H.R. 5442, The Technologies for Restoring Users' Security and Trust (TRUST) in Health Information Act
Introduced by Rep. Markey (D-MA), Rep. Emanuel (D-IL) and Rep. Capps (D-CA)
Section-by-Section
February 14, 2008

TITLE I – HEALTH INFORMATION PRIVACY AND SECURITY

Sec. 100 Summary of privacy rights and security obligations

- Recognition of individual's right to health information privacy and security
- An opportunity to exercise that right through the mechanism of informed consent
- Employment, choice of health plan cannot be conditioned upon providing informed consent
- Individuals can inspect, copy, correct inaccuracies in their personal health information
- Particularly sensitive personal health information (e.g., mental health treatment, cancer, HIV/AIDS, domestic violence) can be segregated to limit access
- Notification of actual or suspected security breaches that exposes individuals' personal health information
- Audit trails of all electronic disclosures of an individual's personal health information provided upon request
- Individuals must receive written notification of the privacy practices of entities using or disclosing their personal health information
- Such entities must establish and maintain appropriate security safeguards to protect individuals' personal health information
- Entities must make publicly available on the Internet a list of data partners with which they have entered into contracts to provide services involving personal health information
- Entities must establish and update their risk management processes to protect against vulnerabilities to the privacy and security of individuals' personal health information
- Personal health information only can be used for marketing if explicit, specific, separate authorization provided

Subtitle A - Access to and Accuracy of Personal Health Information

Sec. 101 Inspection and copying of personal health information

- Individuals can inspect, copy, correct inaccuracies in their personal health information
- Entity using or disclosing personal health information establishes reasonable procedures; copying fees not to exceed actual copying costs
- Deadlines for complying with inspection and/or copying

Sec. 102 Modifications to personal health information

- Individuals can supplement, correct, amend, segregate or remove personal health information, subject to certain procedures and limitations

- Entity may refuse to modify the personal health information, in which case statement explaining the individual's disagreement with the refusal must be, at individual's request, included in subsequent disclosure of disputed information

Subtitle B – Security of Personal Health Information

Sec. 111 Notices of privacy practices

- Prepare written notice of security practices, including information that follows
- Right of individual to privacy, security, confidentiality of their personal health information
- Procedures for exercising consent to disclosures of personal health information and revoking consent
- Right to inspect and copy and modify own personal health information
- Right not to have employment, receipt of services, choice of health plan conditioned on execution of consent, subject to limitations
- Receipt of employment categories of those who have access to individual's personal health information
- Right to limit disclosures to certain categories
- Receipt of information about circumstances under which personal health information will be lawfully used or disclosed with the individual's consent
- Right to pay for health care services privately, thereby restricting disclosure of personal health information only to designated health care providers, subject to limitations
- Notification in the event of breach
- Right of individual to opt-out of any health information network or system
- Model notices developed and disseminated after notice and public comment

Sec. 112 Establishment of safeguards

- Establish and maintain appropriate administrative, technical and physical protections for safeguarding personal health information
- Employ an individual whose responsibilities include management of entity's information security
- Personal health information must be protected against any reasonably anticipated vulnerabilities
- Model guidelines developed and disseminated after notice and public comment

Sec. 113 Notification in case of breach

- Entities must, following discovery of a breach of personal health information, notify each individual whose information has been, or is reasonably believed to have been, acquired as a result of such breach
- Notifications made within 15 business days or earlier if determined appropriate by the HHS Secretary
- Methods of notice stipulated, including written, telephone, email, media and to the Secretary
- Content of notice described, including description of personal health information breached, toll-free number for individual to contact entity
- Entities that use, access, store, dispose of or collect personal health information but do not own or license it shall notify owner or licensee of the information following discovery of a breach
- Forms of notice specified, including written, telephone, email, and content of notification specified. HHS Secretary to be notified when health information of a significant number of individuals is breached
- Delay in notification permitted for law enforcement

Sec. 114 Transparency

- Entities using and disclosing health information must establish a public list of data partners with which they have entered into contracts involving health information; list available on the Internet
- If data partner overseas: U.S.-based entity liable for any violations, individual's whose personal health information involved must give informed consent before his/her health information offshored
- Secretary maintains a public list of entities that have lost, stolen, disclosed health information in an unauthorized manner in cases when 1,000 or more individuals' information involved; list available online at HHS Web site

