August 29, 2014

Please Provide the Entire Electronic Medical Record

Jonathan H. Lomurro, Esq. LLM

Please Provide the *Entire* Electronic Medical Record

By: Jonathan H. Lomurro, Esq. LLM

"By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care." – President George W. Bush, State of the Union Address (Jan. 20, 2004)

The former President's comments initiated the computerize health records initiative. The initiative to push computerized health records was, thereafter, enhanced by signing his signing of two executive orders which required the Department of Health and Human Services (HHS) to help advance efforts to achieve the goal. The first Executive Order directed that that Secretary of HHS establish the position of a National Health Information Technology Coordinator (NHITC).[1] Per the Order, the NHITC would be required to craft a plan which would advance the development, adoption, and implementation of health care information technology standards nationally. The second Executive Order promoted the expansion of health information technology (HIT) to the private and public sector.[2]

"We will make sure that every doctor's office and hospital in this country is using cutting edge technology and electronic medical records so that we can cut red tape, prevent medical mistakes, and help save billions of dollars each year."[3] - President Barack H. Obama, Radio Address (Dec 6, 2008)

The current President continued the former President's health records initiative by signing into law the Health Information Technology for Economic and Clinical Health Act (HITECH), within the larger American Recovery and Reinvestment Act of 2009 (ARRA), and the Patient Protection and Affordable Care Act (PPACA), signed in 2010. The HITECH Act codified the Office of the National Coordinator for Health Information Technology (NCHIT). It provided billions of dollars in incentives for clinicians and hospitals for the "meaningful use" of certified health information technology. (Note: in 2015, physicians and hospitals will be penalized for not using certified products in a meaningful way; going from incentivize to penalize). The Act established a goal of "utilization of a certified electronic health record

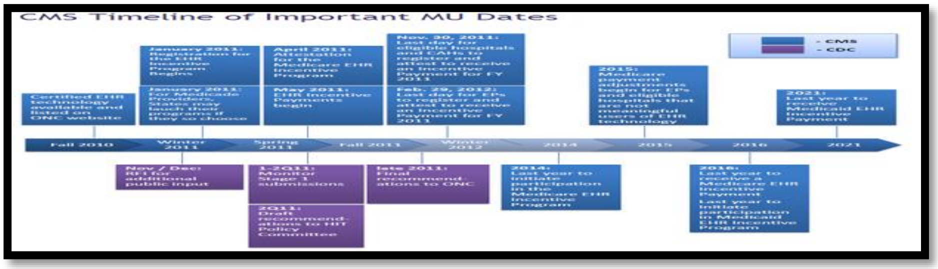
[1] April 27, 2004 – Executive Order: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator

[2] August 22, 2006 – Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs

[3] December 6, 2008 – President Obama Radio Address

for each person in the United States by 2014."[4] PPACA was designed to drive improvements in medical care and costs. In order to accomplish its goals, PPACA established the Center for Medicare and Medicaid Innovation (CMI). Also, the PPACA provided the CMI the ability to administer the EHR incentive program for clinicians and hospitals for the meaningful use of electronic health records (EHRs) discussed in the HITECH Act.

The Secretary had to publish, in the Federal Register, the determinations made for the adoption of required standards based on the corroboration of the National Coordinator and the Health Information Technology Standards Committee.[5] On September 26, 2010, the final rules, as related to meaningful use for Stage 1, became effective.[6] And on September 27, 2010, Medicare and Medicaid Services started offering incentive payments to clinicians and hospitals who meaningfully used certified EHR technology and meet electronic records requirements.[7] "The incentive payments [were] part of a broader effort under the HITECH Act to accelerate the adoption of HIT and utilization of qualified EHRs."[8] On August 23, 2012, the final requirements for Stage 2's Meaningful Use that hospitals and health care providers must meet in order to qualify for incentives was released.[9]


CMS Timeline of Important MU Dates
Certified EHR technology available and listed on ONC website
January 2011: Registration for the EHR Incentive Program Begins
January 2011: For Medicade Providers, States may lauch their programs if they so choose
April 2011: Attestation for the Medicare EHR Incentive Program
May 2011: EHR Incentive Payments begin
Nov. 30, 2011: Last day for eligible hospitals and CAHs to register and attest to receive an Incentive Payment for FY 2011
Feb. 29, 2012: Last day for EPs to register and attest to receive an Incentive Payment for FY 2011
2015: Medicare payment adjustments begin for EPs and eligible hospitals that are not meaningful users of EHR technology
2021: Last year to receive Medicaid EHR Incentive Payment
- CMS
- CDC
Fall 2010
Winter 2011
Spring 2011
Fall 2011
Winter 2012
2014
2015
2016
2021
Nov / Dec: RFI for additional public input
1-2Q11: Monitor Stage 1 submissions
2Q11: Draft recommend-ations to HIT Policy Committee
late 2011: Final recommend-ations to ONC
2014: Last year to initiate participation in the Medicare EHR Incentive Program
2016: Last year to receive a Medicare EHR Incentive Payment
Last year to initiate participation in Medicaid EHR Incentive Program

