Hospital Committee Staff

Ze-Emanuel Hailu, *Senior Legislative Counsel*

Emily Balkan, *Senior Legislative Policy Analyst*

Lauren Hunt, *Finance Analyst*

Committee on Technology

 Irene Byhovsky, *Legislative Counsel*

Charles Kim, *Legislative Policy Analyst*
Sebastian Bacchi, *Finance Analyst*

Florentine Kabore, *Finance Analyst*



## THE COUNCIL

**Briefing paper OF THE HUMAN SERVICES Division
AND the Infrastructure Division**

*Jeffrey Baker, Legislative Director*

*Andrea Vazquez, Deputy Director, Human Services Division*

*Terzah Nasser, Deputy Director, Infrastructure*

**COMMITTEE ON HOSPITALS**

*Hon. Carlina Rivera, Chair*

**COMMITTEE ON TECHNOLOGY**

*Hon. Robert Holden, Chair*

#### **November 20, 2019**

**Oversight: Electronic Health Records**

**I.** **Introduction**

On November 20 2019, the Committee on Hospitals, chaired by Council Member Carlina Rivera, and the Committee on Technology, chaired by Council Member Robert Holden will hold a hearing on Electronic Health Records (“EHRs”). The Committees plan to discuss the use of EHRs in the City’s hospitals as well as their general safety. Witnesses invited to testify include representatives from Health and Hospitals (H+H), community-based organizations, and advocates.

**II. Background**

*EHRs*

An EHR is a digital version of a patient’s typical paper chart, which can include medical and treatment histories as well as additional, broader information, allowing for a more complete picture of the patient.[[1]](#footnote-2) For example, EHRs can include a patient’s treatment plans, allergies, lab test results, and detailed medical history.[[2]](#footnote-3) Due to the nature of EHRs, they allow the patient’s information to be updated in real-time and accessible instantly to authorized users.[[3]](#footnote-4)

By making medical information more available, easier to read, and portable, EHRs have changed the way medicine is delivered and our health care system itself.[[4]](#footnote-5) EHRs were initially developed and used at academic inpatient and outpatient medical facilities as early as 1971, and oftentimes were incomplete and still necessitated the use of paper records.[[5]](#footnote-6) Over time, as technology advanced and became more widely utilized, EHRs became more and more popular, and are now widely utilized.[[6]](#footnote-7) In 2009, 46 percent of the public reported that their health provider usually entered their health information into a computer-based medical record.[[7]](#footnote-8) By 2019, that number almost doubled to 88 percent.[[8]](#footnote-9) Although EHRs have advanced greatly, they raise technical, procedural, ethical, and other issues.[[9]](#footnote-10)

*EHR’s Impact on Patients and their Health*

The public’s perceptions of EHRs have changed over the years.[[10]](#footnote-11) A large proportion of individuals whose physician uses an electronic health record report that their quality of care and their interactions with their physician were “better” because of the EHR (45 percent and 44 percent, respectively); however, similar shares (47 percent, both) say the quality of care they receive and their interactions with their physician have “stayed the same.”[[11]](#footnote-12) Few say that EHRs have made the quality of care they receive or their interactions with their physician “worse” (six percent and seven percent, respectively).[[12]](#footnote-13)

Despite nearly half of the public feeling as if their care was improved, over half reported feeling “very concerned” or “somewhat concerned” about their EHR’s accessibility to unauthorized persons.[[13]](#footnote-14) Additionally, nearly half reported feeling “very concerned” or “somewhat concerned” of errors in their personal health information that can lead to negative impacts on their health care.[[14]](#footnote-15) In fact, 1 in 5 individuals say that they or a family member had already noticed an error in their EHR.[[15]](#footnote-16) Furthermore, doctors and patients alike have felt the change of using electronic medical records (“EMRs”) during meetings and treatments, with doctors oftentimes needing to stare at a screen instead of interacting face-to-fact with their patients.[[16]](#footnote-17)