Sec. 115 Risk management

- Entities create and update annual risk management processes to protect against unauthorized access to personal health information
- Risk management procedures must include means for detecting and recording unauthorized access, limiting physical access, ensuring secure disposal

Sec. 116 Accounting for disclosures and use

- Entities must establish and maintain a record of disclosure of each individual's personal health information
- Records maintained for not less than 6 years
- Individuals permitted to inspect and copy records of disclosures and use of their personal health information

Subtitle C – Use and Disclosure of Personal Health Information

Chapter 1 – General Restrictions

Sec. 121 General rules

- Entity may not disclose, access or use personal health information except as authorized under Title I
- Disclosure or use of personal health information that meets standards of being de-identified health information shall not be construed as a disclosure or use
- Disclosure shall be limited to minimum necessary to accomplish purpose (e.g., name and address, date of service, diagnosis, etc.)
- Before disclosure, access or use of individual's personal health information, individual must opt-in to participation in the health information network or system used by the entity
- Requirements to de-identify, destroy and expunge data to make it indecipherable upon disposal

Sec. 122 Informed consent for treatment and payment

- Employer, health plan, health or life insurer, or health care provider seeking to disclose personal health information for treatment or payment must obtain informed consent from individual. Single consent can be electronic and authorize multiple disclosures
- Informed consent defined - definition includes persons authorized to disclose information, means by which an individual may segregate sensitive information, nature and probability of harm to individual

resulting from authorization for use or disclosure, description of purpose of disclosures, description of extent to which authorize entity will share information with subcontractors, including those overseas

- Limitations include entity's right to require self-pay if individual refuses to consent for billing purposes and health care provider's right to withhold treatment if individual refuses to consent for treatment under certain circumstances - disclosure needed so as not to threaten individual's health and withholding treatment is not life-threatening to individual
- Entities must comply with individual's request to hide, mask or mark separate any type or amount of personal health information held by the entities
- Informed consent can be revoked by individual, subject to limitations
- Record of informed consents and revocations for treatment and payment must be maintained by entities for 6 years
- Model informed consent developed and disseminated after notice and public comment

Sec. 123 Informed consent and authorization for disclosure of personal health information other than for treatment and payment

- Informed consent required for disclosure for purpose other than treatment and payment
- Delivery of treatment, payment of services cannot be conditioned upon receipt of informed consent or authorization described in this section
- No disclosure of personal health information to employees or agents responsible for making employment or personnel decisions without a separate authorization from the individual
- Separate authorization for marketing, with marketing definition consistent with December 2000 Final HIPAA Privacy Rule
- Disclosure of personal health information without informed consent permitted under certain circumstances (e.g., release to coroners and medical examiners)
- Consents and authorizations may be revoked
- Records of consents, authorizations and revocations must be retained for 6 years
- Model informed consents and authorizations developed and disseminated after notice and public comment

Chapter 2 – Exceptions

Sec. 131 Disclosure for law enforcement, national security and intelligence purposes

- Disclosure without informed consent permitted to law enforcement authorities pursuant to a warrant, the National Security Act
- Limitations include prohibition on use of such personal health information under this section for other purposes
- Destruction or return of information required after disclosure

Sec. 132 Disclosure for public health purposes

- Disclosure without informed consent permitted to public health authority when disclosure relates directly to specified public health purpose, is reasonably likely to achieve such purpose, and cannot be achieved using de-identified information
- For such disclosure without consent, it must be of significant importance that it outweighs privacy impact on individual

Sec. 133 Reporting of abuse and neglect to protection and advocacy agencies

- Entity may disclose personal health information to a protection and advocacy agency without individual's consent when there is probable cause to believe that individual is vulnerable to abuse and neglect

Sec. 134 Disclosure to next of kin and directory information

- Disclosure to next of kin about health care services provided is permitted without informed consent if individual has been informed of right to object and has not objected, information is relevant to care currently being provided to individual
- Information for inpatient health care facility's directory contains name of individual, general health status and location of individual in health care facility where individual being treated
- No disclosure if entity believes directory information would lead to physical or mental harm to individual, unless individual expressly authorizes the disclosure

Chapter 3 – Special Circumstances

Sec. 141 Emergency circumstances

- Disclosure without informed consent permitted in event of: threat of imminent harm to individual; threat of serious injury or death to another when individual has ability to carry out such threat and disclosure is necessary to prevent or significantly reduce the possibility of the threat being carried out

