Author for correspondence:
Dr Claudine Murphy,
Department of Otolaryngology,
University College Hospital Galway,
Galway, Ireland
E-mail: claudinemurphy583@gmail.com

The evolution of the medical record from paper to digital: an ENT perspective

C Murphy [ORCID] and I J Keogh

Department of Otolaryngology, University College Hospital Galway, School of Medicine, National University of Ireland Galway, Galway, Ireland

Abstract

Objectives. A national electronic health record is being procured for Health Service Executive hospitals in Ireland. A number of hospitals have implemented an electronic document management system. This study aimed to investigate the efficiency and safety of the electronic document management system in our centre.

Methods. A retrospective audit was performed of patients operated on at Galway University Hospital. The availability and location of patients' admission data on the electronic document management system were recorded. These data were analysed using Microsoft Excel software, version 16.45.

Results. The records of 100 patients were analysed. The main findings were: 5 per cent of operation notes were missing, 80 per cent were in the incorrect section, while 15 per cent were in the correct 'procedure' section on the electronic document management system.

Conclusion. This study shows there is potential for error with 'paper-light' solutions, whereby delayed scanning, misfiling of scanned records and missing records may lead to significant delays in treatment and potential patient safety issues.

Introduction

Electronic health records are being implemented worldwide in a move towards a paperless future. Electronic health records have been recommended as a way to solve some of the many problems in healthcare systems.[1,2] Problems have been reported in the implementation of the electronic health record and the user-friendly capabilities, in the USA.[3,4] In Ireland, there is an action plan in place for all hospitals to be paperless or paper light in the next 10 years. Benefits of the electronic health record include improved communication and decision-making at the points of care, quick and available patient records at any time, and secured sharing of information with other clinicians. This promotes legible, complete documentation that helps with the coding and recording of patient information in order to better share and delegate resources. It should also reduce costs to the healthcare system by reducing the amount of paperwork and storage facilities. Ultimately, the aim would be to improve patient care and safety through a more efficient, user-friendly system.[5] In Ireland, an electronic document management system, Evolve, has been deployed across some hospitals as a step towards a fully integrated electronic health record.

Data breaches are incidents that erode the trust in the electronic health record and systems that manage it. They also prevent technological development, as they can cause large workloads in terms of overcoming the breaches and in improving security for these systems. In the USA, one study published in 2019 reported 2529 breaches, affecting 194.4 million individual records, from years 2010 to 2018. Hacking was responsible for 22.7 per cent of incidents in 2010, but this increased to 43.44 per cent in 2018. It is estimated that the cost of breaches can be up to $6.2 billion.[6]

There are two major problems that occur when a health system is hacked: the data breach and the downtime involved with the hack. A data breach has the obvious main issue that patients' information is being accessed by the hackers and could be used as ransom, as was the case in Ireland in May 2021. Downtime of the system causes unavailability of information, delayed care and duplicate care, and is, most importantly, a patient safety issue. Electronic document management systems and electronic health record systems must have downtime procedures to ensure continuity of care during network outages or cyberattacks. These include redundant parallel systems for renewed access, with layers of protection. For example, a designated downtime computer can be assigned to give 24-hour access to a protected system of information. This computer should have an independent, uninterruptible power source and, in the event of it being breached, be attached to a computer to print off all information as a record catch. This gives multiple layers of downtime protection.

In May 2021, there was a ransomware attack on the Health and Safety Executive of Ireland information technology (IT) systems, exposing a real-time vulnerability within our healthcare system. This data breach caused large-scale disruption across many hospitals. In our centre, the reliance on the electronic document management system

contributed to the cancellation of out-patient clinics, surgical procedures, diagnostic imaging and testing. It highlighted vulnerabilities in our IT systems that need to be addressed to prevent this happening. There was no downtime procedure implemented for the electronic document management system or many Health and Safety Executive systems during the cyberattack. When a hospital is operating at Healthcare Information and Management Systems Society ('HIMSS') stage 7 (the highest rating of the Analytics international Electronic Medical Record Adoption Model), business continuity capable of handling outages as short as 15 minutes is critical to enable safe care. As increasing proportions of the patient record become available in electronic format only, it is essential to consider business continuity as a core part of system rollouts. Ultimate clinical responsibility of patient outcomes lies with the treating physicians; therefore, it remains our ultimate responsibility to petition hospital management for safe and effective IT systems, to enable safe care.

