

THE NONPROFIT HEALTH CARE CORPORATION REFORM ACT (EXCERPT)
Act 350 of 1980

550.1406 Confidentiality of records; disclosures; consent; policy regarding protection of privacy and confidentiality of personal data; violation as misdemeanor; penalty; civil action for damages; effect of section on governmental agencies; compliance with federal law and regulations; "health care operations" defined.

Sec. 406. (1) A health care corporation shall, in order to ensure the confidentiality of records containing personal data that may be associated with identifiable members, use reasonable care to secure these records from unauthorized access and to collect only personal data that are necessary for the proper review and payment of claims and for health care operations, treatment, and research. Except as is necessary to comply with section 603 or for the purpose of claims adjudication, claims verification, health care operations, treatment, research, payment, health oversight activities, or when required by law, a health care corporation shall not disclose records containing personal data that may be associated with an identifiable member, or personal information concerning a member, to a person other than the member, without the prior and specific informed consent of the member to whom the data or information pertains. The member's consent shall be in writing. Except when a disclosure is made to the commissioner or another governmental agency, a court, or any other governmental entity, a health care corporation shall make a disclosure for which prior and specific informed consent is not required upon the condition that the person to whom the disclosure is made protect and use the disclosed data or information only in the manner authorized by the corporation, pursuant to subsection (2). If a member has authorized the release of personal data to a specific person, a health care corporation shall make a disclosure to that person upon the condition that the person shall not release the data to a third person unless the member executes in writing another prior and specific informed consent authorizing the additional release. This subsection does not preclude the release of information to a member, pertaining to that member, by telephone, if the identity of the member is verified. This subsection does not preclude a representative of a subscriber group, upon request of a member of that subscriber group, or an elected official, upon request of a constituent, from assisting the individual in resolving a claim.

(2) The board of directors of a health care corporation shall establish and make public the policy of the corporation regarding the protection of the privacy of members and the confidentiality of personal data. The policy, at a minimum, shall do all of the following:

(a) Provide for the corporation's implementation of provisions in this act and other applicable laws respecting collection, security, use, release of, and access to personal data.

(b) Identify the routine uses of personal data by the corporation; prescribe the means by which members will be notified regarding those uses; and provide for notification regarding the actual release of personal data and information that may be identified with, or that concern, a member, upon specific request by that member. As used in this subdivision, "routine use" means the ordinary use or release of personal data compatible with the purpose for which the data were collected.

(c) Assure that no person shall have access to personal data except on the basis of a need to know.

(d) Establish the contractual or other conditions under which the corporation will release personal data.

(e) Provide that enrollment applications and claim forms developed by the corporation shall contain a member's consent to the release of data and information that is limited to the data and information necessary for the proper review and payment of claims, and shall reasonably notify members of their rights pursuant to the board's policy and applicable law.

(f) Provide that applicants for new or renewed certificates shall be advised that the corporation does not require the use of the applicant's federal social security account number and that, when applicable, another authority does require use of the number.

(3) A health care corporation that violates this section is guilty of a misdemeanor, punishable by a fine of not more than \$1,000.00 for each violation.

(4) A member may bring a civil action for damages against a health care corporation for a violation of this section and may recover actual damages or \$200.00, whichever is greater, together with reasonable attorneys' fees and costs.

(5) This section shall not be construed to limit access to records or to enlarge or diminish the investigative and examination powers of governmental agencies, as provided for by law.

(6) Compliance by a corporation with the health insurance portability and accountability act of 1996, Public Law 104-191, and regulations promulgated under that act, 45 CFR parts 160 and 164, satisfies subsections (1) and (2).

(7) As used in this section, "health care operations" means that term as defined in 45 CFR 164.501.

History: 1980, Act 350, Eff. Apr. 3, 1981;—Am. 2006, Act 218, Imd. Eff. June 26, 2006.

Popular name: Blue Cross-Blue Shield

Popular name: Act 350