Although EHRs have greatly improved medical billing and physician compliance measurements, studies have argued that they have yet to show that they improve patient health.[[17]](#footnote-18) In fact, one study found “significant differences in rates of mortality, readmission, and complications between patients at hospitals with full EHRs or partial EHRs compared to hospitals with no EHRs. However, these differences did not hold when adjusted for patient and hospital factors. Furthermore, the effect of EHR adoption was not associated with improved patient outcomes (specifically inpatient mortality, readmissions, and complications).”[[18]](#footnote-19) Another study found that, while EHRs could generate reports, those reports did not necessarily support quality improvement initiatives, and current EHR measurement functionality may be insufficient to support federal initiatives that tie payments to clinical quality measures.[[19]](#footnote-20)

*Cybersecurity of Medical Data*

*The importance of medical data and its vulnerabilities.*

An Internet connection is a necessity to conduct many online activities in hospitals that involve protected health information. Exchanging patient information electronically, submitting claims electronically, generating electronic records for patients’ requests, and e-prescribing are all examples of online activities that require cybersecurity practices to safeguard systems and information.[[20]](#footnote-21)

It has been estimated that over the past three years, 40 percent of all data breaches in the United States came from the healthcare industry.[[21]](#footnote-22) Medical datais one of the most desirable forms of information on the black market making the industry a growing target.[[22]](#footnote-23) As part of their day-to-day operations, hospitals collect and store vast amounts of personal information, making them a major target for cyber-criminals.[[23]](#footnote-24)

This valuable data can be, among other things, used for identity theft.[[24]](#footnote-25) In the United States, stolen personal health insurance information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid.[[25]](#footnote-26) Medical data breaches are especially serious because this personal data can, in some cases, mean the difference between life and death.[[26]](#footnote-27) For example, it could cause medications to become mixed up – or people might fail to get treatment for conditions such as diabetes.[[27]](#footnote-28)

A breach of medical data often causes greater harm in the future than in the present, with little to no recourse for its victims.[[28]](#footnote-29) Firstly, victims are generally unable to sue for these future harms as at the time of the incident, or filing of a lawsuit, as there was no injury in fact.[[29]](#footnote-30) Additionally, potential financial harm becomes a constantly looming threat, as victims now have the overwhelming task of monitoring when their compromised data will be used for harmful purposes.[[30]](#footnote-31) Therefore, protecting medical data from cyber-attacks or unauthorized disclosure should be essential for hospitals’ IT departments.

*HIPAA, HITECH, and Cybersecurity/Privacy Protection*

The Health Insurance Portability and Accountability Act (“HIPAA”) was enacted in 1996 “to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.”[[31]](#footnote-32) HIPPA has two main objectives.[[32]](#footnote-33) The first objective, “Health Insurance Portability,” aimed to ensure that individuals would be able to maintain their health insurance between jobs.[[33]](#footnote-34) The second objective, “Accountability,” aimed to ensure the security (“Security Rule”) and confidentiality of patient data (“Privacy Rule”).[[34]](#footnote-35)

 The Office for Civil Rights (“OCR”) is responsible for enforcing the HIPAA Privacy and Security Rules.[[35]](#footnote-36) One of the ways that the OCR carries out this responsibility is investigating complaints. If a complaint describes an action that could be a violation of the criminal provision of HIPAA,[[36]](#footnote-37) the OCR may refer the complaint to the Department of Justice or Attorneys General[[37]](#footnote-38) for investigation.

HIPAA imposes a penalty on the covered entity, not the attacker. The penalty for violation is a fine of “up to $50,000, a one-year term of imprisonment or both,”[[38]](#footnote-39) or "if the offense is committed under false pretenses," the fine is "not more than $100,000,”[[39]](#footnote-40) imprisonment for up to 5 years, or both.[[40]](#footnote-41) "If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," the violator may "be fined not more than $250,000, imprisoned not more than 10 years, or both."[[41]](#footnote-42)

While HIPAA began the campaign to increase the privacy and security of medical records, it was the Health Information Technology for Economic and Clinical Health (“HITECH”) Act—passed as Title XIII of the American Recovery and Reinvestment Act of 2009—which primarily focused on EMRs.[[42]](#footnote-43) Among a variety of provisions, HITECH directed the Office for Civil Rights of the United States Department of Health and Human Services (“HHS”) to promulgate further regulations to expand and incentivize EMRs.[[43]](#footnote-44) The rapid expansion created more privacy and security issues,prompting HHS to roll out firmer regulations for “covered entities” and their “business associates.”[[44]](#footnote-45)

