2013

It is OK to be a Copycat: Why the Department of Health and Human Services should look to the SEC's Consolidated Audit Trail for Health Information Exchange

Stephen Bauer

It is OK to be a Copycat: Why the Department of Health and Human Services should look to the SEC's Consolidated Audit Trail for Health Information Exchange

The Health Information Technology for Economic and Clinical Health (HITECH), of the American Recovery and Reinvestment Act of 2009 (ARRA), was passed to increase individuals' rights pertaining to the security of their medical records, motivate the transition to electronic health records (EHRs), and trigger a massive expansion in the exchange of electronic protected health information (PHI). The switch from paper records to EHRs will allow for easier access to patient information. While this will have substantial benefits for health care quality and efficiency, it must have security procedures to prevent personal information from being violated.[1] A curious nurse or doctor[2] having confidential information at their fingertips can have massive consequences.[3] To help prevent these harms, HITECH amended the HIPAA Privacy Rule and expanded coverage of Accountings of Disclosures.

HITECH also mandates the Office of the National Coordinator for Health Information Technology (ONC-HIT) undertake activities consistent with the development of a nationwide health IT infrastructure, allowing for electronic use and

[1] Beth Israel Deaconess Medical Center had more than 2,000 patients personal information may have been stolen from a hospital computer because a computer service vendor had failed to restore proper security settings on a computer after performing maintenance on it. The machine was later found to be infected with a virus, which transmitted data files to an unknown location. The computer contained medical record numbers, names, genders, and birthdates of 2,021 patients, as well as the names and dates of radiology procedures they had undergone. Bray, Hiawatha, Beth Israel Data Breach May Affect Over 2,000, Boston.com, (November 28, 2008), http://www.boston.com/business/technology/articles/2011/07/19/beth_israel_data_breach_may_affect_over_2000/.

[2] "More than two dozen employees at Palisades Medical Center have been suspended after accessing the personal medical records of actor George Clooney, who was taken to the North Bergen, N.J., hospital last month after a motorcycle accident." CNN Entertainment, 27 Suspended for Clooney File Peek, (October 10, 2007), http://www.cnn.com/2007/SHOWBIZ/10/10/clooney.records/index.html.

[3] Over the past three years, over 21 million patients have had their medical records exposed in data security breaches reported to the federal government. U.S. Department of Health and Human Services (HHS) must post a list of breaches of unsecured protected health information affecting 500 or more individuals, as required by section 13402(e)(4) of the HITECH Act. Currently, the displays 498 of these mass breaches.[3]U.S. Department of Health and Human Services, Health Information Services, Breaches Affecting 500 Patients or More, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html, (last visited Nov. 11, 2012).

exchange of secure health information.[4] The Nationwide Health Information Network (NHIN) is health care's current exchange. NHIN is struggling in terms of growth and participation, and the plans for the immediate future raise concerns. While guidelines and security procedures for health information exchange are being determined, ONC-HIT would be wise to look at the SEC's Consolidated Audit Trail (CAT). While there are economic and pragmatic obstacles, improved medical quality and safety justify the means. CAT has laid a solid foundation for secure information exchange using unique identifiers and central, uniform oversight structure to maximize efficiency and security. Meaningful use of EHRs[5] and the amended accounting of disclosures establish a solid foundation for audit trials. Extending these procedures towards interoperability and adopting certain aspects from CAT will create a secure, efficient nationwide exchange for health information.

HIPPA Privacy Rule

While most of our medical records do not draw much attention as George Clooney's, our personal health information does not need to be someone's entertainment or leverage. Hospitals and medical health providers can place internal policies and supervise them as closely as possible, but human oversight cannot fully control an individual's curiosity or error. The *Standards for Privacy of Individually Identifiable Health Information* (Privacy Rule[6]) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule standards address the proper uses and disclosures of individuals' protected health information as well as outline individuals' rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (OCR) has

[4] The Office of the National Coordinator for Health Information Technology, HealthIT.gov, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200, (last visited Nov. 10, 2012).
[5] Meaningful Use, HealthIT.gov, http://www.healthit.gov/policy-researchers-implementers/meaningful-use (last visited Nov. 20, 2012).
[6] 45 C.F.R. § 164.528 (2012).

responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.[7]

HITECH Overview

HITECH requires HHS to adopt an initial set of standards, implementation specifications, and certification criteria for EHR technology.[8] To achieve these goals, HITECH amended the HIPPA Privacy Rule to provide for more expansive and detailed coverage regarding accountings of disclosures. HITECH provides incentive payments to medical professionals for meaningful use of electronic health records.[9] These EHR Incentive Programs will provide incentive payments to covered entities[10] as they demonstrate adoption, implementation, upgrading, or meaningful use of certified EHR technology.[11] EHR incentive programs are designed to support providers in this period of health IT transition and instill the use of EHRs in meaningful ways to help our nation to improve the quality, safety, and efficiency of patient health care.[12] The security and privacy of these records is the key to health IT success.

A covered entity may not use, disclose, or sell[13] a patient's medical health information, except under limited circumstances.[14] [15]However, when it is proper to use or

[7] U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule, OCR Privacy Brief, at 1.
[8] 45 C.F.R. § 171 (2012).
[9] American Recovery and Reinvestment Act of 2009, Division A, Title XII- Health Information Technology § 134000, The HITECH Act defines an electronic health record (EHR) as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." [hereinafter HITECH].
[10] 45 C.F.R. § 160.103 (2012). (1) Defines "covered entity" as: (1) a health plan; (2) A health care clearinghouse; or (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
[11] Welcome to the Medicare & Medicaid EHR Incentive Program Registration & Attestation System, https://ehrincentives.cms.gov/hitech/login.action, (last visited Oct. 28, 2012).
[12] Welcome to the Medicare & Medicaid EHR Incentive Program Registration & Attestation System, https://ehrincentives.cms.gov/hitech/login.action, (last visited Oct. 28, 2012).
[13] HITECH § 13405(d)(1). A covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization that includes, in accordance with such section, a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual.
[14] 45 C.F.R. § 164.502(a)(1)(ii-vi). (ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506; (iii) Incident to a use or disclosure otherwise

disclose protected health information, a covered entity must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[16] Restricting the information to the minimum necessary reduces the chance of exposing a patient's medical health information. By exchanging only data that concerns the immediate matter at hand, the remaining information stays isolated from potential privacy breaches.

Individual EHR Privacy

Accounting of Disclosures Under HIPAA Privacy Rule (Pre-HITECH)

An individual has a right to adequate notice of 1) the uses and disclosures of protected health information that may be made by the covered entity; 2) the individual's rights regarding these uses and disclosures; and 3) the covered entity's legal duties with respect to protected health information.[17] The covered entity must provide notice in plain

---

permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §164.502(b), §164.514(d), and §164.530(c) with respect to such otherwise permitted or required use or disclosure; (iv) Pursuant to and in compliance with a valid authorization under §164.508; (v) Pursuant to an agreement under, or as otherwise permitted by, §164.510; and (vi) As permitted by and in compliance with this section, §164.512, or §164.514(e), (f), or (g).