In the USA, the electronic health record became widespread in 2015. This followed the signing of the Health Information Technology for Economic and Clinical Health ('HITECH') Act of 2009.[7] Ireland is a long way behind having a national electronic health record. Evolve is the electronic document management system platform that has been implemented in our centre. It has been rolled out in the National Children's Hospital, Dublin, and may be used in other hospitals in the future, towards a complete electronic health record. It uses a combination of integrated systems, with access to imaging, laboratory results and specialist test results. Clinical notes, including out-patient notes, procedure notes, anaesthetic records, nursing notes and administration notes to name a few, can be inputted electronically. However, predominantly handwritten clinical notes are scanned onto the record from a centre in Dublin. These notes should be filed into barcoded sections, before going to Dublin where they are scanned into the correct section. This process was supposed to take less than 3 days, but in reality can take up to 4 weeks. Delays in information availability and difficulties in finding the information can be problematic, and pose a potential risk for patients.

Materials and methods

A retrospective audit was performed on patients operated on between July and December of 2020. The operating theatre record was used to recruit patients into the audit. Each patient record was reviewed and the following data were noted: the procedure type, the availability of a letter scheduling the patient for theatre, a booking form, a relevant previous procedure note, a procedure note, and endoscopic imaging and audiology findings. The section they were filed in on the record was also noted. The results were analysed using Microsoft Excel® software, version 16.45.

Results

For this research project, 100 sequential patient records were analysed. All patients had undergone ENT surgical procedures. The availability and filing location of documents were recorded.

Five per cent of operation notes were not filed on the electronic health record. Eighty per cent of operation notes were filed in the incorrect section, while 15 per cent of operation notes were in the correct 'procedure' section. Fifty-four per cent of audiograms were unavailable on the electronic health record; 46 per cent of them were available, but only 28 per cent of these were in the correct 'clinical measurement' section.

Patients frequently undergo more than one otological procedure, and can include a planning examination under anaesthetic for a more complicated operation such as a mastoidectomy. Thirty-four patients were in this category. Sixty per cent of this patient group did not have planning operation notes in their electronic health record.

Ninety-five per cent of referral letters for surgery were available in the correct 'correspondence section' on the electronic health record.

Discussion

The electronic document management system Evolve was implemented in our centre in 2018 and is the planned system platform for more hospitals across the country. It works on a paper-light basis, rather than paperless. A patient is assigned a chart on admission to hospital or the out-patient clinic. Most documents are still handwritten and filed in sections until the patient is discharged. The chart is then sent to a scanning facility in Dublin and documents are scanned onto the electronic document management system. The staff who scan documents are trained to scan as per the section in which they are filed. Each section has a barcode; however, that is not the case for the pages in each section. For example, the procedure section has a barcode, but the actual blue operation note does not.

The results of this audit show that documents are not always in the correct section and are therefore being scanned into the wrong section in the electronic health record. This does not sound like a big problem, but it is often very difficult to find pertinent documents when preparing for a patient to be operated on. If this was an emergency situation soon after a procedure, it is likely the documents would not be available as they would be en route to, or in, the scanning centre. As time goes on, this will only become more difficult as more pages are scanned into this system. Missing documents was a major problem found with this audit. However, after some investigation, all were recovered either in the old 'legacy charts' or through the Evolve co-ordinators here in our centre.

The majority of referral letters or letters scheduling a patient for surgery were available and in the correct section in the electronic document management system. These letters are uploaded to the system once secretaries have typed the letters and they are 'closed' or signed off. This makes the upload into the electronic document management system more straightforward. However, there can be delays with these letters being typed. Delays in the scanning of documents have been reported, although none were recorded in this study. The danger of these missing or delayed documents is that if a patient was brought into hospital in an emergency or had a complication following surgery, these documents would not be available, whereas in the past they would have been in the patient's paper chart. If a patient's safety is breached, the responsibility will always come back on the surgeon, so it is in a surgeon's best interest to make sure end-user engagement is implemented as the move towards electronic health record takes hold into the future.

The aforementioned cyberattack caused significant disruption in our centre because of reliance on the new electronic health record among other things. Similarly, the unavailability of documentation made seeing patients and operating on them compromised by this significant disruption. Downtime systems should have been in place so that there was some way of accessing information.