Despite increased awareness and guidelines on the issue, cybersecurity continues to be a problem for the healthcare industry. In 2015 alone, 113 million electronic health records were compromised, and in 2016, the industry has averaged 4 reportable data breaches per week.[[45]](#footnote-46) The U.S. Department of Health and Human Services reports that in the last 24 months there have been 550 data breaches, with 47,197,424 individuals affected.[[46]](#footnote-47) Thirty of them took place in New York State, and 13 took place in the City of New York, affecting 450,744 individuals.[[47]](#footnote-48) These data breaches include Mount Sinai Hospital.[[48]](#footnote-49) According to the same source, about 106 data breaches in healthcare settings affecting 2,843,316 individuals have been reported since August 2018.[[49]](#footnote-50)

 In New York City, HSS has issued [HIPAA enforcement action](http://www.hhs.gov/news/press/2014pres/05/20140507b.html), entering settlements totaling $4.8 million[[50]](#footnote-51) with two New York organizations tied to the same 2010 [breach](https://www.healthcareinfosecurity.com/breach-response-c-324), New York and Presbyterian Hospital and Columbia University. The incident, which involved unsecured patient data on a network, affected about 6,800 patients.[[51]](#footnote-52)

*EHR Use at H+H*

On January 16, 2013, H+H entered into a 15-year, $302 million contract agreement with Epic Systems Corporation (Epic Systems) to replace H+H’s then-20-year-old EMR system.[[52]](#footnote-53) Epic Systems develops EHRs and currently covers more than 250 million patients.[[53]](#footnote-54) H+H aims to have Epic used at all of their patient care facilities, including 11 hospitals, 4 long-term care facilities, 6 diagnostic treatment centers, and more than 70 community-based clinics.[[54]](#footnote-55) H+H hopes to have Epic at every site by the end of 2019.[[55]](#footnote-56) H+H has discussed Epic at multiple Council hearings, such as a hearing in November 2018, where H+H testified that they are transforming their Epic systems to better meet the needs of those who are transgender and gender non-conforming (TGNC).[[56]](#footnote-57)

H+H’s Enterprise Information Technology Services (EITS) group is responsible for implementing Epic throughout all H+H sites.[[57]](#footnote-58) An audit performed by New York City Comptroller Scott M. Stringer found that, although EITS maintains a 24-hour, 7-days-per-week, agency-wide helpdesk facility to support users in need of technical assistance, the average time frames in which it resolved higher-priority service-restoration issues affecting the Epic EHR at Elmhurst Hospital significantly exceeded its own targets.[[58]](#footnote-59)

**IV. CONCLUSION**

The Committees look forward to hearing testimony from H+H, advocacy groups, community-based non-profit organizations, and other interested members of the public. The Committee hopes to learn more about the Epic roll out at H+H, specifically how the roll-out has progressed, how they see Epic helping with care quality, and how they plan to keep their EHRs secure.