[15] HITECH § 13405(d)(2). Exception to the Sale of Electronic Health Records or Personal Health Information (A) The purpose of the exchange is for public health activities (as described in section 164.512(b) of title 45, Code of Federal Regulations). (B) The purpose of the exchange is for research (as described in sections 164.501 and 164.512(i) of title 45, Code of Federal Regulations) and the price charged reflects the costs of preparation and transmittal of the data for such purpose. (C) The purpose of the exchange is for the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent protected health information from inappropriate access, use, or disclosure. (D) The purpose of the exchange is the health care operation specifically described in subparagraph (iv) of paragraph (6) of the definition of healthcare operations in section 164.501 of title 45, Code of Federal Regulations. (E) The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement. (F) The purpose of the exchange is to provide an individual with a copy of the individual's protected health information pursuant to section 164.524 of title 45, Code of Federal Regulations. (G) The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the exceptions provided in subparagraphs (A) through (F).

[16] 45 C.F.R. § 164.502(b)(1).

[17] 45 C.F.R. § 164.520(a)(1).

language that prominently displays a reminder of the patient's right to access information regarding how their medical information is used and disclosed.[18]

HIPPA requires covered entities to make available an accounting of certain disclosures of an individual's protected health information to him or her upon request.[19] A disclosure is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."[20] Each disclosure must include: the date of the disclosure; the name and address, if known, of the entity or person who received the protected health information; a brief description of the information disclosed; and a brief statement of the purpose of the disclosure or a copy of the written request for the disclosure.[21] Patients have the right to a disclosure every twelve months.[22] Allowing patients to understand who is looking at their personal health information serves as a secondary form of oversight against misuse or breach of privacy, along with federal regulation.

HITECH modified the Privacy Rule for accountings of disclosures and the Breach of Notification Rule relating to EHRs.[23] While the right to a disclosure remains, the content within these reports has changed due to the prevalence and integration of technology. Before HITECH, a covered entity provided a list of research protocols rather than specific information about each disclosure.[24] An individual who requested an accounting of disclosures received a list of research protocols with information about

---

[18] 45 C.F.R. § 164.520(b)(1)(i,ii).
[19] 45 C.F.R. § 164.528(a)(1).
[20] 45 C.F.R. § 160.103.
[21] 45 C.F.R. § 160.528(b)(i-iv).
[22] 45 C.F.R. § 160.528(c)(2).
[23] 45 C.F.R. § 164.528(a)(1)(i-ix). [HIPPA Privacy Rule before HITECH] provides that an accounting must include all disclosures of protected health information, except for disclosures: To carry out treatment, payment and health care operations as provided in § 164.506; To individuals of protected health information about them as provided in § 164.502; Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502; Pursuant to an authorization as provided in § 164.508; For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510; For national security or intelligence purposes as provided in § 164.512(k)(2); To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); As part of a limited data set in accordance with § 164.514(e); or That occurred prior to the compliance date for the covered entity.
[24] HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act, 45 C.F.R. §164, (proposed May 31, 2011)(*referencing* HIPPA Privacy Rule §164.528(b)(4) before HITECH).

each protocol, including contact information, rather than specific information about disclosures for research.[25] Organizing and sending these old-form accountings of disclosures was a burden on health care providers. The data had to be compiled from the paper record, digitized or copied, then sent to the patient. This bundled information was additional labor and time that encumbered most health care providers. Miscommunication and misunderstanding regarding what information was required in these accountings added to the confusion.

Accounting of Disclosures under HITECH

Health care professionals collect a baseline of patient information to meet the first stage of meaningful use of EHRs. Certified EHR technology must have the capability to record the date, time, patient identification, user identification, along with a description of the disclosure, for disclosure made for treatment, payment, and health care operations.[26] With this information readily available in electronic format, as amended under HITECH, the HIPAA §164.528(a)(1)(i) exemption for disclosures- to carry out treatment, payment, and health care operations (TPO)- no longer applies to disclosure through an electronic health record.[27] Meaningfully using certified EHR technology eliminates the additional workload warranting this exemption.

To ease the burden and the confusion on medical health providers, HITECH bifurcated accountings into Accounting of Disclosures and Access Reports.[28] Access reports detail individuals who have accessed electronic protected health information in a designated record set, including access for purposes of treatment, payment, and health care operations.[29] An access report includes each person that has accessed the patient's EHRs, along with the date, time, and module or location of disclosure.[30] This information is already required to be collected for meaningful use of electronic health records.[31] Choosing a short-form access report allows patients to view their medical disclosure

[25] 45 C.F.R. § 164. (*referencing* HIPPA Privacy Rule §164.528(b)(4) before HITECH).
[26] 45 C.F.R. § 170.210, 302 (*citing* 75 Fed. Reg. 2014, 2044, 2046).
[27] 45 C.F.R. § 164.
[28] HITECH **§** 13405(c)(3).
[29] 45 C.F.R. § 164.
[30] *Id.*
[31] *Id.*

history while alleviating the burden on a majority of these requests. In essence, an access report is a summary of the meaningful use of a patient's EHR for his or her viewing.

Patients may also request an accounting of disclosures. An accounting of disclosures is more detailed and burdensome, as the medical provider would have to fill out three years of extra information. Accountings include everything in an access report as well as additional information about the disclosures by persons outside the covered entity and its business associations.[32] The current accounting provision applies to disclosures of paper and electronic protected health information, regardless of whether such information is in a designated record set.[33] Accountings also require a description of the intent behind the access, i.e. why the nurse looked at the file. Accountings of disclosures give the patient a deeper explanation to who saw the patient's files and why. All covered entities *and business associates*[34]- not just those covered by health care providers who maintain personal health information in an EHR- will be subject to the requirement to provide accountings.[35] By adding business associates, there is

---

[32] *Id.*

[33] *Id.*

[34] 45 C.F.R. § 160.103. (1) Except as provided in paragraph (2) of this definition, "business associate" means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) 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, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), 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. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity. (45 CFR 160.103)

[35] HITECH § 134019(a) HITECH took into consideration that your personal health information would likely be viewed by a third party business associate. If you get into a car accident and your

accountability and transparency for *all entities* that have access to a patient's personal health information.