Sec. 142 Health research

- Not later than 24 months after enactment, HHS Secretary shall prepare and submit to Congress detailed recommendations on whether informed consent should be required, and if so, under what circumstances, before personal health information can be used for health research

- Recommendations that must be submitted include a list of all known breaches of health information privacy over the past 5 years in research projects approved by an institutional review boards and a summary of how technology that both facilitates research and preserves privacy could be used to obtain informed consent and remove identifying data for the purpose of research

Sec. 143 Health oversight functions

- Disclosure to a health oversight agency without informed consent to enable agency to perform a health oversight function authorized by law under certain limited circumstances, including the purpose for disclosure cannot be accomplished without using personal health information
- Health oversight agency that receives personal health information shall, to the maximum extent practicable, obtain the informed consent of the individual to whom the personal health information relates before using or disclosing it; secure personal health information in all work papers and documents

Sec. 144 Individual representatives

- Individual authorized by law to act as an agent, attorney, et al. may discharge rights of an individual relating to health information under this Title.
- Rights of minors described – for individuals who are 18 or older, all rights under this title shall be exercised by the individual; or for individuals who are legally capable and can consent to health care without violating any applicable law, the individual shall exercise all rights under this title
- For individuals under 14, all of the individual's rights shall be exercised by the parent or legal guardian; for individuals between 14 and 17 years-old, the rights of inspection, supplementation and modification and the right to authorize use and disclosure of personal health information shall be exercised by the individual where no parent or legal guardian exists, by the parent or the legal guardian when one exists, or by the individual if the parent or legal guardian determined that the individual has the sole right to control the health information

Subtitle D – Enforcement

Sec. 151 In general

- Civil and criminal penalties for violations of this title.
- An individual whose rights under subtitle A, B, or C have been knowingly and negligently violated may bring a civil action to recover relief as determined appropriate by a court
- In case in which violations occurred with such frequency as to constitute a general business practice, a civil penalty of not more than $100,000.

Sec. 152 Enforcement by state attorneys general

- State or local law enforcement agency may bring a civil action on behalf of residents of state or jurisdiction
- Civil penalties calculated by multiplying the number of violations by an amount not greater than $11,000
- Each day that a person is in violation of the requirements of subtitle A, B, or C is treated as a separate violation, up to a maximum civil penalty of $5,000,000

Subtitle E – Miscellaneous

Sec. 161 Office of Health Information Privacy

- Creation of Office of Health Information Privacy within HHS
- Director of the Office to receive and investigate complaints of alleged violations of this Title; conduct audits when appropriate; provide guidance to HHS Secretary on implementation of this Title.
- Not later than 12 months after enactment, Director to establish standards for health information products that protect individual's privacy, security, and confidentiality
- In establishing standards, Secretary shall ensure involvement of stakeholders
- Director shall submit to Congress annual reports on the number of complaints received of alleged violations of Title I; report shall contain any remedial action taken by HHS and be available on HHS Web site.

Sec. 162 Protection for whistleblowers

- Discrimination and retaliation against whistleblowers prohibited
- Compensatory damages described

Sec. 163 Demonstration grant for individuals with limited English language proficiency or limited health literacy

- HHS grants to improve communication of information pertaining to health privacy to individuals with limited English proficiency and health literacy

Sec. 164 Relationship to other laws

- No pre-emption of stronger Federal or state laws relating to personal health information or relating to an individual's access to personal health information
- Nothing in the Act preempts, supercedes or modifies the operation of any state law that governs a minor's rights to access personal health information or health care services; regulates the disclosure or reporting of information concerning an individual's mental health; or requires the reporting of abuse or neglect about any individual; and provides for the reporting of vital statistics such as birth or death information
- HIPAA remains in effect to extent that it is consistent with Title I; HHS Secretary to initiate rulemaking to amend any Federal regulations as required such that they are consistent with Title I.

Sec. 165 Effective date

- Either 30 months after enactment or 12 months after promulgation of regulations (which occurs 12 months after enactment), whichever is earlier.

