

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Accretive Health, Inc.,
File No. 1223077

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Accretive Health Systems, Inc.

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Accretive Health enters into service agreements with hospital systems around the country to provide services related to the hospital systems' "revenue cycle" operations. Revenue cycle operations include registration, transcription, coding and medical documentation, billing, pricing, and collection of past due accounts. In exchange for these services, hospital systems pay Accretive Health both fixed fees and incentive payments based on a percentage of the monetary benefit from increased revenues. Accretive Health employees work at hospital facilities to assist with these services. As part of its service to client hospitals, Accretive Health collects, maintains, and has access to information about hospitals' patients, including sensitive health and personal information. This information may include patient names, dates of birth, billing information, diagnostic information, and Social Security numbers.

The Commission's complaint alleges that Accretive Health unfairly failed to provide reasonable and appropriate security for consumers' personal information it collected and maintained by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access. Among other things, Accretive Health created unnecessary risks of unauthorized access or theft of personal information by:

- a. Transporting laptops containing personal information in a manner that made them vulnerable to theft or other misappropriation;
- b. Failing to adequately restrict access to, or copying of, personal information based on an employee's need for information;
- c. Failing to ensure that employees removed information from their computers for which they no longer had a business need; and
- d. Using consumers' personal information in training sessions with employees and failing to ensure that the information was removed from employees' computers following the training.

The complaint further alleges that these failures contributed to a July 2011 incident in Minneapolis, Minnesota in which an Accretive Health laptop containing over 600 files with over 20 million pieces of information related to 23,000 patients was left in the locked passenger compartment of the employee's car and stolen. The laptop included sensitive health and personal information, including patient names, dates of birth, billing information, diagnostic information, and Social Security numbers. The user of this laptop had data that was not necessary to perform his job.

The proposed order contains provisions designed to prevent Accretive Health from engaging in the future in practices similar to those alleged in the complaint.

Part II of the proposed order requires Accretive Health to establish and maintain, or continue to maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Accretive Health's size and complexity, nature and scope of its activities, and the sensitivity of the information collected from or about consumers. Specifically, the proposed order requires Accretive Health to:

- designate an employee or employees to coordinate and be accountable for the information security program;
- identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;
- design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from Accretive Health, and require service providers by contract to implement and maintain appropriate safeguards; and
- evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to operations or business arrangement, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires Accretive Health to obtain within the first one hundred eighty (180) days after service of the order, and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of sensitive consumer, information has been protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Accretive Health to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, Accretive Health must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Accretive Health submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part VIII is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order or to modify the order’s terms in any way.