[10]

[4] 42 USC 300jj-11(c)(3)(A)(ii)

[5] 32 USC 300jj-14

[6] Federal Register, Vol. 75, No. 144, Wed. July 28, 2010, rules and regulations, (ONC) Part II, pp. 44314-44588 (42 CFR 412, 413, 422 et. al) and (CMS) Part III, pp. 44590-44654 (45 CFR 170)

[7] 42 C.F.R. 495.2

[8] Federal Register, Vol. 75, No. 144, Wed. July 28, 2010, rules and regulations, supra. at 44316

[9] Federal Register, Vol. 77, No. 171, Tues. Sep. 4, 2012, Department of Health and Human Services (CMS – Center for Medicare and Medicaid Services) Part II, pp. 52968-54162 (45 CFR 170; 42 CFR 412, 413, and 495) and (ONC – Office of the National Coordinator for Heath Information Technology) pp. 54163-54292 (45 CFR Part 170)

[10] CMS Timeline of Important MU Dates, Center for Disease Control and Prevention, www.cdc.gov/EHRmeaningfuluse/timeline.html

HIPPA, the Health Insurance Portability and Accountability Act, passed on August 21, 1996, originally held two objectives: ensure individuals would be able to maintain their health insurance between jobs and ensure the security and confidentiality of patient information and data.[11] The responsibility for developing privacy standards was delegated to the Department of Health and Human Services (HHS).[12] In 2003, HHS promulgated the HIPPA privacy rules and Security rules.[13] After the signing of ARRA and PPAC, the required regulations set forth by HHS and HIPAA were updated to create a uniform standard for electronic transactions; assemble unique health identifiers for each individual, employer, health care plan, and health care provider; and establish code sets for certain data elements.[14]

The rules created standards to address how health information may be used and protected. One of its purposes was to ensure that medical records could not be altered without detection; "protect the security and privacy of individual identifiable health information ('IIHI')."[15] As brilliantly explained by Judge Marina Corodemus (Ret.):

> "The passage of HIPAA and the enactment of the Privacy Rule mark a dramatic departure from the current state of medical and legal practice. The change is a myopic examination of a lone example of what may be the single most important question raised in the 21st century by Americans, namely balancing privacy concerns versus technological advancements. The more accessible personal information becomes, the more critical it is to create intelligible guidelines to provide an equitable balance between the individual's interest in his or her privacy and the national interest, in this instance, HIPAA compliance."

[11] "Health Insurance Portability and Accountability Act of 1996". Public Law 104-191 (HR 3103), 104th Congress, 110 Stat 1936 (codified as amended in various sections of Titles 18, 26, 29, and 42 of USC)

[12] Smith v. Am. Home Prods. Corp. Wyeth-Ayerst Pharm., 372 N.J.Super 105, 110 (Law Div. 2003)

[13] 67 Fed. Reg. 53, 182 (Aug. 14, 2002), 68 Fed. Reg. 8333, 8334 (to be codified at 45 C.F.R. 160, 162, 164; finalized in 45 C.F.R. 160, 162, 164 (2003)

[14] 45 C.F.R. 160.101 et seq.

[15] Smith v. Am. Home Prods. Corp. Wyeth-Ayerst Pharm., 372 N.J.Super 105, 110 (Law Div. 2003)

The HIPAA Security Rule required regular monitoring of system activity, including audit logs and access reports, by IT personnel or compliance officers on at least a quarterly basis. [16] Additionally, HIPAA Security Rules required every covered entity or business associate to use standard "audit controls" through implementation of "hardware, software, and/or procedural mechanisms to record and examine system activity in information systems that contain or use electronic protected health information."[17] The entities are required to "implement policies and procedures to protect electronic protected health information from improper alteration or destruction" and implement "[m]echanism[s] to authenticate electronic protected health information… to corroborate that electronic health information has not been altered or destroyed in an unauthorized manner."[18] In addition to authenticating the records, it was required they implement procedures to authenticate the person or entity seeking access.[19]

New Jersey has been a leader in Health Information Technology. In 1993, the State of New Jersey commissioned the Heath Information Technology Study, attempting to document the savings that could be achieved from health IT.[20] In 1999, New Jersey enacted the Health Information Electronic Data Interchange Act (the "HINT Act") to create a regulatory framework to advance standardized electronic submission of health care claims.[21] The HINT Act directed the New Jersey Department of Banking and Insurance (NJ DOBI) to adopt rules requiring the use of the federal HIPAA Transaction and Codes Sets (TCSs).[22] This was accomplished, on October 1, 2001, when NJ DOBI adopted N.J.A.C. 11:22-3.6.

