plan's policy is to maintain a record of hardware and electronic media and any person responsible for those items. The Security Official will create and maintain this list. The Security Official will use Attachment A to this Form 19, or an equivalent form, as the basis for creating and maintaining the list. The Security Official will update Attachment A as necessary.

- **Data Backup and Storage.** The health plan's policy is to take the necessary steps to be able to create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. This will apply to the following equipment:

- All equipment;
- X Servers and other large hardware;
- Desktop computers;
- Laptop computers;
- Other portable devices including _____ [Describe portable device, e.g., personal digital assistant ("PDA")]; and / or

This will occur by the following methods:

- X Automatically: Veritas "Back up Exec" for Intel Server and OS-400 for the AS-400 system.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: [*Describe policy and procedure; may want to base language off Section A(5), above.*]

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

ATTACHMENT A

Description of Hardware and / or Electronic Media	Responsible Person	Date Responsibility Assigned
Intel Server (QSI, Indian Health Service)	MIS	
AS-400	MIS	

T:\client\045146\0001\A0923182.1

ONEIDA HEALTH CARE BENEFIT PLAN

UNIQUE USER IDENTIFICATION AND EMERGENCY ACCESS PROCEDURE

Purpose: This Form is used to develop a policy and procedure for (1) assigning a unique name and / or number for identifying and tracking user identity; and (2) establishing (and implementing as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will have a procedure for (1) assigning a unique name and / or number for identifying and tracking user identity; and (2) obtaining necessary electronic protected health information during an emergency.

SECTION B: Procedure for Assigning Unique Name and / or Number

1. Review of Current Software. The Security Official will determine whether the health plan's current software automatically assigns a unique name and / or number for identifying and tracking user identity.

2. Action Based on Review. The Security Official believes that the health plan's current software *is* adequate and satisfies this requirement

SECTION C: Obtaining Necessary Electronic Protected Health Information During Emergency.

1. Providing Temporary, Emergency Access. The Security Official implements the following technical procedures for allowing temporary access to electronic protected health information to an approved user during an emergency:

Relying on current software capabilities to allow temporary, emergency access (e.g., have a current procedure providing for a temporary password);

2. Termination of Temporary Access. Temporary, emergency access provided pursuant to Section C(1) shall be terminated immediately if the Security Official determines that the access has resulted in misuse of electronic protected health information. Temporary, emergency access provided pursuant to Section C(1) shall be terminated as soon as the emergency access is no longer needed. This is determined and occurs:

Automatically by software (e.g., terminates after one day) {Note: automatic termination must occur quickly, or there is a risk that user will have access that is not "temporary" or not related to the "emergency"};

By software upon direction from Security Official; and / or

Name of Security Official: Victoria L. Krueger

Signature: _____

Victoria L. Krueger

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0923555.1

ONEIDA HEALTH CARE BENEFIT PLAN
AUTOMATIC LOGOFF AND ENCRYPTION AND DECRYPTION

Purpose: This Form is used to document the health plan's decision whether to implement policies and procedures regarding the Automatic Logoff and Encryption and Decryption Implementation Specifications. The Form also establishes any selected policies and procedures related to each chosen Specification.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Automatic Logoff and Encryption and Decryption

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Automatic Logoff—Consider whether to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- Encryption and Decryption—Consider whether to implement a mechanism to encrypt and decrypt electronic protected health information.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Automatic Logoff and Encryption and Decryption Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- Automatic Logoff Low Medium High
- Encryption and Decryption Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Automatic Logoff Low Medium High
- Encryption and Decryption Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Automatic Logoff Low Medium High
- Encryption and Decryption Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Automatic Logoff Feasible and Not Difficult Feasible but Difficult Not Feasible
- Encryption and Decryption Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan X will will not adopt a policy and procedure regarding the following Implementation Specifications:

- X Automatic Logoff
- X Encryption and Decryption

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Automatic Logoff.** The health plan's policy is to implement electronic procedures that terminate an electronic session after *2 minutes on PC, 5 minutes on AS-400*. This will be accomplished by:

- X Using the following, existing software: Windows password protected screen savers _____;
- Purchasing and using the following software: _____;
- Designing custom software to accomplish the purpose; and / or
- _____.