Notification in the Case of Breach

In addition to access reports and accountings of disclosures, covered entities must notify an individual if his or her personal health information has been breached[36]. Notification of breach is an additional safeguard on personal health information. If a covered entity discovers unauthorized access to a patient's file, the covered entity has a duty to notify the individual.[37] This accountability extends to business associates, as they have an obligation to notify the covered entity that provided the personal health information in the event of a breach or reasonable belief of a breach.[38] Breach notifications encourage cryptic securities such as passwords to prevent wandering eyes or accidental contact by unauthorized parties. In cases where more than 500 electronic health records are breached, the covered entity must alert HHS[39] and the media.[40] HHS posts these mass breaches on their website.[41]

---

medical information needs to be disclosed to the law firm covering your case, this law firm is now held to the same audit trail standards as the medical professionals that provide this information. Every associate or paralegal that accesses your medical health information is accounted for.

[36] HITECH § 13400(1) defines "breach" as the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information

[37] HITECH § 13402(a) A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

[38] HITECH § 13402(b)(4) A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

[39] [39] HITECH § 13402(e)(4), Posting on HHS Public Website, The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.

[40] HITECH § 13402(e)(2), Media Notice, Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if

Resistance from Medical Professionals

Practical concerns like cost and technological congruency interfere with the adaptation and implementation of EHR systems. Medical health professionals, especially large hospitals, have been outspoken against the HITECH amendments. University Hospital provided approximately 5 million outpatient encounters, 153,000 emergency department visits, and more than 56,000 inpatient and outpatient surgeries.[42] In a recent analysis of ten EHR charts from inpatient stays ranging from 6 to 30 days, University Hospital found that the selected charts were accessed an average of *861 times* while the patients were in the hospital. The one 30-day stay patient in the sample had *2693 touches* in the record during that one stay alone, and the audit report during the stay totaled 82 pages.[43]

University Hospital and other medical health professionals complain that the amended accountings do not appropriately balance the relevant privacy interests of individuals with the burdens on a covered entity.[44] Many comments include the imbalance between the burdens of creating accountings and the benefit individuals receive.[45] Critics back this position with records of one or few accountings actually requested by patients.[46] While hospitals may find this inequality and infrequency as legitimate reasons for rejecting HITECH's accounting amendments, it is shortsighted in viewing audit trails as a process solely for accountings. It is imperative not to overlook the value of these accounting procedures when applied to secure, transparent information

---

the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

[41] Department of Health and Human Services, Breaches Affecting 500 people or More, *supra* note 3.

[42] Jennifer L. Edlind, HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011), Aug. 1, 2011, at 1 (*responding* to request for comment on HIPAA Privacy Rule and Accounting of Disclosures in capacity as University Hospital Privacy Officer).

[43] Elind, University Hospital, at 5.

[44] Elind, University Hospital, at 2.

[45] Larry Davis, Attention: HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011), July 21, 2011, at 3 (*responding* to request for comment on HIPAA Privacy Rule and Accounting of Disclosures in capacity as St. Bernards Healthcare Corporate Compliance Officer).St. Bernards p3

[46] Davis, St. Bernards, at 3.

exchange. These same data collection burdens are justified when viewed with the understanding of interoperability as the next stage of use for accountings.

Bite the Bullet, Open the Wallet

HITECH's amendments to the Privacy Rule and Notification of Breach add boost accountability, transparency, and self-policing, in an attempt to increase patient trust. Accountings of disclosures, access reports, and breach notifications improve the detection of PHI violations and assist with the identification of weaknesses in existing privacy and security practices. HITECH's goal, however, is not just meaningful use within individual EHRs. The objective is to securely exchange personal health information. Nationwide interoperability of medical information has the ability to improve medical care through the exchange of ideas to better treat patients, understand progressive procedures, and compile data to prevent, curb, and cure diseases.

The Securities and Exchange Commission (SEC) faced similar obstacles and resistance when implementing the consolidated audit trail. Self-Regulating Organizations (SROs) had audit trail systems in place for oversight of trades and transactions within financial markets. These systems, however, are antiquated. SROs were unable to keep pace with the evolution of the industry they regulated.[47] The SEC knew decisive action must be taken to remedy the shortcomings of current audit trails.[48] Instead of putting band-aids on bullet wounds, the SEC decided to overhaul audit trail procedures. SROs and market participants understood that for this to successful and sustainable, they were going to have to pay large up front costs. Although there were objections and complaints, after weighing the options, the choice was clear that CAT was necessary.

University Hospital and other large medical institutions complain of the quantity of data compiled for accountings. The financial sector accepted CAT's additional costs and work. The health care industry needs to match this commitment for the benefit of secure health information regulation and exchange. In order to meet the goals of

[47] 17 C.F.R. § 242 (2012).
[48] 17 C.F.R. § 242 (*citing* 76 Fed. Reg. 46960, August 3, 2011).
"Recent experience with implementing incremental improvements to the EBS system has illustrated some of the overall limitations of the current technologies and mechanisms used by the industry to collect, record, and make available market activity data for regulatory purposes".

HITECH, the health care industry must prioritize IT expenses and meet the efforts of other industries.[49] The financial sector spent over 10% of total revenue towards IT repairs and advancement.[50] The healthcare industry spent less than half of that. This inequality cannot be blamed on a lack of activity in finance with the quantity and frequency of National Market System (NMS) securities[51] transactions.[52] The consolidated audit trail's format, procedures, and costs should serve as a model for ONC-HIT when establishing personal health information exchange.

Table 1

Industry	**2007**	**2008**	**2009**	**2010**
Financial Services	**524,120**	**548,025**	**502, 616**	**515,927**
Public Sector	438,829	464,288	443,368	459,969
Manufacturing	448,461	470,606	433,244	436,024
Communications	202,325	215,060	201,882	206,386
Retail	216,822	226,815	210,816	214,161
Services	171,459	182,274	172,061	175,046
Utilities	115,562	122,169	114,306	118,218
Transportation	103,522	105,565	99,842	101,711
Healthcare	**79,592**	**85,058**	**79,798**	**82,207**
Agriculture, Mining, and Construction	27,509	27,962	25,391	25,805
Total	2,328,200	2,450,920	2,283,325	2,335,453

*IT Spending by Industry Markets Worldwide (Millions of U.S. Dollars)

[49] Gartner Corporate Marketing, Perspective IT Spending 2010 at 16 (*See* tbl. 1).
[50] Nash, Kim, Information Technology Budgets: Which Industry Spends the Most?, CIO.com. Nov. 2, 2007. 2008 ("State of the CIO" survey of 558 heads of IT. Survey respondents in financial services, government, health care and wholesale/retail industries said they expect to be hiring IT staff in the next 12 months)(*See* tbl. 2).
[51] 17 C.F.R. § 242.600(a)(46) defines NMS security as "any security or class of securities for which transaction reports are collected, processed, and made available pursuant to an effective transaction reporting plan, or n effective national market system plan for reporting transactions in listed options."
[52] Securities Industry and Financial Markets Association, Statistics and Data Pertaining to Financial Markets and the Economy, (Nov. 11, 2012), http://www.sifma.org/research/statistics.aspx (*See* tbl. 3 at 26).