Demonstrating its commitment to encouraging the adoption of new technology in the medical field, in 2003, New Jersey became the first State to promulgate regulations permitting a pharmacist to

[16] 45 CFR 160, 162, 164; 45 CFR 164.308(a)(1)(ii)(C); 45 CFR 164.312(b)

[17] 45 CFR 164.312(b)

[18] 45 CFR 164.312(c)(1) and (2)

[19] 45 CFR 164.321(d)

[20] New Jersey Application: Office of the National Coordinator for Health Information Technology State Health Information Exchange Cooperative Agreements Program's Project Narrative: p.2

[21] Id.

[22] Id.

"accept for dispensing an electronic prescription."[23] In 2008, Governor Jon S. Corzine signed into law the Health Information Technology Act of 2007, creating the Health Information Technology Commission and the Office of e-HIT in the State's Department of Banking and Insurance.[24]

In New Jersey's Health Information Technology Act, the Legislature found and declared that:

> "it is in the public interest for New Jersey residents to have all appropriate personal health information available to them.... Health information technology has great potential as one means of furthering progress towards achieving affordable, safe, and accessible health care for all persons by:… providing consumers with their own health information…. It is in desirable to implement an electronic health information infrastructure in the context of a Statewide health information technology plan that includes standards and protocols to promote patient education, patient privacy, physician best practices… in New Jersey."[25]

The Act defines Health information Technology as that which is used to electronically collect, store, retrieve, and transfer clinical, administrative, and financial health information.[26] The Acts plan was to create standards providing a means that entities are able to enhance data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks in such a way that the clinical or operational purposes and meaning of the data are preserved and unaltered.[27]

The Act established the New Jersey Health Information Technology Commission.[28] The Act also established, in the Department of Banking and Insurance, the Office for the Development, Implementation, and Deployment of Electronic Health Information Technology in New Jersey, to be known as the Office for e-HIT.[29] The HIT Commission and the Office for e-HIT were to collaborate to

[23] N.J.A.C. 13:39-7.11
[24] Id.
[25] N.J.S.A. 26:1A-133
[26] N.J.S.A. 26:1A-134
[27] N.J.S.A. 26:1A-134
[28] N.J.S.A. 26:1A-136
[29] N.J.S.A. 17:1D-1

develop, implement and oversee the operation of a State-wide health information technology plan.[30] The plan was required to comply with all State and federal privacy requirements.[31] On October 16, 2009, the New Jersey Plan for Health Information was released.[32] And, on August 13, 2010, the State HIT Operational Plan, submitted to the Office of the National Coordinator for Health Information Technology was created.[33] In December 2010, it was updated and finalized.[34]

The New Jersey Health Information Technology Extension Center (NJ-HITEC) was granted $23 million in Federal Funds to establish the statewide regional center.[35] This was accomplished by having the United States Department of Health and Human Services' Office of the National Coordinator for Health IT (ONC), in January 2011, adopt New Jersey's Operational HIT Plan; the plan includes helping healthcare providers make the transition to electronic health records, establish health information organizations, and facilitate data exchange among the HIOs operating in the state and provide a gateway to connect to other states.

In New Jersey, the New Jersey Health Information Technology Coordinator's Office, located within the Department of Health, oversees the New Jersey Health IT Program and implementation of the New Jersey Operational HIT Plan.[36] The core mission of the program is "[p]roviding all New Jersians with electronic health records."[37] Similar to the federal HITECH Act, in the State's HIT Operational Plan, part of New Jersey's Vision Statement was "we envision a New Jersey HIT environment by 2014 where: All NJ

[30] Id.
[31] Id.
[32] New Jersey Plan for Health Information Technology, October 16, 2009
[33] State HIT Operational Plan of August 13, 2010 containing December 2010 Updates
[34] Id.
[35] Id.
[36] New Jersey Health IT Program Overview found at http://www.nj.gov/health/njhit/document_files/NJ_HIT_Program_Information_Sheet_v4.pdf
[37] Id.

consumers have a secure electronic health record that includes all health related information and services."[38]

