HIPAA Security Manual

WinCo Foods, Inc.

Authored by J. Kevin West

TABLE OF CONTENTS

INTRODUCTION

About this Manual

Under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) has promulgated rules and regulations regarding the security of health plan participants' ("plan participants") electronic Protected Health Information (ePHI). These rules will be referred to in this Manual as the HIPAA Security Rule (Security Rule). The deadline for compliance with the Security Rule was April 21, 2005, for large health plans, and April 21, 2006, for small plans.

The Security Rule encompasses protections for electronic protected health information that are in addition to the protections contained in the HIPAA Privacy Rule, which took effect in April 2003 (April 2004 for small plans). As with the Privacy Rule, compliance with the Security Rule is not optional for employer-sponsored group health plans. The Security Rule is a requirement of federal law and will require many group health plans to implement written policies and procedures, as well as certain changes in company practices.

Who and What is Regulated by the Security Rule?

Those employers and group health plans that currently (or in the future) must comply with the HIPAA Privacy Rule must also comply with the Security Rule. The Security Rule applies to all Protected Health Information (PHI) stored or maintained in electronic formats ("electronic Protected Health Information" or "ePHI"). The following are common examples of ePHI:

- Plan participant medical and claim records maintained on the Company's computer system
- Plan participant information transmitted via the Internet
- Health claim information transmitted electronically to insurance companies, brokers or third party administrators
- Emails containing plan participant information or communications
- Plan participant health information in laptops, PDAs and cell phones
- Claim history or payment reports/spreadsheets on Company computers

Commonly Used Terms

The following abbreviations and shorthand expressions will be used for ease of reference in this Manual:

HHS	Health and Human Services.
Company	The organization which implements or uses this Manual.
Company personnel	All personnel, including owners, of the Company.
Group health plan	All employee health, dental or vision benefit plans sponsored by the Company. Includes flexible spending accounts for health care.
Plan participant health information	"Protected Health Information," as defined by HIPAA (see Glossary of Terms).
Electronic PHI or ePHI	"Protected Health Information," in an electronic format.
Manual	This HIPAA Security Manual.
HIPAA	Health Insurance Portability and Accountability Act of 1996.
Business Associate	A company or individual that provides services to health care providers and who receives PHI or ePHI in the course of providing those services. Business Associates contractually agree with their clients to follow HIPAA standards.

POLICIES AND PROCEDURES

Section A: An Introduction to Basic Security Concepts and Compliance

Section B: Administrative Safeguards

Section C: Physical Safeguards

Section D: Technical Safeguards

Section A: An Introduction to Basic Security Concepts and Compliance

1. Purpose of the Security Rule

The general goal of this Security Manual is to:

- Ensure the confidentiality, integrity and availability of all ePHI that the Company creates, receives, maintains or transmits;

- Protect against any reasonably anticipated threats or hazards to the security or integrity of plan participant ePHI; and

- Ensure compliance by the Company's workforce.

2. Security Rule Concepts

The Security Rule was written to be flexible enough to be implemented by either large or small companies. Though the Rule involves many technical matters, no particular brand or technology is required. In most instances, companies should be able to continue the use of existing technology.

The Security Rule consists of eighteen standards, which are organized into the following three categories:

- **Administrative Safeguards** – Administrative safeguards are the policies and procedures the Company should implement to protect ePHI.

- **Physical Safeguards** – Physical safeguards are the security measures that protect the Company's physical facility and information systems. Physical safeguards require the restriction of access to ePHI through the use of such things as door locks or magnetic cards, and by providing backups for all ePHI, such as having a second computer hard drive to perform a daily backup of computer programs containing ePHI.

- **Technical Safeguards** – Technical safeguards are the security measures installed to protect information contained in the information systems. Examples of technical safeguards include individual passwords for each employee accessing ePHI, ensuring that the person accessing ePHI is authorized and is who he/she claims to be, and ensuring that information contained in ePHI is not improperly altered.

For each of the eighteen standards found in these three safeguard categories, there are accompanying "implementation specifications." The eighteen standards describe what must be done to achieve security compliance; the implementation specifications describe how compliance with a standard may be accomplished. Some of the implementation specifications are mandatory; others are optional. The mandatory specifications are referred to in the Security Rule as "required specifications;" the optional specifications are referred to as "addressable specifications." If the Company chooses not to implement an addressable specification, it must document the reason for that choice and what, if anything, is being done in its place.

The goal of the Security Rule is to decrease and/or eliminate security incidents. A "security incident" is some breach of confidentiality, integrity or accessibility of the Company's ePHI. A security incident may be the result of a "threat" (anything that could harm the Company's information system, such as hackers, natural disasters or disgruntled Company personnel), that takes advantage of a "vulnerability" (any weakness in the Company's security measures or information systems).

Section B: Administrative Safeguards

1. Personnel Designations

Security Officer. The Company will designate a person to act as its security officer. The security officer will have responsibility for the overall implementation and oversight of the Company's compliance with the HIPAA Security Rule. The same person may be designated as both security officer and privacy officer. Specifically, the security officer will:

- Oversee the implementation of the policies and procedures contained in this Manual.
- Ensure that all Company personnel are trained regarding the policies and procedures in this Manual as appropriate for their positions and job functions.
- Provide a copy of this Manual to applicable Company personnel and ensure that such personnel follow the policies and procedures contained herein.
- Investigate and respond to security incidents and take appropriate action in response.
- Maintain all documentation required by this Manual and the HIPAA Security Rule.
- Review activity that takes place in all Company information systems to detect possible Security Rule violations and security incidents.
- Respond appropriately to all security incidents and eliminate or mitigate any damaging effects.