The software will be tested when it is initially installed to ensure it functions properly. The software will be tested on an as-needed basis thereafter.

- **Encryption and Decryption.** The health plan's policy is to implement a mechanism to encrypt and decrypt electronic protected health information. This will be accomplished by:

- X Using the following existing software: Groupwise _____;
- Purchasing and using the following software: _____;
- Designing custom software to accomplish the purpose; and / or
- _____.

The software will be tested when it is initially installed to ensure it functions properly. The software will be tested on an as-needed basis thereafter.

The health plan will encrypt electronic protected health information:

X When transmitted electronically (e.g., email); and / or

When stored electronically (e.g., on a computer's hard drive) at all locations or at the following locations: _____

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. Description of Alternatives. If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

2. Cost, Benefit and Feasibility of Alternative Measures. Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. Policy. Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows

Name of Security Official: Victoria L. Krueger

Signature: _____

Victoria L. Krueger

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0925250.1

ONEIDA HEALTH CARE BENEFIT PLAN
AUDIT CONTROLS

Purpose: This Form is used to develop a policy and procedure for the health plan to implement hardware, software and / or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will implement hardware, software and / or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

SECTION B: Procedure.

1. Identification of Audit Control Features. The Security Official will identify audit control features of the health plan's existing software that can help determine which users have accessed electronic protected health information. This is as follows: Access is controlled by menu options, application controls for authorization levels, identity of last user to update file in Encore , and lab has full audit trail.

2. Determination of Needed Audit Controls. The Security Official has determined that:

- The audit controls identified above are sufficient; or
- The audit controls identified above are not sufficient. Additional audit controls will be implemented: _____

3. Implementation of Audit Controls. The Security Official will implement the audit controls identified above.

4. Testing of Audit Controls. The Security Official will test the audit controls when initially implemented to determine their functionality. The Security Official will re-test the audit controls on an as-needed basis.

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0925334.1

ONEIDA HEALTH CARE BENEFIT PLAN
MECHANISM TO AUTHENTICATE ELECTRONIC
PROTECTED HEALTH INFORMATION

Purpose: This Form is used to document the health plan's decision whether to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Mechanisms to Authenticate Electronic Protected Health Information

The Security Official must determine whether it is reasonable and appropriate to implement the Mechanisms to Authenticate Electronic Protected Health Information Implementation Specification. This Specification requires the health plan to decide whether to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

The Security Official will determine whether this Implementation Specification is reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Implementation Specification, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing the Implementation Specification:

Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for the Implementation Specification:

Low Medium High

Explanation of analysis: _____

4. Feasibility. Determine the feasibility of implementing a procedure for the Implementation Specification:

Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan will will not adopt a policy and procedure regarding the Mechanism to Authenticate Electronic Protected Health Information Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible.

The health plan's policy is to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. The health plan will do this by:

Using existing mechanisms: Access is controlled by available menu options, application controls for authorization levels, identification of last user to update file.

Obtaining additional mechanisms: _____

The Security Official will monitor these mechanisms, and new mechanisms that become available, on an as-needed basis to ensure that the plan continues to maintain appropriate electronic mechanisms.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding the Implementation Specification.

1. **Description of Alternatives.** If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures.

Cost Low Medium High

Benefit Low Medium High

Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows: *[Describe policy and procedure; may want to base language off Section A(5), above.]*

Name of Security Official: Victoria L. Krueger

Signature: 

Date: April 20, 2005

Version 1, 09/04

ONEIDA HEALTH CARE BENEFIT PLAN
PERSON OR ENTITY AUTHENTICATION

Purpose: This Form is used to develop a policy and procedure for the health plan to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Policy.