Another part of the Vision Statement, developed by the NJHITC and the Office for e-HIT, published in the NJ State Health Information Technology Plan was "Patient Accessible and Portable. All patients will have access to a secure, electronic and portable health record."[39] This follows the New Jersey Bill of Rights for hospital patients which states that every person admitted to a general hospital shall have the right to access all records pertaining to the patient's treatment and receipt of a copy thereof.[40]

The New Jersey Patient Rights for hospital patients states that a patient shall have prompt access to and can obtain a copy of the information contained in the patient's record and can obtain a copy.[41] As explained in the New Jersey Plan, technology exists that provides a way for patients to have access to their personal health records (PHRs).[42] And the New Jersey Health Information Technology Act found and declared that it is in the public interest for New Jersey residents to have all appropriate person health information available to them.[43] Electronic records make copying and dissemination easier. This is important because licensees, in New Jersey, are required to provide access to professional treatment records, including records from other licensees or other health care providers that are part of the patient's record, to a patient no later than 30 days from receipt of a request from a patient or authorized representative.[44]

[38] State HIT Operational Plan of August 13, 2010 containing December 2010 Updates, Section 1.0 Executive Summary, p. 7 of 167.
[39] New Jersey Plan for Health Information Technology, October 16, 2009, at p. 7
[40] N.J.S.A. 26:2H-12.8
[41] N.J.A.C. 8:43G-4.1(24), (25)
[42] New Jersey Plan for Health Information Technology, October 16, 2009, at p. 7
[43] N.J.S.A. 26:1A-133
[44] N.J.A.C. 13:35-6.5

So, the question becomes what is contained in the electronic health record. “The term ‘health information’ means any information, whether oral or recorded in any form or medium, that – (A) is created or received by a health care provider… and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.”[45] One of the benefits of electronic medical records is the metadata associated with it.

Metadata is commonly described as “data that describes other data.” It is information that helps to organize, utilize and understand other information. Metadata has been around for centuries. But it has only become part of everyday vernacular because of its association with electronically-stored information or ESI.

The easiest example of metadata is located within a library’s card catalog. The card catalog contains a plethora of information about the library’s books without actually providing a summary of the work itself. The metadata found on a catalog card will enable a person to find the book’s author, title, subject, location in the library, category, edition, literary or topical character, year of publication, publisher, number of pages, and any other pertinent “data about the data.”

Another easy way to understand metadata is to look at a globe. Think of the earth as the data. The metadata would be listed on the globe: latitude, longitude, axis, topography, meridian line, country lines, names and locations, and additional “data about the data.”

Moving from the physical metadata to digital metadata is not complicated. It is just like the globe and the card catalog. You just need to know where to look and what to look for. Digital metadata is commonly used to describe the contents, context, creation, editing and usage of the digital data. A file may contain metadata with several property fields: program or hardware that created the file, propose of the file, time and date of creation of file, last edited time and date, creator or author of file,

[45] 42 U.S.C. 1320d(4)

location on computer/network, and standards used in creation. As stated in one federal case, "[t]o understand why the importance of metadata varies, it is first necessary to explain what it is and distinguish among its principle forms."[46] Metadata is an electronic fingerprint utilized to authenticate, explain, and expand.

There are several ways to describe the different types of visual and hidden information contained in digital metadata.[47] It is the term used to describe the structural information of a file that contains data about the file, as opposed to describing the content.[48] In *Aguilar*, the court explained that, in order to understand the concept of metadata, it is easiest to break the information into three subsections: System, Substantive and Embedded.[49]

System metadata or application metadata is created by hardware such as a digital camera, phone, computer system or other device. It also includes the information management systems or

[46] Aguilar v. Immigration & Customs Enforcement, 255 F.R.D. 350, 354 (S.D.N.Y. 2008).

[47] The Sedona Conference, a well-known nonprofit and educational institute crafted to the advancement of technology within a legal technology working group, found at www.thesedonaconference.org, has crafted substantial and influential legal/tech glossary: Sherry B. Harris, *The Sedona Conference Glossary: E-Discovery & Digital Information Management,* 4th ed. 2014, *available at* https://thesedonaconference.org/publication/, providing an extremely comprehensive definition of most tech terminology. Their subpart definitions of metadata includes the following seven types of metadata: "**Application Metadata**: Data created by the application specific to the ESI being addressed, embedded in the file and moved with the file when copied; copying may alter application metadata. **Document Metadata**: Properties about the file stored in the file, as opposed to document content. Often this data is not immediately viewable in the software application used to create/edit the document but often can be accessed via a "Properties" view. Examples include document author and company, and create and revision dates. **File System Metadata**: Metadata generated by the system to track the demographics (name, size, location, usage, etc.) of the ESI and, not embedded within, but stored externally from the ESI. **Email Metadata**: Data stored in the email about the email. Often this data is not even viewable in the email client application used to create the email, e.g., blind copy addressees, received date. The amount of email metadata available for a particular email varies greatly depending on the email system. *Contrast with File System Metadata and Document Metadata* (*emphasis added*). **Embedded Metadata**: Generally hidden, but an integral part of ESI, such as "track changes" or "comments" in a word processing file or "notes" in a presentation file. While some metadata is routinely extracted during processing and conversion for e-discovery, embedded data may not be. Therefore, it may only available in the original, native file. **User-Added Metadata:** Data, possibly work product, created by a user while copying, reviewing, or working with a file, including annotations and subjective coding information. **Vendor-Added Metadata**: Data created and maintained by the electronic discovery vendor as a result of processing the document. While some vendor-added metadata has direct value to customers, much of it is used for process reporting, chain of custody, and data accountability."