2. Training of Company Personnel

2.1 **Training – Generally.** The Company will train applicable Company personnel regarding the HIPAA Security Rule, as well as this Manual, as is reasonable and appropriate for personnel to carry out their respective job duties. Appendix H contains an acknowledgment of receipt and review of this Manual for all Company personnel to sign.

2.2 **Time for Completion of Training.** Initial training of existing Company personnel will be completed prior to October 1, 2013. Training of employees hired after that date will be completed within sixty (60) days of hiring. Ongoing training will be provided to Company personnel as necessary to maintain competency regarding HIPAA policies and procedures, or as needed for changes in the HIPAA Security Rule or this Manual.

2.3 **Documentation of Training.** Training of Company personnel will be recorded in the Security Training and Education Log (Appendix C), and this log will be maintained by the Company for a minimum of six (6) years.

2.4 **Methods of Training.** Company management and the security officer will use their discretion as to the method, location and frequency of training. Such training may, however, include some or all of the following:

- In-service meetings among Company personnel for updates in the Security Rule.
- Review of this Manual.
- Attendance at programs and seminars.
- Review of professional literature and publications.
- Use of Internet resources (Appendix G).
- Retained consultants and professional advisers.

3. Security Management

3.1 **Security Assessment of the Company.** Using the Risk Analysis Checklist in Appendix A, the Company has conducted an accurate and thorough assessment of the current status of the Company's security compliance.

3.2 **Implementation of Security Measures.** Based upon the information obtained in the security assessment, the Company will implement through this Manual the necessary policies and procedures to address the risks and vulnerabilities of the Company's ePHI.

3.3 **Enforcement of Security Policies.** All Company personnel are expected to adhere to the policies and procedures set forth in this Manual. Company personnel who violate the provisions of this Manual will be subject to discipline, which may include:

- A written warning in the employee's personnel file.
- Placement on probation.
- Mandatory additional training regarding the HIPAA Security Rule.
- Demotion or reassignment of job duties.
- Termination.

The security officer will maintain a record of all disciplinary action for a minimum of six (6) years.

3.4 **Reporting of Security Violations.** Company personnel are required to report any violation of the provisions of this Manual, and any security incident, to the security officer. The Company will not retaliate against any employee for reporting these matters. The security officer will track security incidents on the security incident tracking report (see Appendix E).

3.5 **Prevention of Further Violations.** To the extent that security incidents or deficiencies are reported or discovered, the Company will take reasonable steps to ensure that similar violations do not occur in the future by taking appropriate corrective measures.

3.6 **Regular Review.** The security officer will regularly review records of all information system activities for possible security incidents and will implement procedures to correct possible and/or known security incidents. The Company's information system should also be checked frequently and regularly to ensure that daily back-ups have been done and that intrusions into the system have not occurred.

4. Information Access Management

To the extent necessary and reasonable, the Company will protect ePHI from unauthorized access. Company policy will be that –

- Computer and database passwords that give access to ePHI must be authorized by the Company's Privacy Officer, in consultation with Company management;

- Only those personnel listed on page 13 of the Company's HIPAA Privacy manual will have access to rooms, offices or file cabinets containing ePHI; and

- Passwords to computers containing ePHI will be changed at least every one hundred eighty (180) days.

5. Workforce Security

5.1 **Authorized Personnel.** Company will only allow Company personnel or other authorized individuals to access ePHI for purposes allowed under HIPAA.

5.2 **Logoffs.** At the end of the day, all computer users who have access to ePHI must log off and/or shut down computers to prevent unauthorized disclosures.

5.3 **Minimum Necessary.** Company personnel authorized to access ePHI will only be authorized to access the minimum necessary ePHI to perform their job function. Access to any additional ePHI is prohibited.

5.4 **Departing Employees.** Precautions shall be taken to eliminate access to ePHI of Company personnel whose employment is terminated. Such precautions may include, but are not limited to:

- Requiring the return of building/office keys, ID badges or access cards;
- Changing locks on building/office doors;
- Changing computer passwords;
- Requiring the return of laptop computers, PDAs, computer disks, etc.

6. Security Incident Procedure

6.1 **Generally.** Company personnel will report security incidents to the security officer.

6.2 **Respond to Security Incidents.** The Company will respond to security incidents in an appropriate manner depending on the particular incident. This response will ensure that any damage that has occurred is minimized and corrected. If the security incident involves an unauthorized disclosure of PHI, the security officer will follow the plan participant notification procedure set forth in section B.10 of this Manual.

6.3 **Documentation.** Once the harmful effects of the incident have been mitigated, the security officer will document that incident in the Security Incident Tracking Report (see Appendix E for a sample report). This report will include the date and time of the incident, the type of incident and how it occurred, and all measures taken to remedy the breach and prevent similar breaches from recurring.

7. Emergency Plan

7.1 **Data Backup.** The Company will create and maintain ePHI in duplicate form, such as paper copies, tape back-ups, CD-ROM or other external storage device (e.g. a "key or thumb drive"). A back-up copy should be kept both on- and off-site.

7.2 **Emergency Mode Operation Plan.** The Company will establish and implement, as needed, procedures to enable continuation of critical health plan processes of the Company, as well as protection of the security of ePHI during and immediately after a crisis situation. This may require the backup of all systems or may only require the backup of critical programs, depending on the computer system of the Company.

8. Evaluation

The Company will perform periodic evaluations of both technical (e.g. computers) and non-technical (e.g. door locks) security safeguards to determine compliance with the Security Rule. Evaluations should be performed any time there are significant environmental or operational changes that could affect the security of PHI.

