Chapter 17
Enhancing Clinical Performance and Improving Patient Safety Using Digital Health

Mitchell G. Goldenberg and Teodor P. Grantcharov

Abstract Patient confidentiality has remained a central issue in the current "big data" era of healthcare. Protections such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) exist to ensure that digital personal health information (PHI) are legally secure from threats and breaches that would threaten confidentiality. To be compliant with HIPAA regulations, steps must be taken by health care providers and digital health platforms, and these fall under the Privacy Rule, which outlines appropriate uses and disclosures of PHI, and the Security Rule, which lays out with granularity the steps that must be taken to adhere to the HIPAA regulations. Through deliberate design of secure digital health platforms, we can use technological advances in the collection, measurement, and delivery of health care to advance care and improve patient safety. Renewed efforts to optimize and standardize health care delivery has facilitated the implementation of electronic and digital health solutions that benefit medical and surgical training and efficiency while minimizing harm to patients. Cross-industry innovations such as the OR Black Box® will allow us to accomplish these lofty goals. Finally, we must strive to include patients in this digital health movement, as now more than ever we can create knowledge translation solutions that ensure that patients understand their health in a meaningful way.

Keywords Digital health • Patient privacy • Black box • Patient safety • Surgical technology

M.G. Goldenberg, M.B.B.S. • T.P. Grantcharov, M.D., Ph.D., F.A.C.S. (✉)
International Centre for Surgical Safety, Keenan Centre for Biomedical Science,
St. Michael's Hospital, University of Toronto, Toronto, Canada
e-mail: grantcharovt@smh.ca

H. Rivas, K. Wac (eds.), *Digital Health*, Health Informatics,
https://doi.org/10.1007/978-3-319-61446-5_17

17.1 What Is the Health Insurance Portability and Accountability Act?

As the world of modern healthcare continues to move toward the use of “Big Data” to guide research and policy-making, it is imperative that systems are developed to not only facilitate analysis of multiplatform data on a large scale, but also ensure that this confidential patient information is kept secure in its transfer and storage. With the introduction of widespread electronic health records (EHR) use in most contemporary health care settings, there has been a subsequent explosion in the availability of raw population-level data (Services DOHAH 2012). The EHR captures demographic, economic, and outcomes-based information, and this heterogeneity has driven stakeholders to create novel and robust methods of analysis that can account for this inherent diversity (Murdoch and Detsky 2013). The concept that Big Data can be used as a measure of healthcare delivery quality is embodied by the National Surgical Quality Improvement Program (NSQIP), (Berwick 2015) which uses a collation of EHR data from 400 United States hospitals in particular to measure hospital outcomes in patient safety. Big Data also has the potential to be used as a means of creating standards in the prevalence of patient morbidity, by accounting for case-mix variation at a hospital-by-hospital level (Bohnen et al. 2016). The use of large-scale, real-world information to drive decision making is important in health care, and this chapter will discuss both the use of clinical data in quality improvement, as well as measures in place to protect its use. We will begin by discussing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implications in the growing field of digital health.

The HIPAA was passed as a two-part Act of The United States Congress, signed by President Bill Clinton in 1996. The second part of the bill, known as the Administrative Simplification (AS) provisions, created a mandate for the Department of Health & Human Services (HHS) to create privacy and security laws regarding the use and transmission of personal health information (PHI) in clinical medicine and research (Nass et al. 2009). The AS provisions contain two primary ‘rules’ which concern the protection of health data. The first of these, termed *Standards for Privacy of Individually Identifiable Health Information*, or “Privacy Rule” is a set of published standards relating to the disclosure of sensitive patient information (Services UDOHAH 2013). It functions to prevent the disclosure of confidential information by what are called “covered entities,” which includes any group that takes part in transactions of PHI (healthcare providers, medical insurers, etc.). It instructs these groups to monitor and ensure that only appropriate employees have access to patient’s PHI, and that any disclosures made are as minimal as possible, and only with the patient’s consent (Naam and Sanbar 2015; Register 2010). This same rule outlines the exceptions to confidentiality in the United States, for example child abuse and missing person’s cases. It further seeks to give the individual control and notice regarding the use and distribution of one’s PHI. The second rule outlined by the AS provisions is the *Security Standards for the Protection of Electronic Protected Health Information”*, also called the “Security Rule.” This rule relates to the storage and protection of electronic PHI, and serves to standardize security measures around EHR use (Services UDOHAH 2013). Under the security rule, covered entities must maintain the confidentiality, integrity and availability of electronic medical data, and safeguard it against "reasonably anticipated" threats or breaches. It further mandates the need for ongoing risk analysis and management, stating that, "a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to electronic PHI (Services UDOHAH 2013)." It also puts forward specific types of protective safeguards that should be employed by a covered entity, including administrative, physical, and technical safeguards. Enforcement of the Security rule is through the Office for Civil Rights (OCR), which is responsible for prosecuting any violations set out in the HIPAA (Stevens 2003). If one's confidentiality is breached by a covered entity, they do not sue the entity based on the HIPAA, rather, they must file a complaint with the OCR in order to trigger an investigation (Nass et al. 2009).

