

APPROVED: April 9, 2003
EFFECTIVE: April 21, 2003

SNOHOMISH COUNTY COUNCIL
Snohomish County, Washington

ORDINANCE NO. 03-035

AN ORDINANCE RELATING TO PRIVACY OF HEALTH INFORMATION
UNDER THE HEALTH INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT OF 1996 ("HIPAA") AND
ADOPTING CHAPTER 2.51A SCC

WHEREAS, in 1996, Congress adopted the Health Insurance Portability and Accountability Act (Pub. L. 104-191)("HIPAA") in order to improve the efficiency of the nation's health care system and protect the security and confidentiality of health information; and

WHEREAS, on August 14, 2002, the United States Department of Health and Human Services published final regulations implementing requirements relating to privacy of individually identifiable health information, set out at 45 C.F.R. 160 and 45 C.F.R. subpart E (collectively the "HIPAA privacy regulations"); and

WHEREAS, Snohomish County must comply with applicable requirements of the HIPAA privacy regulations no later than April 14, 2003; and

WHEREAS, on February 20, 2003, the United States Department of Health and Human Services published final regulations implementing requirements relating to security of electronic protected health information, set out at 45 C.F.R. 160 and 45 C.F.R. subpart C (collectively the "HIPAA security standards"); and

WHEREAS, Snohomish County must comply with applicable requirements of the HIPAA security standards no later than April 21, 2005; and

WHEREAS, Snohomish County desires to enact provisions necessary to implement the requirements under the HIPAA privacy regulations and HIPAA security standards;

NOW, THEREFORE, BE IT ORDAINED:

Section 1. A new chapter 2.51A is added to the Snohomish County Code to read:

Chapter 2.51A

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 COMPLIANCE

- 2.51A.010 Purpose.
- 2.51A.020 Definitions.
- 2.51A.030 Scope.
- 2.51A.040 Interpretation and construction of provisions.
- 2.51A.050 HIPAA privacy officer - appointment and responsibility.
- 2.51A.060 No retaliation.
- 2.51A.070 No waiver of rights.
- 2.51A.080 HIPAA security officer - appointment and responsibility.

2.51A.010 Purpose.

The purpose of this chapter is to ensure compliance with the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) and its implementing administrative regulations set forth in 45 C.F.R. parts 160-164.

2.51A.020 Definitions.

The following definitions shall apply to terms used in this chapter:

- (1) "Business associate" has the same meaning as that phrase is defined in 45 C.F.R. 160.103.
- (2) "Covered component" has the same meaning as the phrase "health care component" defined in 45 C.F.R. 164.103.
- (3) "Covered function" has the same meaning as that phrase is defined in 45 C.F.R. 164.103.
- (4) "Electronic protected health information" has the same meaning as that phrase is defined in 45 C.F.R. 160.103.
- (5) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191).
- (6) "HIPAA privacy regulations" means those regulations set out at 45 C.F.R. 160 and 45 C.F.R. subpart E.
- (7) "HIPAA security standards" means those regulations set out at 45 C.F.R. 160 and 45 C.F.R. subpart C.
- (8) "Hybrid entity" has the same meaning as that phrase is defined in 45 C.F.R. 164.103.
- (9) "Protected health information" has the same meaning as that phrase is defined in 45 C.F.R. 160.103.

2.51A.030 Scope.

Ordinance No. 03-035
Relating to Privacy of Health Information under
HIPAA and Adopting Chapter 2.51A SCC - 2

Snohomish County is a hybrid entity. This chapter shall apply to all county programs which perform health plan or health care provider activities that fall within the definition of a covered function.

2.51A.040. Interpretation and construction of provisions.

The rules and requirements set forth in this chapter shall be construed in favor of giving effect to the HIPAA privacy regulations and HIPAA security standards.

2.51A.050 HIPAA privacy officer - appointment and responsibility.

(1) The Director of Information Services shall be the county-wide HIPAA privacy officer.