Table 2

Industry	IT Budget as a Percent of Revenue	Users per IT Staffer
Financial Services	10.5	15.7
Government	7.8	37.8
Education/nonprofit	6.2	48.3
Health Care	5.0	25.4
Wholesale and Retail	3.9	47.5
Manufacturing	3.4	40.9
Overall Sample	6.7	35.1

Consolidated Audit Trail

Stocks, bonds, derivatives, and other financial instruments are traded in fractions of a second. With the vast emergence of high-frequency trading (HFT), these transactions are too fast and too complex than human traders keep pace with.[53] This exposes investors, brokers, and exchanges to error and opportunity for fraud. Understanding the evolution of the markets, the Securities and Exchange Commission adopted Rule 613 under the Securities Exchange Act of 1934. The goal of Rule 613 is to create a comprehensive consolidate audit trail and a central repository that allows regulators to efficiently and accurately track all activity in NMS securities throughout the U.S. markets.[54] The SEC will use data compiled under Rule 613 to improve its understanding of how markets operate and evolve, including new trading practices, the reconstruction of atypical or novel market events, and the implications of new markets or market rules.[55]

Rule 613 mandates that the self-regulatory organizations, including the Financial Industry Regulation Authority (FINRA), submit the NMS Plan to create, implement, and maintain a consolidated order tracking system with respect to the trading of national

[53] Bowley, Graham, The New York Times, *Fast Traders, In Spotlight, Battle Rules*, (July 17, 2011), "Trading mostly with their owners' money, [HFTs] scoop up hundreds or thousands of shares in one transaction, only to offload them less than a second later before buying more. They can move millions of shares around in minutes, earning a tenth of a penny off each share.", http://www.nytimes.com/2011/07/18/business/fast-traders-under-attack-defend-work.html?_r=0.
[54] 17 C.F.R. § 242.
[55] 17 C.F.R. § 242.

market system securities.[56] The NMS Plan would capture customer and order event information for trades in national market system securities, across all markets, from the time of order inception through routing, cancellation, modification, or execution.[57] While the SROs are responsible for creating the NMS Plan, Rule 613 sets forth certain minimum requirements that must be included in the NMS Plan.[58] Rule 613 requires that the SROs propose a plan that includes provisions regarding: (1) the operation and administration of the NMS plan; (2) the creation, operation and oversight of a central repository; (3) the data required to be provided by SROs and their members to the central repository; (4) clock synchronization; (5) compliance by national securities exchanges, FINRA, and their members with Rule 613 and the NMS plan; and (6) a plan for the possible expansion of the NMS plan to products other than NMS securities.[59]

The NMS Plan

While SROs have not completed the details on the NMS Plan, Rule 613's minimum standards set a solid foundation for secure, efficient, and practical audit trail system. Each participant in a financial trade or transaction will mark their role with a thumbprint, attaching liability in the oversight of financial markets. Rule 613 seeks transparent, efficient markets that demand accountability throughout the lifecycle of a trade.

The lifecycle of an order[60] or a reportable event[61] required by Rule 613 typically originates with the customer[62] sending an order containing the type of security, size, and

[56] 17 C.F.R. § 240 (2012).
[57] 17 C.F.R. § 240.
[58] 17 C.F.R. § 242.
[59] 17 C.F.R. § 242.
[60] SEC Rule 613 Consolidated Audit Trail (CAT) SRO NMS Plan Industry Call, (September 19, 2012), (i) Any order received by a member of a national securities exchange or national securities association from any person; (ii) Any order originated by a member of a national securities exchange or national securities association; or (iii) Any bid or offer.
[61] 17 C.F.R. § 242.613(j)(9). The term *reportable event* shall include, but not be limited to, the original receipt or origination, modification, cancellation, routing, and execution (in whole or in part) of an order, and receipt of a routed order.
[62] 17 C.F.R. § 242.613(j)(3). The term *customer* shall mean: (i) the account holder(s) of the account at a registered broker-dealer originating the order; and (ii) Any person from whom the broker-dealer is authorized to accept trading instructions for such account, if different from the account holder(s).

price to the originating broker-dealer. This price is based on the SEC's mandate that published National Best Bid Offers (NBBO) be included in the report.[63] The broker-dealer then finds the other side of the trade order either internally at another broker-dealer desk within the firm, an external broker-dealer, national securities exchange, or national securities association. The order is modified, cancelled, or executed, in whole or in part.

These participants are now tagged with unique identifiers to trace their respective roles and the order information in a trade. Customers who originate the order are identified by their Customer-ID.[64] The customer's order is tagged with a CAT-Order-ID.[65] The customer then sends the order to the originating broker-dealer. The receiving broker-dealer or exchange is itself identified by a Cat-Reporter-ID.[66] The broker-dealer records the material terms[67] of the order, and the deal now transitions from origination[68] to routing.[69] At this juncture, the trade can be modified, cancelled[70], or executed in whole

[63] 17 C.F.R. § 242.613(e)(7)(i).
[64] 17 C.F.R. § 242.613(j)(5). The term *Customer-ID* shall mean, with respect to a customer, a code that uniquely and consistently identifies such customer for purposes of providing data to the central repository
[65] 17 C.F.R. §242.613(j)(1). The term *CAT-Order-ID* shall mean a unique order identifier or series or unique order identifiers that allows the central repository to efficiently and accurately link all reportable events for an order, and all orders that result from the aggregation or disaggregation of such order.
[66] 17 C.F.R. § 242.613(c)(7)(i)(C). The term *CAT-Reporter-ID* shall mean, with respect to each national securities exchange, national securities association, and member of a national securities exchange or national securities association, a code that uniquely and consistently identifies such person or purposes of providing data to the central repository.
[67] 17 C.F.R. § 242.613(j)(7). The term *material terms of the order* shall include, but not be limited to, the NMS security symbol; security type; price (if applicable); size (displayed and non-displayed); side (buy/sell); order type; if a sell order, whether the order is long, short, short exempt; open/close indicator; time in force (if applicable); if the order is for a listed option, option type (put/call), option symbol or root symbol, underlying symbol, strike price, expiration date, and open/close; and any special handling instructions.
[68] 17 C.F.R. § 242.613(c)(7)(i). For original receipt or origination of an order:(A) Customer-ID(s) for each customer; (B) The CAT-Order-ID; (C) The CAT-Reporter-ID of the broker-dealer receiving or originating the order; (D) Date of order receipt or origination; (E) Time of order receipt or origination (using time stamps pursuant to paragraph (d)(3) of this section); and (F) Material terms of the order.
[69] 17 C.F.R. § 242.613(c)(7)(ii). For the routing of an order, the following information: (A) The CAT-Order-ID; (B) Date on which the order is routed; (C) Time at which the order is routed (using time stamps pursuant to paragraph (d)(3) of this section); (D) The CAT-Reporter-ID of the broker-dealer or national securities exchange routing the order; (E) The CAT-Reporter-ID of the broker-dealer, national securities exchange, or national securities association to which the order is being routed; (F) If routed internally at the broker-dealer, the identity and nature of the department or desk to which an order is routed; and (G) Material terms of the order.