9. Disclosure to Business Associates

9.1 **Business Associates.** "Business associates" are third parties who provide services to the Company and in so doing have access to electronic plan participant health information (ePHI). (Examples include: brokers, third party administrators, attorneys. A more extensive definition may be found in Appendix F.)

9.2 **Requirement for Business Associate Agreements.** The Company may disclose plan participant health information to its business associates only if the business associate has signed an agreement to (1) protect plan participant privacy by following HIPAA Privacy Rule, and (2) protect security of ePHI by following HIPAA Security Rule.

9.3 **Time for Obtaining Business Associate Agreements.**

9.3.1 The Company shall have its current business associates sign an agreement the same as or similar to that found in Appendix B.

9.3.2 Those business associates with whom the Company forms a relationship after the above date, must also sign an agreement the same or similar to that found in Appendix B. Plan participant health information may not be disclosed to business associates who fail or refuse to sign agreements by these dates.

10. Plan Participant Notification of Breach of Protected Health Information

10.1 **General Rule.** If the Company discloses unsecured PHI to an unauthorized person, or otherwise allows an unauthorized disclosure of unsecured PHI, the Company must notify the affected plan participant(s), as set forth below. Unsecured PHI means health information that is not protected by technology that renders it unusable or unreadable to unauthorized persons.

10.2 **Plan Participant Notification Procedures**

10.2.1 In the event of an unauthorized disclosure of unsecured PHI, affected plan participants must be notified in writing by first class mail. If the Company does not have current mailing information, notice may be given by telephone or email.

10.2.2 If the Company does not have current contact information on ten (10) or more plan participants affected by the unauthorized disclosure, the Company must give notice by posting on the Company's website for at least 90 days, or by placing a notice in a major print or broadcast media in the geographic area where the plan participants most likely reside.

10.2.3 If the unauthorized disclosure involves 500 or more plan participants, the Company must give notification through major media outlets serving the state(s) in which the plan participates reside. This may be done in the form of a press release.

10.2.4 The written notification given to plan participants will include, to the extent possible, the following:

- A brief description of what happened, including the date of the unauthorized disclosure and the date of its discovery;
- A description of the type of health information involved in the disclosure (e.g. name, Social Security number, date of birth, diagnoses, etc.);
- The steps the plan participant should take to protect himself/herself from potential harm resulting from the disclosure;
- A brief description of what the Company is doing to investigate the disclosure, mitigate its impact and to protect against future unauthorized disclosures; and

- Contact information for the plan participant to ask questions (a toll free telephone number, email address, website or postal address). The template in Appendix I may be used to assist in preparing the notification to the plan participant.

10.2.5 The notice to plan participants described in subsection 10.2.4 must be provided as soon as possible, but in no event later than sixty (60) days after discovery of the unauthorized disclosure by the Company.

10.2.6 If the unauthorized disclosure involved less than 500 plan participants, the Company must maintain a log of the incident and submit the log to the federal Department of Health and Human Services (DHHS) at the end of the calendar year. If the disclosure involves more than 500 plan participants, the Company must notify DHHS immediately.

10.3 **Exceptions.** Plan participant notification of an unauthorized disclosure of PHI will not be required where:

10.3.1 The disclosure is to a member of the Company's workforce, was made in good faith, and does not result in further disclosure;

10.3.2 The disclosure is made under circumstances in which it is unlikely that the unauthorized recipient would be able to retain the information.

11. Technical Standards Published by the Federal Government Regarding Security of PHI

From time to time, the Department of Health and Human Services may publish guidance on technologies and methodologies that will render PHI unusable, unreadable or indecipherable to unauthorized individuals. The Security Officer will review this guidance, if any, on a quarterly basis, and determine whether such may be implemented in the Company's electronic systems.

12. Record Retention and Disposal

12.1 **Policies and Procedures Maintained.** The Company will keep and maintain written policies and procedures that reflect its compliance with HIPAA Security Rule.

12.2 **Document Retention Period.** The Company will retain, for a minimum of six (6) years, all records, documents or information that is generated, created or required to be kept under the policies and procedures in this Manual, or as otherwise required by the HIPAA Security Rule. The six-year period shall run from the date the record was prepared, or the date it was last in effect, whichever is later.

12.3 **Storage in Secure Locations.** Electronic PHI of the Company will be kept or stored in safe, secure locations. Computers or other electronic equipment or media that are stored offsite will be placed only in secure facilities.

13. Reproductive Health Care

13.1 The following is in response to the final regulations issued by the U.S. Department of Health and Human Services on April 22, 2024 and is effective December 23, 2024 if and until the final regulations are modified to provide otherwise.

13.2 PHI and ePHI shall not be used or disclosed where reproductive health care is lawfully provided (or presumed lawful):

- To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care;
- To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care; or
- To identify any person for any purpose described in the two bullets above.

13.3 Where PHI or ePHI sought is potentially related to reproductive health care and is for health care oversight, judicial or administrative proceedings, law enforcement purposes, or to a coroner or medical examiner, a valid attestation as described in 45 CFR Section 164.509 must be obtained before the PHI or ePHI is used or disclosed.

13.4 The foregoing shall be interpreted and applied consistent with the final regulations and associated guidance/applicable law.

Section C: Physical Safeguards

1. Facility Access Controls

The Company will limit unauthorized access to its building and offices, as well as to its information systems. The Company will also ensure appropriate access by Company personnel to ePHI.

2. Computer Workstation Use and Security

2.1 **Minimum Necessary.** Computer workstation access for computers containing ePHI will be limited to those individuals who are authorized to use the workstation. Where such computer workstations are used by more than one person, or where multiple Company computers are part of a network, access by Company personnel will be limited to those programs and databases applicable to the specific job duties of Company personnel.