1. *What is an Electronic Health Record* *(EHR)?,* The Office of National Coordinator for Health Information Technology (ONC), September 10, 2019, available at <https://www.healthit.gov/faq/what-electronic-health-record-ehr>. [↑](#footnote-ref-2)
2. *Id.* [↑](#footnote-ref-3)
3. *Id.* [↑](#footnote-ref-4)
4. R. S. Evans, *Electronic Health Records: Then, Now, and in the Future*, Yearb Med Inform, 2016; (Suppl 1): S48–S61, Published online 2016 May 20, doi: 10.15265/IYS-2016-s006, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5171496/> (hereinafter Evans). [↑](#footnote-ref-5)
5. *Id.* [↑](#footnote-ref-6)
6. *Id.* [↑](#footnote-ref-7)
7. Munana, C., et al., *Data Note: Public’s Experiences With Electronic Health Records,* Kaiser Family Foundation, March 18, 2019, available at <https://www.kff.org/other/poll-finding/data-note-publics-experiences-with-electronic-health-records/> (hereinafter Munana). [↑](#footnote-ref-8)
8. *Id.*  [↑](#footnote-ref-9)
9. Evans, *supra* note 4. [↑](#footnote-ref-10)
10. Munana, *supra* note 7. [↑](#footnote-ref-11)
11. *Id.* [↑](#footnote-ref-12)
12. *Id.*  [↑](#footnote-ref-13)
13. *Id.*  [↑](#footnote-ref-14)
14. *Id.*  [↑](#footnote-ref-15)
15. *Id.*  [↑](#footnote-ref-16)
16. Ofri, D., *The EMR has changed the doctor-patient duet into a menage-a-trois*, STAT News, October 31, 2019, available at <https://www.statnews.com/2019/10/31/emr-changed-doctor-patient-duet-into-menage-a-trois/?utm_source=STAT+Newsletters&utm_campaign=dadf2f9acd-MR_COPY_02&utm_medium=email&utm_term=0_8cab1d7961-dadf2f9acd-151778981>. [↑](#footnote-ref-17)
17. Yanamadala, S., et al., *Electronic Health Records and Quality of Care: An Observational Study Modeling Impact on Mortality, Readmissions, and Complications*, Medicine (Baltimore), 2016 May; 95(19): e3332, published online 2016 May 13, doi: 10.1097/MD.0000000000003332, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4902473/>. [↑](#footnote-ref-18)
18. *Id.*  [↑](#footnote-ref-19)
19. Cohen, D., et al., *Primary Care Practices’ Abilities And Challenges In Using Electronic Health Record Data for Quality Improvement*, HealthAffairs, April 2018, available at <https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.2017.1254>. [↑](#footnote-ref-20)
20. Guide to Privacy and Security of Electronic Health Information, Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity, <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-4.pdf>. [↑](#footnote-ref-21)
21. Addressing Gaps in *Cybersecurity*: OCR Releases Crosswalk Between *HIPAA* Security Rule and NIST *Cybersecurity*Framework, U.S. DEP'T. OF HEALTH & HUMAN SERVS, Feb. 23, 2016, <http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/>. [↑](#footnote-ref-22)
22. *6 Reasons Why Healthcare is the Biggest Target for Cyberattack*, SWIVELSECURE, <https://swivelsecure.com/us/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/>. [↑](#footnote-ref-23)
23. #  [Kate O'Flaherty](https://www.forbes.com/sites/kateoflahertyuk/), *Why Cyber-Criminals Are Attacking Healthcare -- and how to Stop Them*, October 5, 2018, <https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#4a2c96167f69>.