or in part.[71] If the trade is executed in whole or in part, the broker-dealer or exchange finds a counterparty and carries out the order.[72] The data is to be recorded contemporaneously with the reportable event, but does not need to be sent to the central repository until 8:00am Eastern Time the following trading day.[73] Every broker-dealer and exchange that touches an order must record the required data with respect to actions it takes on the order, contemporaneously with the reportable event, to ensure that all relevant information is accurately captured and reported to the consolidated audit trail.[74] This method prevents duplicative reporting of audit trail information because each market participant is required to report only the audit trail data for the actions it has taken with respect to an order.[75]

Investors rely on the integrity of broker-dealers and exchanges to execute their requested trade at the NBBO. Because these trades can occur in less than a millisecond[76],

---

[70] 17 C.F.R. § 212.613(c)(7)(iv). If the order is modified or cancelled, the following information: (A) The CAT-Order-ID; (B) Date the modification or cancellation is received or originated; (C) Time the modification or cancellation is received or originated (using time stamps pursuant to paragraph (d)(3) of this section); (D) Price and remaining size of the order, if modified; (E) Other changes in material terms of the order, if modified; and (F) The CAT-Reporter-ID of the broker-dealer or Customer-ID of the person giving the modification or cancellation instruction.

[71] 17 C.F.R. § 242.613(c)(7)(v). If the order is executed, in whole or part, the following information: (A) The CAT-Order-ID; (B) Date of execution; (C) Time of execution (using time stamps pursuant to paragraph (d)(3) of this section); (D) Execution capacity (principal, agency, riskless principal); (E) Execution price and size; (F) The CAT-Reporter-ID of the national securities exchange or broker-dealer executing the order; and (G) Whether the execution was reported pursuant to an effective transaction reporting plan or the Plan for Reporting of Consolidated Options Last Sale Reports and Quotation Information.

[72] 17 C.F.R. § 242.613(c)(7)(vi), If the order is executed, in whole or part, the following information: (A) The account number for any subaccounts to which the execution is allocated (in whole or part); (B) The CAT-Reporter-ID of the clearing broker or prime broker, if applicable; and (C) The CAT-Order-ID of any contra-side order(s).

[73] 17 C.F.R. § 242.613(c)(3).

[74] 17 C.F.R. § 242 (*citing* note 280) For example, if a member receives an order from a customer, the member will be required to report its receipt of that order (with the required information) to the central repository. If the member then routes the order to an exchange for execution, the member will be required to report the routing of that order (with the required information) to the central repository. Likewise, the exchange receiving the routed order will be required to report the receipt of that order from the member (with the required information) to the central repository.

[75] 17 C.R.F. § 242 (*citing* note 280).

[76] Securities and Exchange Commission Open Meeting: Creating a Consolidated Audit Trail, (July 11, 2012), http://www.sec.gov/news/press/2012/2012-134.htm.

there is opportunity for manipulation or front-running[77] trades. If the originating broker-dealer is required to record the time of each order, in a rapid series of principal orders regulators will be able to more accurately reconstruct the sequence of those orders when conducting market surveillance.[78] Therefore, the date and time are reported to the millisecond at each stage of the order lifecycle.[79] Once all of the unique identifier information is compiled, it must be sent to the central repository. Here, the data is received, consolidated, and retained by the SROs and their members.[80] The SEC and SROs will use of this data to performing their respective regulatory and oversight responsibilities.[81] The central repository will specify a maximum error rate to be tolerated for any data reported, measure the error rate each business day, and promptly take appropriate remedial action if the error rate exceeds the maximum. [82]Information regarding when a broker-dealer received a routed order could prove useful during investigations of best execution violations to see if there were delays in executing an order.[83] Requiring the originating broker-dealer to record the time an order was received from a customer could then help regulators more accurately determine whether the broker-dealer traded ahead of the customer.[84] If a regulator needs to investigate a delay between the time a market participant received an order and the time the market participant acted on the order, they can use information recorded and reported by the market participant itself.[85]

Complimentary to Rule 613, the SEC adopted two rules to improve public disclosure of order execution and routing practices. Under Rule 11Ac1-5, market centers that trade NMS securities will be required to make available to the public monthly

---

[77] *Financial Dictionary*, http://financial-dictionary.thefreedictionary.com/Front+Running, defines Front-Running as: Entering into an equity trade, options or futures contracts with advance knowledge of a block transaction that will influence the price of the underlying security to capitalize on the trade. This practice is expressly forbidden by the SEC. Traders are not allowed to act on nonpublic information to trade ahead of customers lacking that knowledge.
[78] 17 C.F.R. § 242.
[79] 17 C.F.R. § 242.
[80] 17 C.F.R. § 242.613(e)(1).
[81] 17 C.F.R. § 242.613(e)(2).
[82] 17 C.F.R. § 242.613(e)(6)(ii,iii).
[83] *Id.*
[84] *Id.*
[85] *Id.*

electronic reports that include uniform statistical measures of execution quality.[86] Broker-dealers that route customer orders in equity and option securities will be required to make quarterly reports publicly available that, among other things, identify the venues to which customer orders are routed for execution.[87] In addition, broker-dealers will be required to disclose to customers the venues to which their individual orders were routed upon request.[88] By making visible the execution quality of the securities markets, the rules are intended to spur more vigorous competition among market participants to provide the best possible prices for investor orders."[89]

Costs

SROs will face significant costs implementing the systems and infrastructure required for a successful audit trail. These costs include: the purchase and maintenance of servers and systems to receive, consolidate, and retain audit trail data, and to allow access to and searches on the data; the development of policies and procedures relating to the timeliness, accuracy, completeness, security, and confidentiality of the data collected the development and maintenance of a comprehensive information security program for the central repository; and dedicated staff, including a COO.[90]

Each SRO, on average, would incur a one-time cost of approximately $717,600 to prepare and file the NMS plan.[91] The 17 participating SROs would then total $12,200,200.[92] The NMS plan must include additional provisions relating to enforcement mechanisms, security and confidentiality, and the preparation of a document every two