[48] Ibid.

[49] Aguilar, 255 F.R.D. at 354 (S.D.N.Y. 2008).

networking data. The information is completely crafted by the system or application and does not involve user input. Substantive Metadata reflects the changes to the document's content by the user within an application (track changes, text changes, editorial comments etc.). The depth and history of this metadata information is application specific.

"[T]he more interactive the application, the more important the metadata is to understanding the application's output."[50] And electronic health records are required to be very interactive and specifically contain certain metadata, specifically audit information.

Turning back to Federal Regulations, the 2009 HITECH Act specified that electronic medical record (EMR) systems must satisfy certain requirements, such as recording access to patient records, showing who viewed or changed information, when this was done, and from what location; together, these statutes provide requirements that organizations using EMRs track and maintain a log of all access to electronic records.[51]

An audit trail is created by automated monitoring software that contemporaneously records the manipulation of a patient's EMR as it occurs. In laymen's terms, every time a user views, edits, prints, deletes, downloads, exports, or otherwise manipulates any part of a patient's EMR, the system makes a record of that activity. This record is known as an audit log or audit trail. The audit trail provides direct evidence of exactly what was done, when, and by whom, to a patient's medical record. Audit trail information, as described as metadata, is actually part of the patient's EMR. And federal law requires these audit controls.[52]

HIPAA required that the Secretary adopt Security Standards for health information which shall take into account the technical capabilities of record systems used to maintain health information and

[50] *Id.* at 353.
[51] Jennifer Keel. Follow of the Audit Trail; Trial, May 2014; citing 42 U.S.C. 1320d, 45 C.F.R. 160, 164, and 170.
[52] 45 C.F.R. 164.312

the value of audit trails in computerized record systems.[53] It required each person who maintains health information to maintain administrative, technical, and physical safeguards to ensure the integrity and confidentiality of the information.[54] Pursuant to the Secretary's authority, the provisions of 45 CFR 164 et seq. were adopted.[55] This set forth the standard and requirement specifications that apply to a health care provider, health care clearing house, and a health plan; which will be referred to as a covered entity.[56] Those covered entities must comply with the applicable standards, implementation specifications, and requirement of the subpart, for Security Standards for the Protection of Electronic Protected Health Information, will respect to electronic protected health information of a covered entity.[57]

Covered entities and business associations must ensure the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains or transmits.[58] It requires the covered entities to have an information system activity review: implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.[59] It requires the entity to maintain a record of the movements of hardware and electronic media and create a retrievable, exact copy of electronic protected health information when needed, before movement of the equipment.[60]

Audit controls are required.[61] They include implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.[62] This follows with the requirement of verifying integrity of the

[53] 42 USCA 1320d-2(d)(1)
[54] 42 USCA 1320d-2(d)(2)
[55] 45 C.F.R. 164.102
[56] 45 C.F.R. 160.102, 45 C.F.R. 160.103
[57] 45 C.F.R. 164.302
[58] 45 C.F.R. 164.306(a)(1)
[59] 45 C.F.R. 164.308(a)(1)(ii)(d)
[60] 45 C.F.R. 164.310
[61] 45 C.F.R. 164.312
[62] 45 C.F.R. 164.312(b)

record by implementing policies and procedures to protect health information from improper alteration or destruction.[63] The entity must document the policies and procedures for the required specifications.[64] To assist in understanding the standards, the subchapter of Health Information Technology's Part named Health Information Technology Standards, Implementation Specifications, and Certification Criteria and Certification Programs for Health Information Technology was adopted.[65]