Subtitle F – Definitions

TITLE II – Promotion of Health Information Technology

Subtitle A – Improving the Interoperability of Health Information Technology

Sec. 201 Office of the National Coordinator of Health Information Technology

- Classifies the position of the National Coordinator of HIT, which will be appointed by and report directly to the Secretary of HHS
- Calls for Coordinator to coordinate HIT initiatives across HHS and other relevant federal agencies, serve on both the American Health Information Community (AHIC) and the Partnership for Health Care Improvement ("Partnership") and act as a liaison between the AHIC, Partnership, and the federal government
- Requires the Office of the National Coordinator to:
    - develop and publish a strategic plan for implementing a nationwide interoperable health infrastructure
    - maintain and update a website with information related to standards and use cases, AHIC/Partnership recommendations, quality measures, funding, and post-sunset transition plans
    - report on major public and private HIT systems
    - assess the impact of HIT in communities with health disparities and identify best practices to increase the adoption of HIT by providers in those communities.
- Authorizes such sums as necessary for fiscal years 2009 and 2010 and sunsets the Office of the National Coordinator (ONC) and the position of the National Coordinator on September 30, 2014.

Sec. 202 Partnership for Health Care Improvement

- Establishes the public-private Partnership to advise the Secretary and the nation on specific actions to achieve a nationwide interoperable HIT infrastructure
- Makes recommendations on standards, implementation specifications, and certification criteria for adoption by the federal government.
- Serves as forum for participation from a diverse range of stakeholder groups with specific technical expertise in standards development, implementation specifications, and certification criteria.
- Requires the Partnership to develop and maintain a website that outlines governance rules, a business plan, meeting information, and a process for public comment
- Sets forth guidelines for appointing members to the Partnership, specifically requiring participation from outside groups, including those with expertise in: health information privacy, health information security, health care quality and patient safety, medical and clinical research data exchange, developing HIT standards and new HIT. Instructs the Partnership to take into account the recommendations of the AHIC in carrying out its duties.
- Standards and Implementation Requirements:
    - Requires the Partnership within 90 days to develop and publish in the Federal Register and on the HHS website an annual assessment schedule for standards and implementation specifications.
    - Within one year after enactment, the Partnership will recommend to the Secretary and publish in the Federal Register and on the ONC website any standards and implementation specifications to be reviewed by the Secretary, HHS, VA, DoD, and other agencies.

- The Partnership, in consultation with the Secretary, may designate one or more private entities to develop and recommend standards and implementation specifications. The Secretary, or a recognized private entity, may also conduct pilot projects to test the standards and implementation specifications.
- If appropriate and approved, the President will provide for federal adoption of proposed for federal adoption of proposed recommendations – provided they are consistent with HIPAA – to be published in the Federal Register and ONC website within 30 days of interagency review.

- Certification:
  - The Partnership, in consultation with the Secretary, may designate one or more private entities to develop certification criteria to certify that HIT products are in compliance with adopted standards.
  - The criteria for certification of HIT products will be reviewed, and possibly adopted by the Secretary, based on Partnership recommendations.
  - A third party may also be designated by the Secretary to carry out certification responsibilities.
  - Mandates that nothing in the section should disrupt certification and standards development activities. Authorizes appropriation of $2,000,000 for each of the fiscal years 2009 and 2010.

Sec. 203 American Health Information Community Policies

- Establishes the public-private American Health Information Community (AHIC) to serve as a broad discussion forum for stakeholders to:
  - improve HIT adoption and implementation;
  - advise the Secretary and other department heads on policy considerations related to HIT;
  - to make annual recommendations related to a policy framework for and national adoption of nationwide interoperable HIT infrastructure.
- The policy recommendations will encompass privacy and security protections, consumer education, appropriate uses of health information, and chronic disease management. The recommendations will be published on the ONC website and in the Federal Register. The Secretary will determine which recommendations will be endorsed by the federal government.
- Sets forth guidelines for appointing AHIC members to 3-year terms and requires the membership to designate a Chairperson and Vice Chairperson.
- Allows for detailees from other federal agencies and provides for participation in the AHIC by outside groups, including those with expertise in health information privacy and security, health information security, health care quality and patient safety, medical ethics, medical and clinical research data exchange, and developting HIT standards and new HIT.
- Applies the Federal Advisory Committee Act to the AHIC for 7 years, sunsets the section on September 20, 2014. Authorizes $2,000,000 for fiscal years 2008 and 2009.