[86] 17 C.F.R. § 240 (*Summarizing* Rules 11Ac1-5,6).
[87] 17 C.F.R. § 240 (*Summarizing* regarding Rules 11Ac1-5,6).
[88] 17 C.F.R. § 240 (*Summarizing* Rules 11Ac1-5,6).
[89] 17 C.F.R. § 240 (*Summarizing* Rules 11Ac1-5,6).
[90] 17 C.F.R. § 242.
[91] 17 C.F.R. § 242. Commission staff estimates that each SRO would incur an aggregate one-time cost of (700 Attorney hours x $378 per hour) + (300 Compliance Manager hours x $279 per hour) + (880 Programmer Analyst hours x $196 per hour) + (880 Business Analyst hours x $201 per hour) = $697,660 per SRO to prepare and file an NMS plan. In addition, Commission staff estimates that each SRO would incur a one-time external cost of (50 legal hours x $400 per hour) = $20,000. As a result, the Commission staff estimates that the aggregate one-time cost to each SRO to prepare and file an NMS plan, including external costs, would be ($20,000 in external costs) + ($697,660 in aggregate internal costs) = $717,660 per SRO to prepare and file an NMS plan.
[92] 17 C.F.R. § 242.

years that contains a retrospective assessment of the performance of CAT.[93]
The Commission now estimates that the aggregate one-time burden hour amount for preparing and filing an NMS plan would be approximately 2,760 burden hours with $20,000 in external costs per SRO,[94] or approximately 46,920 burden hours and $340,000 in external costs in the aggregate.[95] The SEC firmly believes that requiring every market participant that touches an order to record and report the audit trail data to the central repository is worth the effort and expense.[96] Vital to the effectiveness of CAT are the unique identifiers.[97] The inclusion of unique customer identifiers should greatly facilitate the identification of the orders and actions attributable to particular customers and thus substantially enhance the efficiency and effectiveness of the regulatory oversight provided by the SROs and the SEC.[98]

Now that HITECH has established baseline rules regarding access reports, accounting of disclosures, and breach notifications for individual's health records, the focus must be turned on how to continue this system on a national scale. Secure interoperability is the core of HITECH, without which, the goals and benefits are compromised. HITECH directs ONC-HIT to undertake activities consistent with the development of a nationwide health IT infrastructure, allowing for electronic use and exchange of secure health information.[99] HITECH presented specific goals for ONC-HIT

---

[93] 17 C.F.R. § 242.613(b)(6)(i-v).
[94] 17 C.F.R. § 242. Commission staff estimates that each SRO would spend an aggregate one-time amount of (700 Attorney hours) + (300 Compliance Manager hours) + (880 Programmer Analyst hours) + (880 Business Analyst hours) = 2,760 burden hours per SRO to prepare and file an NMS plan. In addition, Commission staff estimates that each SRO would incur a onetime external cost of (50 legal hours x $400 per hour) = $20,000.
[95] 17 C.F.R. § 242 Final Rule at 381 Commission staff estimates that the SROs would incur an aggregate one-time amount of (2,760 burden hours per SRO) x (17 SROs) = 46,920 burden hours to prepare and file an NMS plan. Commission staff estimates that ($20,000 per SRO) x (17 SROs) = $340,000 in external costs to prepare and file the NMS plan.
[96] 17 C.F.R. § 242.
[97] 17 C.F.R. § 242.
[98] 17 C.F.R. § 242.
[99] HITECH § 13001 (c)(3)(A)(i-viii.) (ONC-HIT's responsibilities via HITECH) (1) ensures that each patient's health information is secure and protected, in accordance with applicable law; (2) improves health care quality, reduces medical errors, reduces health disparities, and advances the delivery of patient centered medical care; (3) reduces health care costs resulting from inefficiency, medical errors, inappropriate care, duplicative care, and incomplete information; (4) provides appropriate information to help guide medical decisions at the time and place of care; (5) ensures the inclusion of meaningful public input in such development of such infrastructure;

to achieve regarding electronic health information.[100] Accountings of disclosures provide patients insight into who views an individual's medical records and why. There is a need to continue this security through the exchange of information. For the same reasons we feel that a snoopy nurse peeking at a medical record is invasive, an inconsistent, under-regulated exchange will leave patients vulnerable and oblivious to where their personal information travels. The infrastructure and standards regarding the transfer and exchange of EHRs are in its infancy. ONC-HIT is developing regulations for a secure, interoperable exchange. In doing so, it would be wise to look to the Securities and Exchange Commission's Consolidated Audit Trail as a model of how to send information in a secure, yet efficient manner.

National Health Information Network

ONC-HIT is working with the federal Health Information Technology Policy Committee (HIT-PC) on the development of the Nationwide Health Information Network establishing a set of standards, services, and policies that enable the secure exchange of

---

(6) improves the coordination of care and information among hospitals, laboratories, physician offices, and other entities through an effective infrastructure for the secure and authorized exchange of health care information; (7) improves public health activities and facilitates the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks; ''(8) facilitates health and clinical research and health care quality; (9) promotes early detection, prevention, and management of chronic diseases; (10) promotes a more effective marketplace, greater competition, greater systems analysis, increased consumer choice, and improved outcomes in health care services; and (11) improves efforts to reduce health disparities.

[100] HITECH 13101(c)(3)(a)(i-vii) (i) The electronic exchange and use of health information and the enterprise integration of such information; (ii) The utilization of an electronic health record for each person in the United States by 2014; (iii) The incorporation of privacy and security protections for the electronic exchange of an individual's individually identifiable health information; (iv) Ensuring security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable; (v) Specifying a framework for coordination and flow of recommendations and policies under this subtitle among the Secretary, the National Coordinator, the HIT Policy Committee, the HIT Standards Committee, and other health information exchanges and other relevant entities; (vi) Methods to foster the public understanding of health information technology; (vii) Strategies to enhance the use of health information technology in improving the quality of health care, reducing medical errors, reducing health disparities, improving public health, increasing prevention and coordination with community resources, and improving the continuity of care among health care settings; (viii) Specific plans for ensuring that populations with unique needs, such as children, are appropriately addressed in the technology design, as appropriate, which may include technology that automates enrollment and retention for eligible individuals.

health information over the internet.[101] NHIN is a key component of the nationwide health IT strategy and will provide a common platform for health information exchange across entities helping to achieve the goals of HITECH.[102] A successful national health information exchange policy includes cost effective interoperability and trusted exchange that raises the level of standards in the healthcare system.[103] HIT-PC admits that there is a need for a nationwide governance framework.[104] The fragmentation of governance methods and approaches at local and regional levels has increased the time, cost, and complexity of exchange-to-exchange governance.[105] This ad-hoc governance approach has led to asymmetries in the policies and technical standards, evident in the various local, regional, and state exchange activities.[106]