2.2 **Log Off.** Employees must log off of a computer before leaving it unattended for an extended period of time, including at night.

2.3 **Physical Surroundings.** The physical surroundings of computer workstations will be arranged in a way that promotes security and avoids inadvertent, unauthorized viewing of ePHI.

3. Device and Media Controls

3.1 **Disposal.** When disposing of hardware or electronic media on which ePHI is stored, the data must be destroyed or deleted prior to disposal.

3.2 **Media Reuse.** Any electronic media that is being reused must be erased of all ePHI prior to that reuse.

3.3 **Movement of Information Systems.** The Company will document the receipt or removal of all computer hardware and electronic media that contain ePHI. The Company will also document the destruction or deletion of ePHI when disposing of such hardware and electronic media.

Section D: Technical Safeguards

1. Access Controls

1.1 **Authorized Persons.** Only authorized persons will be allowed access to electronic information systems that store ePHI.

1.2 **User Identification.** All Company personnel with access to ePHI must be assigned a unique user name and/or number for identifying and tracking their identity in the electronic information system. Company personnel cannot share the same password. Passwords to computers containing ePHI will be changed at least every one hundred eighty (180) days.

1.3 **Emergency Access Procedure.** In the event of an emergency, such as a power outage caused by natural and/or manmade disasters, ePHI that is essential for the continuation of plan participant care must be accessible. The security officer and/or network administrator will ensure access to any system containing protected health information in the event of an emergency.

2. Audit Controls

The Company will implement mechanisms to record and examine activity in information systems that include ePHI. The particular auditing mechanism should be appropriate to Company needs and circumstances as determined by the Company's risk analysis.

- The security officer will review firewall audit logs at least monthly to ensure that there has been no improper breach of the network's firewall.

3. Integrity of ePHI

The Company will protect ePHI from improper alteration or destruction by means of security software:

- The Company will maintain updated virus protection software.
- The Company will maintain a sufficient firewall to prevent breaches of security by outside third parties, such as hackers.

4. Person or Entity Authentication

Prior to allowing access to ePHI, the Company will verify the identity of any person or entity seeking such access and will require the use of an authorized password.

5. Transmission Security

The Company will guard against unauthorized access to ePHI transmitted over an electronic communications network.

- Where possible, the Company will avoid sending emails containing ePHI where the plan participant can be identified in the body of the email.

- Where ePHI must be sent via email, the content of the email must be transmitted as a password-protected attachment.

APPENDICES

A. Risk Analysis Checklist

B. Business Associate Agreement

C. Security Training and Education Log

D. Company Resolutions

E. Security Incident Tracking Report

F. Glossary of Terms

G. HIPAA Resources

H. Acknowledgment of Receipt/Review of HIPAA Security Manual

I. Plan Participant Notification of Unauthorized Disclosure

APPENDIX A

Risk Analysis Checklist

RISK ANALYSIS CHECKLIST

The following risk analysis should be completed for your Company. Thinking about and answering these questions will help you recognize security issues in your Company. Completing this checklist will also help you in customizing this Manual to the particular circumstances of your Company.

A. General Information

1. Inventory of computer and electronic hardware owned or used by the Company

- List by name and model each computer owned/used by the Company and which contains ePHI: _____ _____ _____ _____

- List by name and model all laptop computers, personal digital assistants (PDAs) or other portable electronic devices or equipment owned/used by the Company and which contains ePHI: _____ _____ _____ _____

- List all printers and facsimile machines owned/used by the Company and which are used to transmit ePHI: _____ _____ _____ _____

- List by name, address and telephone numbers all vendors or service providers who maintain the above-listed hardware. _____ _____ _____ _____

- For all hardware listed above, does the Company have the drivers and master operating system disks? Yes ☐ No ☐

    - Where are these kept? _____ _____

2. Inventory of company software

- For each computer or laptop listed above, state the operating system (e.g. Windows XP, windows 2000) it uses. _____ _____ _____ _____

- List each software program currently owned or used by the Company (include billing, company management, virus protection, firewall, charting, word processing and spreadsheet programs) to store, transmit or safeguard ePHI. _____ _____ _____ _____

- List passwords or codes, if any, needed to access the above-listed software programs. _____ _____ _____ _____

- For each software program listed above, state whether it has been upgraded and the date of the upgrade. _____ _____ _____ _____

- For each software program listed above, does the Company have the master software disks? Yes ☐ No ☐

  - Where are these kept? _____ _____

  - Are all software licenses current? Yes ☐ No ☐

- List by name, address and telephone number your software vendors and service providers. _____ _____ _____ _____

3. Networks

- Are your Company computers connected via a Local Area Network (LAN) or some other network system? Yes ☐ No ☐

If so, what type of network hardware and software do you have? _____
_____
_____
_____

- List name and type of server hardware. _____
_____
_____

4. Online Transmission and Access

- Does your Company transmit any ePHI electronically? Yes ☐ No ☐

  If so, is this done via:

  ☐ dial-up telephone connection
  ☐ dial-up Internet connection?
  ☐ high speed Internet connection (e.g. DSL, cable, T-1 line)?
  ☐ wireless access?

- Can Company personnel access ePHI your computer system from remote locations? Yes ☐ No ☐

  If so, is this done via:

  ☐ dial-up modem/Internet?
  ☐ high speed Internet?
  ☐ wireless access?

5. Emergency and Security

- Where does the Company keep backup tapes or disks containing ePHI? _____
_____

- Does the Company have:

  ☐ an Emergency Power Supply (EPS)?
  ☐ surge protectors?
  ☐ smoke alarms and fire extinguishers?
  ☐ security alarm system for building or office suite?