The standards and implementation specification adopted apply to complete electronic heath records (EHRs) and EHR Modules.[66] In those, the Secretary adopted certain standards to protect electronic health information created, maintained, and exchanged.[67] The Secretary required the entity to record actions related to electronic heath information: the date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action occurred and by whom must also be recorded.[68] A hashtag algorithm is required to insure the electronic health information has not been altered in transit.[69] However, the most important requirement are set forth in sections 7.2 through 7.4, 7.6, and 7.7 of the standard audit log content ASTM E2147-01, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems (Audit Standards).[70] The Audit Standards were incorporated by reference.[71]

"In concert with organizational confidentiality and security policies and procedures, permanent audit logs can clearly identify all system application users who access patient identifiable information, record the nature of the patient identifiable information, record the nature of the patient information

[63] 45 C.F.R. 164.312(c)
[64] 45 C.F.R. 164.316
[65] 45 C.F.R. 170
[66] 45 C.F.R. 200
[67] 45 C.F.R. 210
[68] 45 C.F.R. 210(b)
[69] 45 C.F.R. 210(c)
[70] 45 C.F.R. 210(e)(1)(i) and (h)
[71] 45 C.F.R. 170.299

accessed, and maintain a permanent record of actions taken by the user."[72] "Such logs are specified in and support policy on information access monitoring ad are tied to disciplinary sanctions that satisfy legal, regulatory, accreditation and institutional mandates."[73] An audit log is defines as a record of actions, for example, creation, queries, views, additions, deletions, and changes performed on data.[74] An audit trail is a record of users that is documentary evidence of monitoring each operation of individuals on heath information; audit trails may be comprehensive or specific to the individual and information; for example an audit trail may be a record of all actions taken by anyone on a particularly sensitive file.[75] Authentication is defined as the provision of assurance of the claimed identity of an entity, receiver or object.[76] Health information is any information, whether oral or recorded in any form or medium that is created or received by a health care provider.[77]

An audit log is a record of actions (queries, views, additions, deletions, changes) performed on data by users and should be recorded at the time they occur.[78] Audits should identify and track individual users' access, including authentication and signoff, to a specific patient's or provider's data. This function should be done in real time and captured in audit logs.[79] The entity should allow for easy retrieval, report within a reasonable timeframe, and provide search capability by user and patient identification, date range, type of data accessed, and type of access (queries, views, additions, deletions, change).[80] The 5 specific requirement sections addressed in 45 C.F.R. 210(e)(1)(i) are:

> 7.2 *Date and Time of Event* – The exact date and time of the access event and the exit event
> 7.3 *Patient Identification* – Unique identification of the patient to distinguish the patient and his/her health information from all others
> 7.4 *User Identification* – Unique identification of the user of the health information system
> 7.6 *Type of Action (additions, deletions, changes, queries, print, copy)* – Granularity should be

[72] ASTM E2147-01 p. 1 (2009) reapproved with same language in (2013)
[73] Id.
[74] Id. p. 2
[75] Id.
[76] Id.
[77] Id.
[78] Id. at p. 3
[79] Id.
[80] Id.

> specific enough to clearly determine if data designated by federal and state law as requiring special confidentiality protection has been accessed. Specific category of data content, such as demographics, pharmacy data, test result, and transcribed note type, should be identified.[81]
> Understanding the information, E21470-01 Section 8 addressed disclosure of the log content.

Legal Disclosure, addressed in section 8.2, requested court docket number, names of the parties, the name and location of the court where the proceeding is held, and a description of the documents provided.[82] And under Section 9, on-demand reports to patients should be available and provided.[83] It specifically states, in that section, that an audit log should be able to be used to determine for a given patient, the users who viewed the data including their identity, the date/time of access, etc.[84]

The Secretary further requires that, in order to obtain general certification criteria, all EHRs and EHR Modules must contain audit logs that record actions related to electronic health information including date, time, patient identification, and user identification when the information is created, modified, accessed, or deleted; and which action occurred and by whom.[85] The EHRs and EHR Modules shall enable a user to generate an audit log for a specific time period and to sort entries in the audit log.[86] Further, the EHRs and EHR Modules must have the ability to detect the alteration of audit logs and verify that the person seeking access to the electronic health information is the one claimed and is authorized.[87]

The Secretary additionally required, for certification criteria for Complete EHRs and EHR Modules,[88] authentication, access control, authorization, auditable events, tamper-resistance, and audit reports.[89] It requires notification regarding whether and when an entity disabled the audit log.[90] Even if