Sec. 204 Research Access to Health Care Data and Reporting on Performance

- Researchers who meet the Secretary's criteria will be permitted access to all federal health care data and can report on the performance of providers and suppliers in an identifiable format.

Subtitle B—Facilitating the Widespread Adoption of Interoperable Health Information Technology

Sec.211 Facilitating the Widespread Adoption of Interoperable Health Information Technology

- Competitive Grants for Adoption of Technology:
  - The Secretary may provide grants to eligible entities to facilitate purchase and enhance utilization of qualified HIT systems
  - Outlines eligibility fro grants including requirements for strategic plans, adoption of voluntary federal standards, implementation of adopted quality measures, agreement to notify patients of wrongful disclosure of their individually identifiable health information, consideration of input by healthcare providers' employees on implementation and use of HIT systems, significant financial need, and a matching provision of $1 to $3 of Federal funds provided under the grant.
- Competitive Grants for Development of State Loan Programs:
  - The Secretary may give grants to States to establish loan programs for health care providers, provided the state has established a qualified HIT loan fund. Grant dollars for the state loans will be deposited directly into the loan fund. Outlines eligibility requirements for state receiving grants and requires the establishment of state loan funds and annual state strategic plans. Requires providers receiving funds by way of the grant-enabled loan fund to meet certain mandates related to interoperability, privacy/security and others. Describes the types of assistance the state loan funds may provide and provides limitations on the cost of administering. Allows for private sector contributions and imposes a matching requirement of $1 to $1 in federal funds. Authorizes the Secretary to give a preference in awarding state loan grants to states that adopt value-based purchasing programs.
- Competitive Grants for the Implementation of Regional or Local HIT Plans:
  - The Secretary may give grants to entities to implement regional or local health information plans, pursuant to standards, implementation specifications and certification criteria, and other requirements adopted by the Secretary.
  - Outlines the eligibility requirements for entities, including financial need, a governance structure with participation from specific sectors of the health care community, adoption of nondiscrimination and conflict of interest policies, adoption of federally-adopted HIT standards, adoption of quality measures, and implementation of policies to notify patients if health information is wrongfully disclosed
  - Requires applicants to submit an application to the Secretary that outlines specific objectives, strategies, and plans for improving health care quality through standards adoption, quality measures, privacy/security practices, sound governance and financial plans, and the promotion of HIT use by providers.
  - Requires a match of $1 to $2 in federal funds – non-federal contributions can be in the form of cash or in kind, including equipment, technology or services. Outlines the manner in which the grant money may be used and requires an annual report to the Secretary outlining the specific benchmarks. Authorizes $139 million for FY09, $139 million for FY10, and such sums as necessary through 2012.

Sec. 212 Demonstration Program to Integrate Information Technology Into Clinical Education

- The Secretary may give competitive grants, pursuant to peer review to entities or consortia to carry out demonstration projects to develop academic curricula integrating HIT systems in clinical education or analyze clinical data to discover quality measures for improved clinical outcomes.
- Outlines eligibility requirements and identifies entities that may apply. Limits the use of funding to collaboration between 2 or more disciplines – prohibits purchase of the hardware, software, or services.
- Requires matching funding of $1 to $2 in federal funds.
- The Secretary will provide for evaluation of the projects, distribute the findings and report to Congress with one year. Authorizes $2,000,000 for each of fiscal years 2009 and 2010. All funds will be made available through September 30, 2012.

Sec. 213 Qualified Health Information System Defined

- System defined as computerized system (including hardware and software) that safeguards privacy, security, and confidentiality of personal health information in accordance with the requirements of Title I, maintains and provides permitted access to health information in an electronic format, preserves and audit trail, incorporates decision support to reduce medical errors and enhance health care quality, complies with Federal government standards under section 202, has the ability to transmit and exchange information among various entities and allows for reporting of quality measures under section 221.