Pilots Off Course

ONC-HIT established pilot programs to test procedures and policies best suited for secure information exchange. It began with select organizations participating in a collaborative to test and demonstrate the exchange of private and secure health information among providers, patients, and other health care stakeholders.[107] The participants of the NHIN Cooperative were bound by the Data Use and Reciprocal Support Agreement (DURSA) technical interoperability requirements.[108] DURSA is a legally binding, multi-party agreement requiring members to follow certain security protocols as a condition of joining the health information exchange.[109] DURSA highlighted the need for consistent implementation of the Privacy Rule to strengthen trust in the exchange. DURSA's main fault is that it operates as a "members-only" club, isolating smaller, yet willing participants. Health care providers of lesser capabilities

[101] 45 C.F.R. § 171 (2012).
[102] 45 C.F.R. § 171.
[103] Office of the National Coordinator for Health IT, Governance RFI, HIT-PC Comments, at 2
[104] Office of the National Coordinator for Health IT, Governance RFI, HIT-PC Comments at 3. "Absence of a nationwide framework has not prevented the establishment of health information exchange, but the disparate efforts to create local, regional, and statewide governance approaches has increased the cost and burdens substantially."
[105] Office of the National Coordinator for Health IT, Governance FRI, HIT-PC Comments, at 3.
[106] 45 C.F.R. § 171.
[107] 45 C.F.R. § 171.
[108] 45 C.F.R. § 171.
[109] National Health Information Network, Data Use and Reciprocal Support Agreement, at 1 (November 18, 2009).

cannot exchange within DURSA. This "you're in or you're out" approach is directly against the goals of HITECH. Exchanging with small or financially restricted participants helps elevate their capabilities and medical proficiency, raising the national standard from the bottom up.

Another program ONC-HIT began was the Direct Project. The Direct Project was created to identify the standards, services, and policies necessary to enable a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the internet.[110] The Direct Project, however, focused mainly at the local level. These trials exposed the limitations of a "network of networks" approach and highlighted the need for nationally accepted standards, services, and policies.[111] Both projects were intended to facilitate secure health information exchange, however, HIT-PC noticed that a sum of parts would not likely lead to a fully functioning whole.

The success of a nationwide health information exchange depends on assurances that personal health information will remain confidential and secure.[112] In response to the shortcomings of the Direct Project, HIT-PC established Conditions for Trusted Exchange (CTEs)[113] to serve as the rules of the road for trusted, secure, and interoperable electronic exchange, nationwide.[114] CTEs would serve as the baseline standards, services, and policies that would be flexible to change to evolve with health information technology.[115] CTEs would be divided into three categories: Interoperability, safeguards, and business practices.[116] The intent of CTEs is to certify participants who meet the standard.

---

[110] 45 C.F.R. § 171.
[111] 45 C.F.R. § 171.
[112] *Id.*
[113] *Id.* [HITPC] believes that the CTEs could serve as a foundational set of requirements that could be used in one or more combinations to support many different forms of electronic exchange. CTEs appear to best be grouped into three categories: safeguards, interoperability, and business practices. *Safeguards CTEs* would focus on the protection of IIHI to promote its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. *Interoperability CTEs* would focus on the technical standards for the exchange and integration of electronic health information so that it is useful for the recipient. *Business Practices CTEs* would focus on the operational and financial practices or standards to which NVEs would need to adhere in support of trusted electronic exchange.
[114] *Id.*
[115] *Id.*
[116] *Id.*

HIT-PC anticipates that an entity's validation by the CTEs could be leveraged onto non-certified participants to meet certification requirements. The inference in this is the certified CTEs would not exchange with participants below grade. Once CTEs certify an entity, it is recognized as a Nationwide Health Information Network Validated Entity (NVE).[117] NVEs would likely be a network of exchanges from the Direct Project that have established systems, but are now following national certification standards.

Where NHIN Should Go From Here

There are two ways to approach successfully implement secure information exchange. One, is to establish high standards that only a select few can meet, and deny participation in exchange until lagging entities eventually catch up to approval thresholds. The other is through an extension of already-encouraged compliance with meaningful use of EHRs including accountings of disclosures through audit trails. Secure information exchange is more easily monitored by understanding who has viewed or accessed personal health information. Implementing audit trail procedures similar to CAT eliminates the need to recreate the wheel and promotes inclusion in nationwide health information exchange.

Right now, OCR is following the first path. DURSA and other exchange pilot programs have excluded participants who cannot make immediately meet their agreement requirements. This method isolates eager, yet temporarily unable entities from accessing information that will help increase profitability and efficiency. NVE approval confirms this members only mentality. Secure interoperability was mandated to help increase the quality of health care nationwide, not simply for those who can afford to make the immediate payments. Yes, audit trails require funds as well, but these are the same investments that are already supplemented by government incentive programs. Health care professionals are already allocating expenses in this direction; why not use them for both micro and macro purposes? The consolidated audit trail faced the same issues that HIT-PC and OCR are addressing now.

[117] 45 C.F.R. § 171.

The consolidated audit trail provides a template that directly relates to the secure information exchange desired by HIT-PC.[118] Trust and transparency are the foundation to successful, secure information exchange. The use of Customer-IDs, CAT-Order IDs, and CAT-Reporter IDs could help alleviate any of these concerns. Customer-IDs should be sent to each medical health professional that qualifies for meaningful use of EHRs. Meaningful use will not only come with incentive payments, but also a renewal of the entity's Customer-ID. NVEs would play the role of the investor in CAT. Each information exchange sent or requested should be marked with an Order-ID[119]. The exchange of personal health information is akin to the investor's trade sent to a broker-dealer or exchange. Similar to how originating broker-dealers must mark the reportable data for a trade, the NVE that accepts the information from the medical health professional will have a Reporter-ID and should have the same liability as the CAT broker-dealer or exchange in the same position. Providing these unique identifiers would not be a significant burden in relation to CTE standards.[120]

NHIN is not a physical network that runs on servers at HHS nor is it a large network that stores patient records. Exchanges look to CONNECT[121] software to ensure

---

[118] 45 C.F.R. §171. Condition I-2: "An NVE must follow required standards for establishing and discovering digital certificates" (HIT-PC elaborating on this condition, "Digital certificates are used to create a high-level assurance that an organization exchanging electronic health information is the entity it claims to be." Using CAT-Customer IDs and following the consolidated audit trail procedures achieves this goal).

[119] 45 C.F.R. §171. Condition I-3: "An NVE must have the ability to verify and match the subject of a message, including the ability to locate a potential source of available information for a specific subject." (HIT-PC elaborating on this condition, "The intent of this CTE is to provide guidance for NVEs to verify and match message subjects (i.e. patients) using a record locater services, master patient index, or another approach." A Customer-ID would directly cover this requirement.).

[120] 45 C.F.R. §171. Condition S-10: "An NVE must have the means to verify that a provider requesting an individual's health information through a query and response model has or is in the process of establishing a treatment relationship with that individual." (Each request for health information must accompany reasonable proof of a relationship to an individual related to health information. Any arguments regarding burden against a one-time Reporter-ID or Customer-ID attachment fall short comparing time and labor to S-10).