[81] Id. at p. 4
[82] Id.
[83] Id. at p. 5
[84] Id.
[85] 45 C.F.R. 170.302(r)(1)
[86] 45 C.F.R. 170.302(r)(2)
[87] 45 C.F.R. 170.302(s)(3); 45 C.F.R. 170.302(t)
[88] 45 C.F.R. 170.302 was general certification criteria; 45 C.F.R. 170.314 is certification criteria
[89] 45 C.F.R. 170.314(d)(1)(2) and (3)
[90] 45 C.F.R. 170.314(d)(2)(i)(B)

the entity disables the audit log, the EHRS and Modules require the applicable technology to record the audit log status (enabled or disabled) and continue to record the exact date and time of access events and exit event and the unique identification of the user of the health information system.[91] The EHRs and Modules must enable a user to create an audit report for a specific time period and to sort entries.[92] In order to verify that electronic health information has not been altered, the EHRs and Modules must allow for the creation of a message digest.[93]

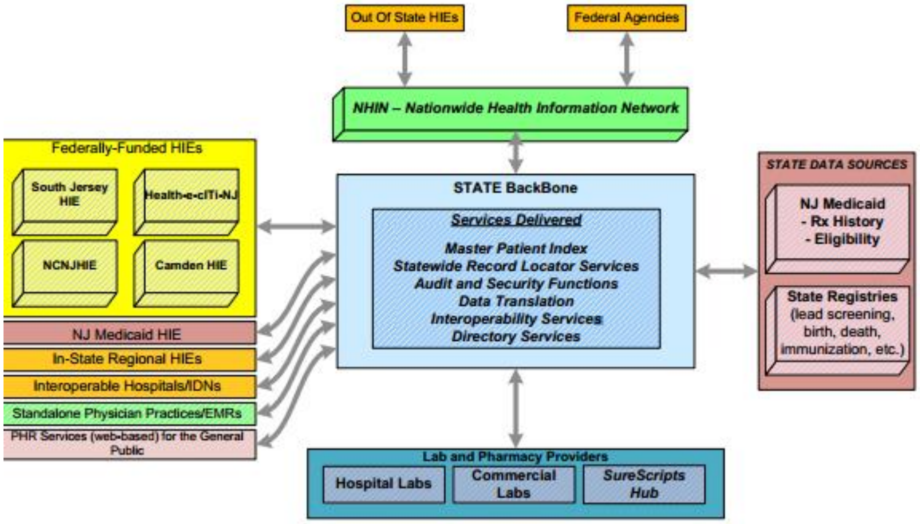
Audit trails are data specifically created and recorded by a health care provider during the provision of health care to an individual. “The term ‘standard’ means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with regard to the data element or transaction under 1320d-1 through 1320d-2 of [the Public Health and Welfare].”[94] All standards shall apply to a health care provider who transmits any health information in electronic form.[95]

Protected health information means individually identifiable health information transmitted by electronic media or maintained in electronic media.[96] An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set.[97] The covered entity must permit the individual to request access or obtain a copy of the protected health information and the covered entity must act no later than 30 days after receipt of the request.[98] The entity is allowed only one extension of time for no more than 30 additional days of they explain the reasons in writing for

[91] 45 C.F.R. 170.314(d)(2)(i)(B)
[92] 45 C.F.R. 170.314(d)(3)
[93] 45 C.F.R. 170.314(d)(8)(i)
[94] 42 U.S.C. 1320d(7)
[95] 42 U.S.C. 1320d-1
[96] 45 C.F.R. 160.103
[97] 45 C.F.R. 164.524
[98] 45 C.F.R. 164.524(b)