It is the policy of the health plan that the plan will verify that a person or entity seeking access to electronic protected health information is the one claimed.

SECTION B: Procedure.

1. Identification of Ways of Accessing Electronic Protected Health Information. In *Form 5, Information System Activity Review*, the health plan previously identified where electronic protected health information is stored in physical form (e.g., disks and CD-ROMs) and in electronic form (e.g., on servers' hard drives). The Security Official will review *Form 5, Information System Activity Review*, when completing this form.

2. Methods of Ensuring Person or Entity Authentication. The health plan adopts the following methods of ensuring that the person or entity accessing or requesting access to electronic protected health information is the one claimed:

X Physical Form:

Passwords;

Tokens;

Biometric methods: _____

[Describe; e.g., fingerprint recognition];

Personal identification number ("PIN"); and / or

X Identification Cards _____

X Electronic Form:

X Passwords;

Tokens;

Biometric methods: _____

[Describe; e.g., fingerprint recognition];

Personal identification number ("PIN"); and / or

3. Different Methods Depending on Access. If different methods of authentication exist depending on the method of access (e.g., password is used for remote access when person connects through computer at home; fingerprint

recognition used when accessing electronic protected health information at health plan's facilities) describe the different methods: _____

Name of Security Official: Victoria L. Krueger

Signature: *Victoria L. Krueger*

Date: April 20, 2005

Version 1, 09/04

T:\cienta\045146\0001\A0927081.1

ONEIDA HEALTH CARE BENEFIT PLAN

INTEGRITY CONTROLS AND ENCRYPTION

Purpose: This Form is used to document the health plan's decision whether to implement policies and procedures regarding the Integrity Controls and Encryption Implementation Specifications. The Form also establishes any selected policies and procedures related to each chosen Specification.

Retention: This Form must be retained in the health plan's records for at least six (6) years from the date below.

SECTION A: Determination of Need for Integrity Controls and Encryption

The Security Official must review the following Implementation Specifications and determine whether it is appropriate to implement one, both or none of these Implementation Specifications:

- Integrity Controls—Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
- Encryption—Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

The Security Official will determine whether these Implementation Specifications are reasonable and appropriate based on the factors listed below, in (1) – (4). (If the Security Official already knows it is reasonable and appropriate, or has already implemented the Integrity Controls and Encryption Implementation Specifications, skip (1) – (4) and proceed directly to (5).)

1. Risk. Rate the risk if the health plan does not have a procedure in place regarding the Implementation Specification:

- Integrity Controls Low Medium High
- Encryption Low Medium High

Explanation of analysis: _____

2. Cost. Determine or estimate the cost of implementing procedures addressing each Implementation Specification:

- Integrity Controls Low Medium High
- Encryption Low Medium High

Explanation of analysis: _____

3. Benefit. Determine or estimate the benefit of implementing a procedure for each Implementation Specification:

- Integrity Controls Low Medium High
- Encryption Low Medium High

Explanation of analysis: _____

4. **Feasibility.** Determine the feasibility of implementing a procedure for each Implementation Specification:

- Integrity Controls Feasible and Not Difficult Feasible but Difficult Not Feasible
- Encryption Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

5. **Policy.** Based on the above, the health plan X will will not adopt a policy and procedure regarding the following Implementation Specifications:

- X Integrity Controls
- X Encryption

The following policies and procedures shall be used for each selected Implementation Specification. All actions shall be performed by the Security Official (unless otherwise noted) as soon as reasonably possible:

- **Integrity Controls.** The health plan's policy is to implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. This will be accomplished by: Using existing software and possibly digital signatures.

- **Encryption.** The health plan's policy is to implement a mechanism to encrypt electronic protected health information when appropriate. The following situations are always deemed appropriate for encryption of electronic protected health information:

- X Transmissions to third party administrator;
- X Transmissions to other business associates (e.g., attorney, accountant, benefits consultant);

This will occur by the following methods:

- X Automatically: Groupwise has proprietary encryption;
- X Case-by-Case Basis: Use PGP for e-mail correspondence as required; and / or
- X Data from most EPHI systems is a point to point transmission with user ID's and passwords required to create a private "tunnel." If such transmissions become internet based in the future, PKI certs. would be used.