Subtitle C—Improving the Quality of Health Care

Sec. 221 Fostering Development and use of Health Care Quality Measures

- The Secretary will provide for the development of quality measures to evaluate quality and efficiency by designating an arrangement with a single organization to provide advice and recommendations on priorities, within 90 days of enactment. The designated organization, which will need 7 years of experience, will be responsible for developing an integrated national strategy for establishing quality measures; coordinating/harmonizing the development and testing of quality measures; establish standards for the development and testing of quality measures; endorsing national consensus quality measures; recommending quality measures to the Secretary for adoption and use; promoting the development and use of electronic health records with automated collection, aggregation and transmission of quality measures; and providing recommendations to the Partnership (on integration of quality measures into certification process) and AHIC (on national policies).
- The organization will be a private, non-profit entity, governed by a Board of Directors with a President/CEO. Sets forth guidelines for membership on the governing Board of Directors with respect to sector representatives and fields of experience. The designated organization's activities will be open and transparent, providing opportunity for public comment, and will operate as a voluntary consensus standards setting organization.
- Establishes requirements for development and annual update of quality measures, including ensuring they are evidence-based, reliable, and valid. The Secretary may award grants through AHRQ to support the development and testing of quality measures – the grants may not exceed $50,000 each.

Sec. 222 Adoption and Use of Quality Measures; Reporting

- In order to ensure use and uniformity of private entity quality measures, the Secretary will adopt quality measures recommended by multi-stakeholder organizations and endorsed by the designated quality measures organization, and ensure standards adopted for federal purchasing and data collection integrate the adopted quality measures and do not conflict with SSA programs.
- The Secretary will enable HHS to accept electronic data submissions for the purposes of performance measurement. After consulting with multi-stakeholder groups, the Secretary will promulgate regulations to ensure comparative performance information is available to all appropriate individuals and entities.

Subtitle D – Miscellaneous Provisions

Sec. 231 Health Information Technology Resource Center

- Requires the Secretary to develop a HIT Resource Center (Center) to provide technical assistance and develop best practices to support and accelerate efforts to adopt, implement, and effectively use interoperable health information technology. Among other functions, the Center will serve as a forum for the exchange of knowledge and experience, provide for the establishment of regional and local health information networks, help develop and share best practices.
- To support Center activities and facilitate health information exchange across public and private sectors, the Director can modify the requirements of AHRQ's National Resource Center for HIT to provide necessary infrastructure to the HIT Resource Center. Authorizes such sums as necessary for the establishment of the Center for FY 2009-2010.

Sec. 232 Facilitating the Provision of Telehealth Services Across State Lines

- Amends the PSA to Sec. 330L Telemedicine; Incentive Grants Regarding Coordination Among States:
    - The Secretary can award grants to States that have adopted regional State licensure reciprocity agreements to expedite telemedicine across state lines. The bill authorizes the appropriation of such sums necessary for the grants in FY 2009-1010

Subtitle E - Definitions

TITLE III – ADDITIONAL PROVISIONS

Sec. 301 Federal Purchasing and Data Collection by CMS and other Federal agencies

- Coordination of Federal Spending:
  - Not later than one year following adoption of standards by the President, federal agencies will not be allowed to expend federal funds for the purchase of any new HIT or HIT system for clinical care or for the electronic retrieval, storage, or exchange of health information if the HIT is not consistent with applicable standards adopted by the federal government. This does not restrict the purchase of minor hardware/software to modify, correct deficiencies in, or extend existing components.
- Voluntary Adoption:
  - Federally-adopted standards and implementation specifications are voluntary for private entities, but any private entities that enter into federal contracts must adopt the standards used by the federal government for the purposes of the contract.
- Coordination of Federal Data Collection:

Within 3 years of adoption of data collection standards and implementation specifications, all agencies collecting data in electronic format for quality reporting, surveillance, epidemiology, adverse event reporting, research, etc., will need to comply with those standards.

- Not later than 1 year after the adoption of a recommendation for health IT standards, the Administrator of CMS and the head of any other Federal agency shall not expend Federal funds for the purchase of any new health information technology or health information technology system that is not consistent with applicable standards adopted by the Federal government
- Standards are voluntary for private entities, except that private entities that enter into a contract with the Federal Government shall adopt the standards and implementation specifications adopted by the Federal Government under this section for the purpose of activities under such contract.
- Not later than 3 years after the adoption by the Federal Government of a recommendation, all Federal agencies (including CMS) collecting health data in an electronic format for the purposes of quality reporting, surveillance, epidemiology, adverse event reporting, research, or for other purposes determined appropriate by the Secretary shall comply with the standards and implementation specifications adopted.
- Amends the Social Security Act so that any provider of services or supplier shall be deemed as meeting any requirement for the maintenance of data in paper form under this title if the required data is maintained in an electronic form.