<u>Note</u>: The following are yes/no questions that correspond with the Security Rule standards and the sections of this Manual. A "no" answer suggests a potential security deficiency.

B. <u>Administrative Safeguards</u>

1. Personnel Designations. The Company has appointed a security officer. Yes ☐ No ☐

2. Security Awareness and Training

- The security officer has received training regarding the HIPAA Security Rule. Yes ☐ No ☐
- Applicable Company employees have been trained regarding the Company's security policies and procedures. Yes ☐ No ☐
- The Company has documentation reflecting the training of employees (documentation shows date, content of training and name of employee). Yes ☐ No ☐

3. Security Management

- The Company has done a security risk assessment. Yes ☐ No ☐
- The Company has <u>written</u> security policies and procedures. Yes ☐ No ☐
- All door keys or other access devices are accounted for. Yes ☐ No ☐
- Company employees who violate security policies and procedures receive appropriate educational/disciplinary action. Yes ☐ No ☐
- Company employees are encouraged to report security incidents to the security officer. Yes ☐ No ☐

- The Company's response to security incidents is documented. Yes ☐ No ☐

- The Company's security officer (or another employee assigned by her/him) regularly reviews information system activity for possible security incidents. Yes ☐ No ☐

4. Information Access Management

- The Company has a list of all past and current information system or computer passwords. Yes ☐ No ☐

- The Company keeps a log of all employees with keys, passcards or other access devices to the Company's building or office suite. Yes ☐ No ☐

- Door keys are "Do Not Duplicate"-type keys. Yes ☐ No ☐

5. Workforce Security

- Only authorized Company personnel are permitted to have access to ePHI. Yes ☐ No ☐

- Authorized Company personnel only have access to the minimum necessary ePHI for their job duties. Yes ☐ No ☐

- Computer users log off their computers at the end of the day. Yes ☐ No ☐

- Terminating employees are required to return keys, passcards and other access devices. Yes ☐ No ☐

- Terminating employees are required to return Company laptops, PDAs, cellphones or disks. Yes ☐ No ☐

- Passwords are changed on computers when an employee leaves the Company. Yes ☐ No ☐

- If terminating employees fail to return keys or other Company property, action is taken to prevent improper use or disclosure of ePHI (changing door locks, filing police reports, etc.). Yes ☐ No ☐

6. Security Incident Procedures

- The Company responds appropriately to security incidents by investigating and taking corrective action. Yes ☐ No ☐

7. Emergency Planning

- The Company keeps a duplicate copy (paper or electronic) of all ePHI. Yes ☐ No ☐
- Backup copies of ePHI are updated regularly. Yes ☐ No ☐
- Backup copies are kept off-site at a location known to Company personnel. Yes ☐ No ☐
- The Company could, in the event of an emergency (fire, flood, earthquake) restore ePHI that is lost or damaged. Yes ☐ No ☐
- The Company could, in the event of an emergency, ensure access by Company personnel to ePHI. Yes ☐ No ☐
- The Company keeps off-site, or in a fireproof cabinet on-site, copies of software master disks and hardware drivers. Yes ☐ No ☐
- The Company has an emergency plan for restoring lost data and continuing business and plan participant care operations. Yes ☐ No ☐
- The Company has an Emergency Power Supply (EPS) for server computers. Yes ☐ No ☐

8. Evaluation

- The Company evaluates its security risks each time it –

  - upgrades or installs software — Yes ☐ No ☐
  - obtains new computer hardware — Yes ☐ No ☐
  - moves to a new office facility — Yes ☐ No ☐
  - connects to the Internet or establishes another online connection — Yes ☐ No ☐
  - makes some other significant change to its computer system — Yes ☐ No ☐

9. Business Associates

- Does the Company provide ePHI to vendors or service providers (e.g. brokers, third party administrators)? If so,

  - Does the Company have a Business Associate Agreement in place with those parties? — Yes ☐ No ☐

C. Physical Safeguards

1. Facility Access Controls

- Building/office doors, filing cabinets and desks containing ePHI are locked at night. — Yes ☐ No ☐

- Building/office windows are secure and/or barred. — Yes ☐ No ☐

- The building/office has a security alarm system. — Yes ☐ No ☐

2. Computer Workstation Security

- The Company limits use of computers containing ePHI to employees who have a legitimate need for access to such. — Yes ☐ No ☐

- Company employees log off their computers at the end of each work day. — Yes ☐ No ☐

- Company employees turn off computers at the end of each work day. Yes ☐ No ☐

- Company computers return to the logon screen automatically or have password-enabled screensavers that engage when computers are left inactive for any extended period of time. Yes ☐ No ☐

- Computer monitors are placed in such a way as to prevent viewing by unauthorized persons. Yes ☐ No ☐

3. Device and Media Controls

- The Company removes or destroys ePHI on computer hard drives when disposing of computers. Yes ☐ No ☐

- The Company erases or destroys electronic media (disks, tapes, CD-ROMs) that contain ePHI prior to disposal. Yes ☐ No ☐

- The Company erases ePHI on electronic media that is to be re-used by the Company. Yes ☐ No ☐

- The Company has a written inventory of –

  - all electronic and computer hardware containing ePHI Yes ☐ No ☐
  - all software programs used for ePHI Yes ☐ No ☐

- The Company documents (and keeps such documentation) the receipt, removal or disposal of hardware and electronic media. Yes ☐ No ☐