The electronic health record should be efficient, intuitive and user-friendly. It should make healthcare workers' lives easier, make patients' hospital journey safer and reduce duplicate testing (which was frequent in the past). This audit was performed because, anecdotally, end users were finding the system difficult to use, and frequently commented on missing data. An electronic health record should be a digital application that can dynamically interact with users, enhance data gathering and analysis, and allow for quality improvement. Most importantly, it should improve patient safety. It should not be merely be a digitalised paper chart.[8]

In the USA, there have been issues with implementing electronic health records. Loss of test requests and issues with prescriptions are some of the problems that have been reported. There are different platforms across different hospitals, which can cause a disconnect in the system and confusion for users.[3] Anecdotally, some clinicians in the USA have complained that the introduction of increasingly complex IT systems and a lack of user-friendly design to the systems are tactics used by major healthcare organisations to confound clinicians and encourage disengagement with management.[9] Similarly, in Ireland, one electronic health record is not necessarily on the agenda for the future of all of the hospitals. This seems counter-intuitive when we are such a small country. Surely it would make more sense to implement one electronic health record system across all centres.

- This study highlights the challenges faced when implementing the electronic health record across Ireland's healthcare system
- End-user engagement is vital in the implementation; investment in cyber security and downtime systems should be strongly considered
- There is an opportunity for electronic health records across the health system in Ireland, but there is potential for error with 'paper-light' solutions
- Rapid access to operation records is critical in emergency re-admissions, and surgical follow up relies on operation record availability
- Quality improvement initiatives such as this could help troubleshoot and enhance the electronic health record roll-out
- Electronic document management system roll-out must be forward-compatible with electronic health record deployment, to ensure continuity of care

The cyberattack showed the country the importance of cyber security and the need for a downtime system if such an attack were to happen again. In 2017, the WannaCry ransomware attack on the National Health Service forced clinics to close and to refuse patient care.[10] Studies in the USA have shown that thousands of cyberattacks happened over the last decade. One study demonstrated that hacking was on the rise, while the other study found that hacking only made up 25 per cent of major data breaches but hacking was responsible for 85 per cent of all affected patient records over the study period.[6,7] Hacking can shut down health systems, leading to the standstill of healthcare activity. We saw this with the recent cyberattack on the Health and Safety Executive, which undoubtedly hindered patient care. The future will reveal more.

Conclusion

While it is totally acceptable that the introduction of new systems will have 'settling-in issues', this study highlights the challenges faced when implementing the electronic health record across our healthcare system. There must be end-user engagement throughout the process. When issues were raised, we found IT staff to be very helpful, anxious to troubleshoot and problem-solve if at all possible. Investment into cyber security and downtime systems should be a strong consideration in this process, and we can learn from the cyberattacks on health systems in the UK and USA to help advise on this. There is an opportunity to bring in a successful electronic health record across most of the health system in Ireland. This study highlights that quality improvement initiatives such as this could aid in troubleshooting and enhancing the electronic health record in its roll-out over the coming years.

To conclude, appropriate maintenance of patient safety with multidisciplinary end user engagement is essential throughout this process. Clinicians need to be able to express their concerns, so that any patient safety issues can be highlighted and solved early. Furthermore, any electronic document management system implementation must be forward-compatible with future full electronic health record deployments, to ensure continuity of care.

References

1 Institute of Medicine. *Computer-Based Patient Record: An Essential Technology for Health Care*. Washington, DC: National Academies Press, 1991; 209

2 Hillestad R, Bigelow J, Bower A, Girosi F, Meili R, Scoville R *et al.* Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Aff* (*Millwood*) 2005;**24**:1103–17

3 Fry E, Schulte F. Death by a thousand clicks: where electronic health records went wrong. *Fortune*, 18 March 2019

4 Gorn D. These doctors think electronic records are hurting their relationships with patients. *PBS News*, 21 July 2017

5 HealthIT.gov. What are the advantages of electronic health records? In: https://www.healthit.gov/faq/what-are-advantages-electronic-health-records [18 December 2022]

6 Hossain MM, Hong YA. Trends and characteristics of protected health information breaches in the United States. *AMIA Annu Symp Proc* 2020;**2019**:1081–90

7 Ronquillo JG, Winterholler JE, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open* 2018;**1**:15–19

8 Janett RS, Yeracaris PP. Electronic medical records in the American health system: challenges and lessons learned. *Cien Saude Colet* 2020;**25**:1293–304

9 The Heath Care Blog. How to Discourage a Doctor. In: https://thehealthcareblog.com/blog/2014/09/18/how-to-discourage-a-doctor/ [18 December 2022]

10 Clarke R, Youngstein T. Cyberattack on Britain's National Health Service - a wake-up call for modern medicine. *N Engl J Med* 2017;**377**:409–11