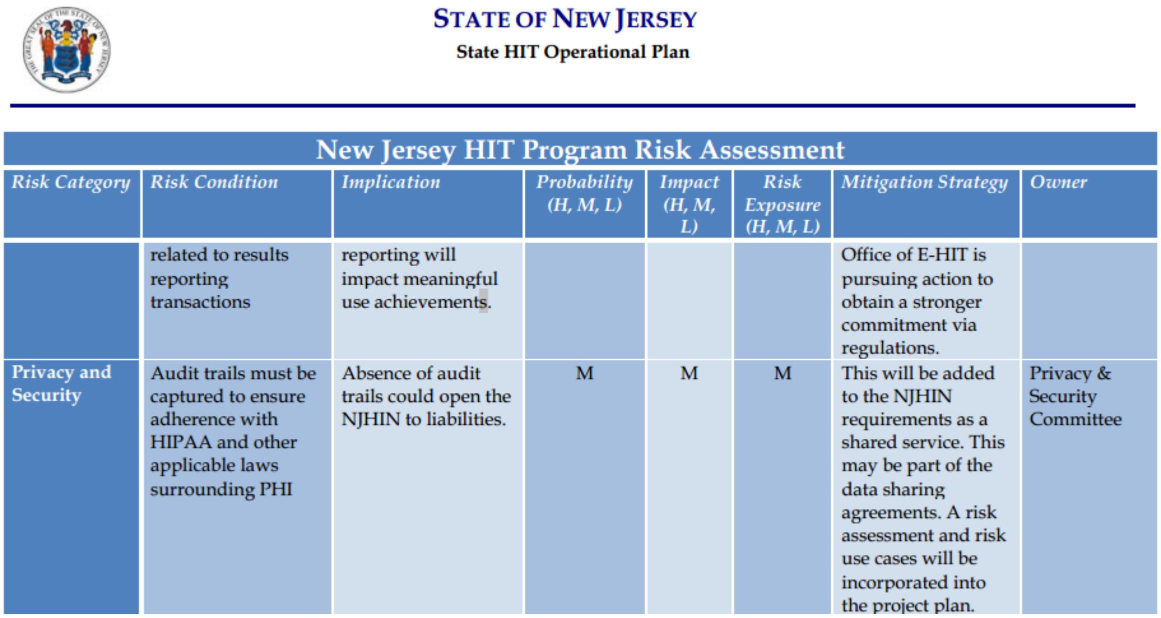
the delay.[99] The entity must provide access **in the form and format** requested by the individual.[100] If requested in electronic format and it the record is maintained in electronic format, the covered entity must provide the individual with access to the protected health information in the electronic form and format, if it is readily producible; or, if not, in a readable electronic form an format as agreed to by the entity and the individual.[101]

New Jersey's Plan for Health Information Technology and the State HIT Operation Plan both required implementation of Audit Trail and Node Authentication (ATNA) which establishes security measures which provide patient information confidentiality, data integrity, and user accountability.[102] The Audit Trail and Node Authentication will provide an audit records about who has accessed patient records.[103] As demonstrated in Figure 1.1, Audit and Security Functions will be part of the State's Backbone of services delivered in the New Jersey Health Information Network.[104]



As with the Federal Plan, the New Jersey Plans makes audit trails are mandatory.

[99] 45 C.F.R. 164.524(b)(2)(ii)
[100] 45 C.F.R. 164.524(c)(2)(i)
[101] 45 C.F.R. 164.524(c)(2)(ii)
[102] Id. pp. 63, 71, and 136. New Jersey Plan for Health Information Technology, October 16, 2009, at pp. 136
[103] State HIT Operational Plan of August 13, 2010 containing December 2010 Updates at p 136.
[104] Id. at p. 11, Figure 1.1 New Jersey Health Information Network (NJHIN)



STATE OF NEW JERSEY
State HIT Operational Plan

New Jersey HIT Program Risk Assessment

Risk Category	*Risk Condition*	*Implication*	*Probability (H, M, L)*	*Impact (H, M, L)*	*Risk Exposure (H, M, L)*	*Mitigation Strategy*	*Owner*
	related to results reporting transactions	reporting will impact meaningful use achievements.				Office of E-HIT is pursuing action to obtain a stronger commitment via regulations.	
Privacy and Security	Audit trails must be captured to ensure adherence with HIPAA and other applicable laws surrounding PHI	Absence of audit trails could open the NJHIN to liabilities.	M	M	M	This will be added to the NJHIN requirements as a shared service. This may be part of the data sharing agreements. A risk assessment and risk use cases will be incorporated into the project plan.	Privacy & Security Committee

As part of that plan, the New Jersey Health Information Network (NJHIN) is governed by the New Jersey Department of Health and Human Services (NJDHSS). One of the things monitored is the mandatory maintaining of “Patient Metadata for purposes of public health and quality purposes (e.g. Public Health objectives, Evidence-Based Analysis) and PHR use.”[105]

In New Jersey, additional auditing data is collected. A program of continuous quality improvement for medical records is required to be integrated into the hospital’s continuous quality improvement program and includes regularly collecting and analyzing data.[106] “Access, authentication, audit, and authorization refer to activities within [New Jersey’s] Collaborative that describe how participants are defined and identified as individual users of the system; how the usage of the system is governed; how users are accurately and appropriately identified; and how records of that usage are captured, stored, and used for carious audit purposes. [New Jersey’s] approach to these vitally important attributes to any data exchange efforts are to enforce our individual member policies with

[105] Id. at 69, See NJHIM – Figure 9.2 New Jersey Health Information Network (NJHIN) Vision – Detail View
[106] N.J.A.C. 8:43G-15.7

strict adherence…"[107] "This means that audit logs will be available and stored centrally at the network level, including detailed information about the type of data accessed, by whom, and when."[108]

[107] New Jersey Plan for Health Information Technology, October 16, 2009, at p. 41, Legal and Policy
[108] Id.