D. <u>Technical Safeguards</u>

1. Access Controls

- All Company personnel are assigned unique user names and passwords. Yes ☐ No ☐

- Company employees do not share passwords. Yes ☐ No ☐
- A master password list is maintained both onsite and offsite in locations known to Company personnel. Yes ☐ No ☐
- User IDs and passwords are not posted on or near workstations. Yes ☐ No ☐
- Laptops, PDAs and other portable electronic equipment containing ePHI are kept physically secured with a lock when not in use. Yes ☐ No ☐
- Passwords are changed on a regular basis. Yes ☐ No ☐
- A history of previously used passwords is kept to prevent reuse. Yes ☐ No ☐

2. Audit Controls

- The Company security officer routinely reviews computer audit logs to check for unusual or unauthorized access to ePHI by Company employees. Yes ☐ No ☐
- The security officer routinely checks for intrusions from outside parties to Company computer systems. Yes ☐ No ☐
- The Company's computer system logs accesses and attempts by date, time, user ID and location. Yes ☐ No ☐
- The Company keeps a log of all security maintenance by date and type of maintenance performed. Yes ☐ No ☐

3. Integrity of ePHI

- The Company has virus protection software, which it keeps updated. Yes ☐ No ☐

- The computer system prevents alteration of "final" or "signed" documents. Yes ☐ No ☐

- For computers containing ePHI that are connected to the Internet, the Company has a firewall. Yes ☐ No ☐

- The Company does regular backups of its electronic data. Yes ☐ No ☐

- The Company regularly audits its user login profiles. Yes ☐ No ☐

- All Company computers have surge protectors. Yes ☐ No ☐

- The Company has smoke alarms and fire extinguishers. Yes ☐ No ☐

4. Person or Entity Authentication

- The Company verifies the identity of those to whom it transmits ePHI. Yes ☐ No ☐

5. Transmission Security

- The Company refrains from transmitting ePHI via the Internet, or only transmits ePHI to secure websites. Yes ☐ No ☐

- If the Company transmits ePHI via the Internet, it uses encryption. Yes ☐ No ☐

- The Company uses only secure dialup lines for purposes of transmitting ePHI electronically. Yes ☐ No ☐

6. Record Retention and Disposal

- The Company retains, for a minimum of six years, all HIPAA compliance documentation. Yes ☐ No ☐

- Computers and electronic media are disposed of properly when discarded by the Company. Yes ☐ No ☐

- Computers and electronic media are stored in secure facilities. Yes ☐ No ☐

APPENDIX B

Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) is made and entered into by and between **WinCo Foods, Inc.** and **_____ [insert name of Business Associate]** on this _____ day of _____, 20___. In consideration of the mutual covenants contained in this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions:

Business Associate. "Business Associate" shall mean **_____ [Insert Name of Business Associate]**.

ePHI. "ePHI" shall mean Protected Health Information transmitted by or maintained in electronic media.

Company. The "Company" shall mean **WinCo Foods, Inc..**

Plan Participant. "Plan Participant" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, as limited to the information created or received by Business Associate from or on behalf of Company.

Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Security Incident. "Security Incident" shall mean a violation of the Security Rule, or the breach of confidentiality, integrity or accessibility of ePHI.

Security Rule. "Security Rule" shall mean the statutes for security of individually identifiable health information at 45 CFR part 164, subpart C.

Unsecured Protected Health Information. Protected Health Information that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals.

2. Obligations and Activities of Business Associate

Business Associate agrees:

(a) Not to use or disclose Protected Health Information other than as permitted or required by this Agreement and the HIPAA Privacy Rule.

(b) To use appropriate safeguards to prevent use or disclosure of the Protected Health Information as specified by the HIPAA Privacy and HIPAA Security Rules.

(c) To mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d) To report to Company any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e) To ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Company, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) To provide access, at the request of Company, and in the time and manner requested by the Company, to Protected Health Information to the Company or, as directed by Company, to Plan Participant in order to meet the requirements under 45 CFR 164.524. Such access may include access to, and copies of,

Protected Health Information maintained by Business Associate in electronic form.

(g) To make any amendment(s) to Protected Health Information in a Designated Record Set that the Company directs or agrees to pursuant to 45 CFR 164.526 at the request of Company or a Plan Participant, and in the time and manner requested by the Company.

(h) To disclose only the minimum necessary Protected Health Information when disclosure must be made. Whenever possible, Business Associate will redact or delete the following items from the Protected Health Information disclosed to others:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images;

(i) Not to sell Protected Health Information that it receives from the Company to any other person or entity.

(j) To make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Company available to the Company, or to the Secretary, in a time and manner requested by the Company or designated by the Secretary, for purposes of the Secretary determining Company's compliance with the Privacy Rule and Security Rule.

(k) To document all disclosures of Protected Health Information and information related to such disclosures as would be required for Company to respond to a request by a Plan Participant for an accounting of disclosures of Protected Health Information in accordance with federal and state laws and regulations.

(l) To report to Company any security incident of which it becomes aware.

(m) To authorize termination of the Agreement by Company, if Company determines that the Business Associate has violated a material term of the contract.

(n) To give notice to a Plan Participant, in the form and manner directed by the Company, if Business Associate causes or allows an unauthorized disclosure of unsecured Protected Health Information.

(o) To follow, to the extent possible, the guidelines published by the Secretary relating to the technology for rendering electronic Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

3. Permitted Uses and Disclosures by Business Associate

[use one of the following versions]

Specific purposes: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Company for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule or Security Rule if done by Company or the minimum necessary policies and procedures of the Company:_____
_____
_____
_____
[List Purposes].

<or>

Underlying services agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities or services for, or on behalf of, Company as specified in the agreement with _____ **[Insert Name of Business Associate]**, provided that such use or disclosure would not violate the Privacy Rule or Security Rule if done by Company or the minimum necessary policies and procedures of the Company.