 [↑](#footnote-ref-24)
24. *Id.* [↑](#footnote-ref-25)
25. *Id*. [↑](#footnote-ref-26)
26. *Id.* [↑](#footnote-ref-27)
27. *Id.*  [↑](#footnote-ref-28)
28. Farai Chideya, Data Theft Today Poses Indefinite Threat of “Future Harm”, THE INTERCEPT, June 12, 2015, <https://theintercept.com/2015/06/12/data-breach-threat-of-future-harm>. [↑](#footnote-ref-29)
29. Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138 (2013). [↑](#footnote-ref-30)
30. Ryan L. Garner, *Evaluating Solutions to Cyber Attack Breaches of Health Data: How Enacting A Private Right of Action for Breach Victims Would Lower Costs*, 14 Ind. Health L. Rev. 127, 133 (2017); Farai Chideya, Data Theft Today Poses Indefinite Threat of “Future Harm”, THE INTERCEPT, June 12, 2015, <https://theintercept.com/2015/06/12/data-breach-threat-of-future-harm>; see also [*Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013)](https://1.next.westlaw.com/Link/Document/FullText?findType=Y&serNum=2029935439&pubNum=0000708&originatingDoc=I8f2feb09b4a311e79bef99c0ee06c731&refType=RP&originationContext=document&transitionType=DocumentItem&contextData=(sc.Search)). [↑](#footnote-ref-31)
31. Health Insurance Portability and Accountability Act of 1996, 1996 Enacted H.R. 3103, 104 Enacted H.R. 3103, 110 Stat. 1936. [↑](#footnote-ref-32)
32. HIPAA *Background*, U. CHI., 1, 1, Oct. 23, 2006, <http://hipaa.bsd.uchicago.edu/hipaa_background_20070122.pdf>. [↑](#footnote-ref-33)
33. *Id.* [↑](#footnote-ref-34)
34. *Id*. [↑](#footnote-ref-35)
35. 45 C.F.R. Parts 160 and 164, Subparts A, C, and E. [↑](#footnote-ref-36)
36. 42 U.S.C. 1320d-6. [↑](#footnote-ref-37)
37. *See* Danielle Keats Citron, *Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law*, University Of Maryland Francis King Carey School Of Law, Legal Studies Research Paper, No.2016–8, February 2016. [↑](#footnote-ref-38)
38. 42 U.S.C. § 1320d-6(b)(1). [↑](#footnote-ref-39)
39. *Id.* § 1320d-6(b)(2). [↑](#footnote-ref-40)
40. *Id.* § 1320d-6(b)(3). [↑](#footnote-ref-41)
41. *Id.* § 1320d-6(b)(3). [↑](#footnote-ref-42)
42. Office of the Assistant Secretary for Planning and Evaluation, *EHR Payment Incentives for Providers Ineligible for Payment Incentives and Other Funding Study Appendices*, U.S. Department of Health & Human Services, June 1, 2013, <https://aspe.hhs.gov/basic-report/ehr-payment-incentives-providers-ineligible-payment-incentives-and-other-funding-study-appendices>. [↑](#footnote-ref-43)
43. *Id*. [↑](#footnote-ref-44)
44. Ryan L. Garner, *Evaluating Solutions to Cyber Attack Breaches of Health Data: How Enacting A Private Right of Action for Breach Victims Would Lower Costs*, 14 Ind. Health L. Rev. 127, 135–36 (2017). [↑](#footnote-ref-45)
45. Nsikan Akpan, *Has health care hacking become an epidemic?,* PBS (Mar. 23, 2016, 6:19 PM), <http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/>; Connor McLarren, *Once More Unto the Breach: How the Growing Threat of Ransomware Affects HIPAA Compliance for Covered Entities*, 15 Ind. Health L. Rev. 305, 330 (2018). [↑](#footnote-ref-46)
46. U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>. [↑](#footnote-ref-47)
47. *Id.* [↑](#footnote-ref-48)
48. *Id.* [↑](#footnote-ref-49)
49. *Id*; Sammy Caiola, *California Hospital Hacks Reveal Weak Links in Health Cybersecurity*, The Sacramento Bee, April 5, 2016, <http://www.sacbee.com/news/local/health-and-medicine/article70113852.html#storylink=cpy>. [↑](#footnote-ref-50)
50. New York and Presbyterian Hospital (NYP) has agreed to pay OCR $3,300,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, and will adopt a corrective action plan to evidence their remediation of these findings. Columbia University (CU) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, including a $1,500,000 monetary settlement and corrective action plan to address deficiencies in its HIPAA compliance program. [↑](#footnote-ref-51)
51. *See* RESOLUTION AGREEMENT between the United States Department of Health and Human Services, Office for Civil Rights (“HHS”) and The New York and Presbyterian Hospital (NYP) dated April 20, 2014, <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf>. [↑](#footnote-ref-52)
52. *Audit Report on the Epic Electronic Medical Record System That NYC Health + Hospitals Implemented at the Elmhurst Hospital Center*, New York City Comptroller Scott M. Stringer, January 31, 2018, available at <https://comptroller.nyc.gov/reports/audit-report-on-the-epic-electronic-medical-record-system-that-nyc-health-hospitals-implemented-at-the-elmhurst-hospital-center/> (hereinafter Audit Report). [↑](#footnote-ref-53)
53. *In a nutshell,* Epic System, available at <https://www.epic.com/about> [↑](#footnote-ref-54)
54. *Audit Report, supra* note 52. [↑](#footnote-ref-55)
55. Hearing Transcript, September 18, 2019, available at [file:///C:/Users/EBalkan/Downloads/Hearing%20Transcript%20(5).pdf](file:///C%3A%5CUsers%5Crdelfranco%5CAppData%5CLocal%5CMicrosoft%5CEBalkan%5CAppData%5CLocal%5CMicrosoft%5CEBalkan%5CAppData%5CLocal%5CMicrosoft%5CEBalkan%5CDownloads%5CHearing%20Transcript%20%285%29.pdf). [↑](#footnote-ref-56)
56. Hearing Transcript, November 2018, available at <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3721024&GUID=5ED77B87-4A4B-4E8F-B444-3D72F5550DCD&Options=&Search=> [↑](#footnote-ref-57)
57. *Audit Report, supra* note 52. [↑](#footnote-ref-58)
58. *Id.* [↑](#footnote-ref-59)