SECTION B: Alternatives if Implementation Specification Not Selected

Complete this Section B only if, pursuant to Section A, the health plan chose not to enact a policy and procedure regarding one or more Implementation Specifications. Complete this Section B for each Implementation Specification that was not selected (attach additional pages as necessary).

1. **Description of Alternatives.** If the health plan determined under Section A that no policy and procedure was appropriate or necessary, describe alternative measures, if any, that the health plan considered to achieve the same goals of the Implementation Specification that was not selected:

2. **Cost, Benefit and Feasibility of Alternative Measures.** Consider the cost, benefit and feasibility standards above, as they apply to the alternative measures. Attach additional pages if multiple alternative measures were considered.

Cost Low Medium High

Benefit Low Medium High

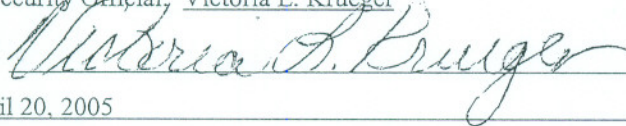
Feasibility Feasible and Not Difficult Feasible but Difficult Not Feasible

Explanation of analysis: _____

3. **Policy.** Based on the above, the health plan will will not enact the alternative measures discussed above. If selected, that policy and procedure is as follows

Name of Security Official: Victoria L. Krueger

Signature: _____



Date: April 20, 2005

Version 1, 09/04

T:\clienta\045146\0001\A0930820.1

ONEIDA HEALTH CARE BENEFIT PLAN
SECURITY RULE PLAN AMENDMENT

WHEREAS, The Plan previously adopted an amendment regarding providing access of protected health information to Wausau Benefits; and

WHEREAS, the Plan Sponsor believe it is reasonable and appropriate to amend the Plan to include provisions relating to the Security Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); and

WHEREAS, the Plan Sponsor reserved the right to amend the Plan.

NOW, THEREFORE, the Plan is amended by adding the following Section 17, effective April 20, 2005:

- 1. **Agents and Subcontractors.** Plan Sponsor will ensure that any agent, including any subcontractor, to which it provides Plan Participants' Electronic Protected Health Information agrees to the restrictions, conditions, and security measures of the Plan Document, as amended by Section 17, with respect to Plan Participants' Electronic Protected Health Information.
- 2. **Security Measures for Electronic Protected Health Information.** Plan Sponsor will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Plan Participants' Electronic Protected Health Information that Plan Sponsor creates, receives, maintains, or transmits on Plan's behalf.
- 3. **Notification of Security Events.** Plan Sponsor will report to the Plan, upon the Plan's request, any attempted or successful (i) unauthorized access, use, disclosure, modification, or destruction of Plan Participants' Electronic Protected Health Information or (ii) interference with Plan Sponsor's system operations in Plan Sponsor's information systems, of which Plan Sponsor becomes aware, except any such security incident that results in disclosure of Plan Participants' Protected Health Information not permitted by the Plan Document, as amended by this Article, must be reported to Plan as soon as reasonably possible.
- 4. **Adequate Separation.** Plan Sponsor will support the adequate separation between Plan Sponsor and the Plan with reasonable and appropriate security measures.
- 5. **Definitions.** For purposes of this Section 17, the term "Participant" means an "individual" as defined in 45 C.F.R. §160.103. All capitalized terms not defined in this amendment shall have the meaning described in the HIPAA Administrative Simplification Rules. Nothing contained in this Document shall be deemed or construed as a waiver of the sovereign immunity of the Oneida Tribe of Indians of Wisconsin.

Adopted : _____

By: _____

Name: _____

Title: _____