4. Obligations of the Company

Company shall:

(a) Notify Business Associate of any limitation(s) in its notice of privacy practices of Company in accordance with 45 CFR 164.520,

to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Company has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5. Permissible Requests by Company

Company shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule or Security Rule if done by Company.

6. Term and Termination

(a) Term: This Agreement shall be effective as of _____ **[Insert Effective Date]**, and shall terminate when all of the Protected Health Information provided by Company to Business Associate, or created or received by Business Associate on behalf of Company, is destroyed or returned to Company, or, if it is impractical to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause: Upon Company's knowledge of a material breach by Business Associate, Company shall either: (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and any related agreement if Business Associate does not cure the breach or end the violation within the time specified by Company; (2) Immediately terminate this Agreement and any related agreement entered into by the parties if Business Associate has breached a material term of this Agreement and cure is not possible; or (3) If neither termination nor cure are feasible, Company shall report the violation to the Secretary.

(c) Effect of Termination:

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Company, or created or received by Business Associate on behalf of Company. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is impractical, Business Associate shall provide to Company notification of the conditions that make return or destruction impractical. Upon providing notice that return or destruction of Protected Health Information is impractical, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction impractical, for so long as Business Associate maintains such Protected Health Information.

7. Miscellaneous

(a) Regulatory References: A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

(b) Amendment: The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Company to comply with the requirements of the HIPAA Privacy Rule or Security Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

(c) Survival: The respective rights and obligations of Business Associate under subsection 4(c) of this Agreement shall survive the termination of this Agreement.

(d) Interpretation: Any ambiguity in this Agreement shall be resolved to permit Company to comply with the HIPAA Privacy Rule or Security Rule.

8. Indemnification

Business Associate shall defend and indemnify the Company from and for any and all liability, claims, proceedings, suits, damages, or causes of action resulting in any way from

Business Associate's breach of this Agreement or breach of the HIPAA Privacy Rule or HIPAA Security Rule. The duty to indemnify shall include the duty to defend the Company by hiring competent legal counsel at Business Associate's expense.

The parties have caused this Agreement to be executed on the date first written above.

WinCo Foods, Inc.	**[Insert name of Business Associate]**
By:_____	By:_____
Its:_____	Its:_____

APPENDIX C

Security Training and Education Log

Security Training and Education Log

Date of Training	Name of Employee	Description of Training	Training Hours	Person/Company Providing Training

APPENDIX D

Company Resolutions

COMPANY RESOLUTION
ADOPTION OF HIPAA SECURITY MANUAL

WHEREAS, **WinCo Foods, Inc.** ("the Company") has authorized the preparation of a HIPAA Security Manual; and

WHEREAS, the Company has reviewed the Security Manual; and

WHEREAS, the Security Manual is intended to satisfy fully the requirements set forth in the federal HIPAA Security Rule;

NOW THEREFORE,

BE IT RESOLVED, that the Company hereby approves of the adoption of the HIPAA Security Manual, effective **October 1, 2013**, with the expectation that all Company employees, including those with an ownership interest in the Company, will be instructed in their respective duties under the Manual and will comply fully therewith.

Date:_____

By:_____
Valerie Davis

COMPANY RESOLUTION
APPOINTMENT OF A SECURITY OFFICER

WHEREAS, **WinCo Foods, Inc.** ("the Company"), having approved the adoption of the HIPAA Security Manual; and

WHEREAS, the Security Manual requires the appointment of a Security officer; and

WHEREAS, the Company having great confidence in the integrity, experience, and judgment of **Brian Garcia**;

NOW THEREFORE,

BE IT RESOLVED, that the Company does hereby appoint **Brian Garcia** to be the Security officer of the Company beginning **May 1, 2016**, and continuing until changed in accordance with the HIPAA Security Manual; and

BE IT FURTHER RESOLVED, that the Security officer will vigorously carry out the duties set forth in the Security Manual and that all applicable employees of the Company will be informed of the importance of adherence to the Security Manual and the importance of their cooperation with the Security officer.

Date:_____

By:_____
Valerie Davis

APPENDIX E

Security Incident Tracking Report

Security Incident Tracking Report

Date: _____

Time: _____

Description of Security Incident:

_____

_____

_____

_____

Measures Taken to Mitigate Effects and Resolve Problem:

_____

_____

_____

_____

Steps Taken to Prevent Recurrence:

_____

_____

_____

_____

Date of Plan Participant Notification (if required per Section B.10):_____

_____

Signature of Security Officer

APPENDIX F

Glossary of Terms

GLOSSARY OF TERMS

Access – The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

Administrative safeguards – Administrative safeguards are the policies and procedures the Company implements to execute the physical and technical safeguards. There are nine components of administrative safeguards in the Security Rule: (1) security management (includes performance of risk analysis, risk management, preparation of sanction policy and monitoring computer systems activities); (2) assignment of a security officer; (3) a system administrator; (4) management of the access of information; (5) security training; (6) incident reporting and investigation; (7) implementation of a contingency plan; (8) periodic evaluation of technology and upgrades; and (9) business associate agreements in place to protect ePHI.

Authentication – The corroboration that a person is the one claimed.

Availability – The property that data or information is accessible and useable upon demand by an authorized person.

Business associate – A person who on behalf of a covered entity performs, or assists in the performance of:

- A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, company management, and repricing; or
- Any other function or activity regulated by this subchapter; or
- A person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity (or to or for an organized health care arrangement in which the covered entity participates) where the provision of the service involves the disclosure of individually identifiable health information from such covered entity (or arrangement), or from another business associate of such covered entity (or arrangement), to the person.

Confidentiality – The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered entity – (1) A health plan (includes insurance companies, Medicare, Medicaid, group health plans, etc.); (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a standard HIPAA transaction (such as electronic billing).