[121] Connect Community Portal: What is CONNECT, "CONNECT is an open source software solution that supports health information exchange – both locally and at the national level. CONNECT uses Nationwide Health Information Network standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country. This software solution was initially developed by federal agencies to support their health-related missions, but it is now available to all organizations and can be used to help set up

compatibility between exchanges.[122] HIT-PC and commentators are contemplating strategies for supervision of NHIN. A central repository that compiles exchange information creates a hub to consolidate regulation and supervision. Regulation through a central repository would also provide for more standardized and consistent enforcement. Legal history is filled with conflicting interpretation of federal law through satellite enforcement. Due to the fact that at the early stages of implementation there will be general or vague standards opening the likelihood for varying interpretations in the network-of-networks model. HIT-PC should strongly consider CAT's central repository while crafting uniform regulatory guidelines and standards.

This fragmented format has also led to apprehension. Hospitals and medical health providers are hesitant to install hardware and software to meet current audit log standards.[123] University Hospital estimates software implementation costs at $700,000 and finds it fiscally irresponsible to constantly upgrade to meet requirements that may and likely will change in the near future.[124] The health care industry, in the infancy of interoperability, will have to adjust to the costs associated with evolving technologies and increasingly short system lives.[125]

HIT-PC overlooks another major issue towards certified exchange. Becoming a certified NVE is voluntary.[126] Non-certified entities are still able to exchange personal health information. HIT-PC presumes that non-certified entities would feel pressured to become an NVE because other NVEs would be hesitant to deal with a non-certified

---

health information exchanges and share data using nationally-recognized interoperability standards. CONNECT can be used to set up a health information exchange within an organization or tie a health information exchange into a regional network of health information exchanges using Nationwide Health Information Network standards."
http://www.connectopensource.org/about/what-is-connect, (last visited Nov. 9, 2012).

[122] Connect Community Portal: What is CONNECT,
http://www.connectopensource.org/about/what-is-connect, (last visited Nov. 9, 2012).

[123] University Hospital, at 6.

[124] University Hospital at 6. "It is not financially feasible for our organization to upgrade all of our systems in the current environment to enable, pay to develop, and store three years' worth of standardized audit logs- in a time when we have already incurred significant expenditures to upgrade our HIT systems for meaningful use standards and especially when we are under increased pressure from the federal and state governments, insurers, and patients to reduce the costs of health care delivery."

[125] Nicolas Terry, Information Technology's Failure to Disrupt Healthcare 36 (2012).

[126] 45 C.F.R. §171.

entity.[127] While this may be true, the fact remains that non-secure entities that have below-standard security *are still able to exchange personal health information*. By making CTE certification voluntary, HIT-PC creates a "Wild Wild West" subsection of health information exchange that is openly susceptible to fraud and security breaches. A non-certified entity could offer medical health professionals incentives to mask and induce use of non-NVE exchange. Should there be an obligation for non-certified entities to disclose their status? HIT-PC addresses the role of NVEs, but bases the remainder of NHIN on the assumption of conformity with NVE certification.

Consistent with this principle, dividing the CTEs into three distinct groups allows for the strong likelihood that conflicts will arise creating policy. Similar to how SROs united to establish the NMS Plan, CTEs cannot work unless they are in unison. For example, Safeguard CTEs and Interoperability CTEs may have the same goal, but their plans or procedures in achieving this goal may clash. Offering opportunity for conflict in pursuit of uniformity is unnecessary for the sake of secure certification standards and should be avoided.

Just as SROs were once individualized in their approach, localized health exchanges and participating members must accept that the up-front costs and burdens for the long-term success of health information exchange. The SEC understood the sustainability and success of secure information exchange and fraud protection has its initial burdens. SROs saw the time, money, and effort saved in future organizational costs. NVEs must come to this conclusion independently. NVEs and health information providers will face costs related to the secure exchange of medical health information regardless of the tactic chosen. Modeling the NMS Plan with unique identifiers, a central repository, and mandatory participation, HIT-PC can meet the security, interoperability, and transparency it desires. Both Rule 613 and NHIN will evolve and expand. The

[127] 45 C.F.R. §171. "The validation process established as part of the governance mechanism would not be mandatory and would only apply in so far as an entity deciding that there would be value (e.g. prestige, competitive advantage) in seeking validation. That said, once the validation process is established, much like other government programs on which subsequent policy objectives could be leveraged, it would be possible for other public and private organizations to specify NVE recognition as a condition in awarding contracts, procurements, and/or in other situations here validation would be beneficial."

consolidated audit trail's centralized format allows for flexibility to grow with their respective markets.

Table 3

STOCK MARKET VOLUME
(Daily Avg., Mils. of Shares.)

NYSE	AMEX/ARCA*	NASDAQ	BATS**	DirectEdge	OTC Markets Group, Inc.
1,643.6	298.4	2,044.1	845.55	1,050.00	6,701.61
1,541.8	284.0	2,095.5	837.89	939.00	7,055.81
1,549.3	343.7	2,020.4	873.30	916.00	6,926.88
1,330.5	264.8	1,929.1	747.80	780.00	5,977.23
1,366.9	316.6	2,034.3	781.95	761.00	5,473.93
1,450.1	319.6	2,021.8	798.60	733.00	4,601.24
1,310.4	293.9	1,893.6	774.46	730.00	3,832.48
2,106.5	527.9	2,521.9	1,303.77	1,120.00	3,471.87
1,678.2	432.1	1,988.6	1,021.15	932.00	3,083.65
1,632.2	410.3	2,003.9	1,044.64	966.00	2,639.71
1,391.4	332.8	1,857.0	843.59	891.00	2,364.52
1,211.7	262.7	1,614.9	710.70	741.00	2,875.63
1,217.3	242.5	1,825.4	766.62	765.00	3,037.37
1,185.1	230.5	1,901.2	757.45	785.00	4,112.30
1,203.8	236.8	1,679.6	723.31	714.00	4,071.38
1,170.4	226.5	1,614.9	746.66	701.00	3,777.14
1,266.4	261.6	1,903.9	830.58	804.00	3,291.54
1,264.5	260.9	1,774.1	789.72	741.00	3,093.43
1,123.8	212.1	1,648.9	750.08	682.00	3,282.54
969.0	179.4	1,562.0	693.62	586.00	3,515.34
1,159.7	219.0	1,796.4	806.54	769.00	3,446.17
1,051.5	197.8	1,747.3	725.54	694.00	3,053.73
1,567.6	352.2	2,060.3	902.91	892.70	4,976.44
1,159.6	226.4	1,743.1	759.01	724.10	3,468.09
-26.0%	-35.7%	-15.4%	-15.94%	-18.89%	-30.31%