(2) The HIPAA privacy officer shall:

(a) Develop, adopt with the approval of the county executive, and maintain HIPAA privacy policies and procedures to provide for:

(i) Training of county employees working within covered components, as necessary to carry out their respective functions, in accordance with 45 C.F.R. 164.530(b), and documentation of such training;

(ii) Ensuring appropriate administrative, technical and physical safeguards are in place to protect protected health information from unauthorized use or inadvertent disclosure to persons other than the intended recipient;

(iii) Assistance in identification of business associates;

(iv) Limitations on access to protected health information;

(v) Conditions for use and disclosure of protected health information;

(vi) Individual rights regarding protected health information maintained by the county;

(vii) A process for complaints concerning HIPAA policies and procedures, or covered components' compliance with HIPAA policies and procedures, or other requirements under the HIPAA privacy regulations;

(ix) Mitigation for any use or disclosure of protected health information that is in violation of the county's HIPAA privacy policies and procedures;

(x) Such policies and procedures necessary to comply with amendments or additions to the HIPAA privacy regulations.

(b) Establish, with the approval of the county executive, and publish sanctions for employees who fail to comply with the county's HIPAA privacy policies and procedures. Sanctions will be appropriate to the nature of the violation and will not apply to whistleblower activities, nor to complaints or investigations.

(c) Designate the county programs which are covered components using standards set out in the HIPAA privacy regulations, update the designations as necessary, and document the designations as provided in 45 C.F.R. 164.530(j).

2.51A.060 No retaliation.

No covered component or county employee may intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by the HIPAA privacy regulations, including the filing of a complaint or as otherwise prohibited under the HIPAA privacy regulations. The provisions of SCC 1.01.100 shall not apply to any violation under this section.

2.51A.070 No waiver of rights.

No covered component or county employee may require any individual to waive his or her right to file a complaint with the secretary of the United States Department of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits. The provisions of SCC 1.01.100 shall not apply to any violations under this section.

2.51A.080 HIPAA security officer - appointment and responsibility.

(1) The Director of Information Services shall be the county-wide HIPAA security officer.

(2) The HIPAA security officer must ensure the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained or transmitted by the county; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the HIPAA privacy regulations; and ensure compliance by the county's workforce. To accomplish these responsibilities, the HIPAA security officer shall:

(a) Develop, adopt with the approval of the county executive, and maintain HIPAA security policies and procedures:

(i) To prevent, detect, contain, and correct security violations;

(ii) To ensure that all members of the county workforce have appropriate access to electronic protected health information (including technical procedures);

(iii) To prevent access to electronic protected health information by those workforce members who do not have authority under the HIPAA privacy regulations (including technical procedures);

(iv) To address security incidents;

(v) To respond to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damage systems that contain electronic protected health information;

(vi) To create and maintain retrievable exact copies of electronic protected health information and to restore any loss of data;

(vii) To enable continuation of critical business processes for protection of security of electronic protected health information while operating in emergency mode;

(viii) To limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed;

(ix) That specify 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;

(x) That govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility;

(xi) To address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored;

(xii) For removal of electronic protected health information from electronic media before the media are made available for re-use;

(xiii) To protect electronic protected health information from improper alteration or destruction;

(xiv) To verify that a person or entity seeking access to electronic protected health information is the one claimed; and

(xv) Such policies and procedures necessary to comply with amendments or additions to the HIPAA security standards.

(b) Implement a security awareness and training program for all members of the county workforce (including management);

(c) Perform a periodic technical and nontechnical evaluation, based initially upon the HIPAA security standards and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which the county's security policies and procedures meet the requirements of the HIPAA security standards;

(d) Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users only;

(e) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information;

(f) Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network; and

(g) Establish, with the approval of the county executive, and publish the sanctions for employees who fail to comply with the county's HIPAA security policies and procedures. Sanctions will be appropriate to the nature of the violation and will not apply to whistleblower activities, nor to complaints or investigations.

PASSED this 9th day of April, 2003.

SNOHOMISH COUNTY COUNCIL
Snohomish County, Washington

ATTEST:

Gary Nelson
Chairperson

Barbara Sikorski
Asst. Clerk of the Council

(X) APPROVED
() EMERGENCY
() VETOED

DATE: 4/11/03

ATTEST:

Laura Nelson

Robert J. Drewel
County Executive

Approved as to form only:

Angela S. Belbeck 3/5/03
Deputy Prosecuting Attorney