Disclosure – Any release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

Electronic media – Includes memory devices in computers (hard drives) and any removable/transportable digital memory medium.

Electronic Protected Health Information (ePHI) – Individually identifiable health information transmitted by electronic media or maintained in electronic media.

Encryption – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility – The physical premises and interior and exterior of a building in which ePHI is located.

HHS or Secretary – The Department of Health and Human Services or the Secretary of Health and Human Services.

Health care – Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health plan – an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(a) A group health plan, as defined in this section.
(b) A health insurance issuer, as defined in this section.
(c) An HMO, as defined in this section.
(d) Part A or Part B of the Medicare program under title XVIII of the Act.
(e) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq*.
(f) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
(g) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
(h) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
(i) The health care program for active military personnel under title 10 of the United States Code.
(j) The veterans health care program under 38 U.S.C. chapter 17.
(k) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

(l) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*
(m) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*
(n) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*
(o) The Medicare + Choice Program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
(p) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
(q) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:
(a) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
(b) A government-funded program (other than those listed above, within this definition):
(i) Whose principal purpose is other than providing, or paying the cost of, health care; or
(ii) Whose principal activity is:
(A) The direct provision of health care to persons; or
(B) The making of grants to fund the direct provision of health care to persons.

Health care provider – A provider of services (as defined in Section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of protected health or health services (as defined in Section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information – Any information, oral or recorded in any medium, that:
- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information – Information that is a subset of health information, including demographic information collected from an individual, and that: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) Which identifies the individual, or (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Information system – An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity – The property that data or information have not been altered or destroyed in an authorized manner.

Minimum necessary – When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Payment – Any of a number of activities by a covered entity involving reimbursement or coverage related to health care or health benefits. The definition of payment includes: obtaining premiums or identifying or providing benefits under a health plan; reimbursement for health services, determining eligibility, coverage, adjudication, or subrogation of health benefit claims; risk adjusting amounts due based on enrollee health status and demographics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance and related health care data processing; review of health care services for protected health necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of certain protected health information relating to collection of premiums or reimbursement (i.e., name and address, date of birth, social security number; payment history; account number; and name and address of the health care provider and/or health plan).

Physical safeguards – Physical safeguards are the security measures that protect the physical facility and computer systems. There are four components of physical safeguards in the Security Rule: (1) facility access controls (locks, screen filters, magnetic cards); (2) workstation use; (3) workstation security; and (4) device and medical controls (disposal, reuse, accountability and backup storage).

Protected health information – Individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is (1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Protected health information excludes individually identifiable health information in employment records held by a covered entity in its role as an employer.

Required by law – A mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Security incident – A violation of security policies and procedures. A security incident includes the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with the operation of an information system. Examples: An unauthorized person accesses ePHI, a door is left unlocked, a hacker gets into the system. All security incidents must be documented.

Security officer – The individual designated by a health care provider to develop and implement security policies and procedures for the provider.

Technical safeguards – Technical safeguards and those electronic and computerized security measures installed (such as passwords) to protect information contained in the facility and computer system. There are five components of technical safeguards in the Security Rule: (1) access control (password encryption); (2) audit control; (3) integrity controls; (4) authorization; and (5) transmission security.

Treatment – The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a plan participant; or the referral of a plan participant for health care from one health care provider to another.

Use – With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation – An electronic computing device, such as a desktop or laptop computer, personal digital assistant (PDA) or other similar electronic device.

APPENDIX G

HIPAA Resources

HIPAA RESOURCES

Helpful General and Government Websites

Listed below are some valuable resources on the Internet that provide general information about HIPAA and the HIPAA Security Rule:

- CMS HIPAA Site: http://www.cms.hhs.gov/hipaa/hipaa2/default.asp
- HHS Administrative Simplification: http://aspe.hhs.gov/admnsimp/index.shtml
- HIPAAlert: http://www.hipaadvisory.com/alert
- SNIP: http://snip.wedi.org
- WEDI: http://www.wedi.org
- OCR website: http://www.hhs.gov/ocr/hipaa
- National Institute of Standards and Technology (NIST) website: http://csrc.nist.gov
- Utilization Review Accreditation Commission (URAC): http://www.urac.org

APPENDIX H

Acknowledgment of Receipt/Review of HIPAA Security Manual

EMPLOYEE ACKNOWLEDGMENT OF RECEIPT/REVIEW

OF

HIPAA SECURITY MANUAL

I, _____, acknowledge that I have received and/or reviewed the HIPAA Security Manual and that I will comply with its provisions. I acknowledge that failure to comply could result in disciplinary action, up to and including termination.

(print full name)

_____ _____

(Signature) (Date)

APPENDIX I

Plan Participant Notification of Unauthorized Disclosure

Plan Participant Notification

Dear _____:
(name of plan participant)

We regret to inform you that on _____[date]_____, 20___, we discovered an unauthorized disclosure of your protected health information, which occurred on _[date]_ _____, 20___. The following health information was disclosed:

[list]

The unauthorized disclosure happened as a result of [describe how disclosure occurred].

In order to protect yourself from potential further harm resulting from this disclosure, we recommend that you do the following: [Give recommendations.]

We are doing the following in order to mitigate the impact of this disclosure: [Explain]. In order to ensure that such disclosures do not happen in the future, we have [state corrective actions].

We sincerely apologize for this incident and hope it will not adversely impact you. If you have any questions or concerns, please contact Darin Risinger at 650 N. Armstrong Place, Boise, Idaho 83704 (208) 672-2137.

Very truly yours,

_____

NOTE: State law may require additional content to the notice beyond what is contained above.