Further action came in 2009, when the Health Information Technology for Economic and Clinical Health Act (HITECH) was passed under the American Recovery and Reinvestment Act. The HITECH contains four "Subtitles," including Subtitle D, a section covering further confidentiality and security regulations around EHR use (Firm 2013). In addition to updating the civil and criminal penalties around breaching PHI, new rules around disclosing a breach in PHI were also implemented, with the HHS issuing guidance around the specifics of keeping information protected to HIPAA levels (Firm 2013). The 2009 update also included rules for "business associates," or those individuals who while not being part of the covered entity, are given access to the data for consultancy purposes. Examples of a business associate as cited by the HHS include a lawyer working for a health plan, or a third party medical transcriptionist (Services UDOHAH 2013). Also included as business associates are those who use eHealth applications or wearable technology (Institute of Medicine (US) Committee 2003). However, not all mobile health applications are covered by HIPAA, including those that collect behavioral and psychometric data from users (Glenn and Monteith 2014). It is important therefore for consumers to understand what the data they provide to third-party software can be used for, including advertising purposes.

17.2 What Makes a Digital Health Platform HIPAA Compliant?

In order for a digital health platform HIPAA compliant, it must satisfy the requirements put forward by the *Security Rule*. Whereas the *Privacy Rule* comprises the principles of use and disclosures of PHI, the Security Rule outlines the measures that must be put in place in order to adequately protect confidential PHI (Bova et al. 2012). However, one important aspect of the Privacy Rule is the Business Associates clause (Institute of Medicine (US) Committee 2003), which as mentioned above, states that a formal contract is needed prior to sharing PHI with a third party that is not part of the covered entity. This is crucial as it is an easily auditable component of your HIPAA compliance and a lack of contractual obligation from a third party to adhere to Privacy Rule guidance is punishable under the HHS.

The Security Rule outlines three main types of "safeguard" that should be implemented in order to ensure the platform is compliant (Services DOHAH 2003). The first are Administrative Safeguards, which according to the HHS are "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." (Services DOHAH 2003) The Administrative Safeguards are broken down (Table 17.1) into different "Security Standards," which include: Security Management Process, Assigned Security Responsibility, Workforce Security, Information Access Management, Security Awareness and Training, Security Incident Procedures, Contingency Plan, Evaluation, and Business Associate Contracts. These nine Administrative Safeguards contain within them specific implementation requirements, termed "required" and "addressable." The only safeguard which is fully required fall under Security Management Process, which include performing a risk analysis (identifying possible security threats), risk management (reducing vulnerability to a security breach), sanction policy (ensure appropriate sanctions brought on those members of the workforce who fail to follow security procedures) and information system activity review (scheduled review of information systems activity including incident reports). Additionally, three "Contingency Plan" specifications are also deemed mandatory: data backup plan (ensure retrievable electronic copies of medical records), disaster recovery plan (ensure implementable process to restore lost data), and emergency mode operation plan (ability to continue crucial processes in the event of an emergency). All additional specifications listed in Table 17.1 are considered addressable, that is the covered entity must make a determination as to whether this process is *reasonable* and *appropriate* given the operational environment.

The second set of components that ensures a digital health platform is compliant with the Security Rule is the "Physical Safeguards" (Table 17.2). These comprise the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." (Services DOHAH 2003) The Physical Safeguards are further subcategorized into: Facility Access Controls, Workstation Use, Workstation Security, and Device and Media Controls. The latter contains two "required" specifications. "Disposal" states that all PHI which is to be erased be done in a permanent manner, and "media re-use" ensures that any medium used to store PHI is completely wiped prior to it being re-purposed.

The final set of measures that are put forth in the Security Rule are termed "Technical Safeguards." These comprise five types of technological precautions: Access Controls, Audit Controls, Integrity, Person or Entity Authentication, and Transmission Security (Table 17.3). Adequate technological security is of great importance at a time when cyber-crime continues to evolve in sophistication (Firm 2013). The Security Rule provides a variety safeguards that covered entities can use

Table 17.1 Administrative safeguards in digital health

Administrative safeguard	Description	Implementation specifications
1. Security management process	Internal policies which prevent and protect against security violations	**1. Risk analysis** **2. Risk management** **3. Sanction policy** **4. Information system activity review**
2. Assigned security responsibility	Identification of a individual within the covered entity who will oversee PHI security	None provided
3. Workforce security	Determine which individuals need access to PHI, and ensure they are granted it	1. Authorization and/or supervision 2. Workforce clearance procedure 3. Termination procedures
4. Information access management	The execution of policy for granting access to those individuals needing PHI access	1. Isolating health care clearinghouse functions 2. Access authorization 3. Access establishment and modification
5. Security awareness and training	Ensure all employees and management of covered entity undergoes security training	1. Security reminders 2. Protection from malicious software 3. Log-in monitoring 4. Password management
6. Security incident procedures	Policy and process to address breaches in security practices, covering identification and documentation, and response	None provided
7. Contingency plan	Ensure a policy is in place to respond to system failures, natural disasters, vandalism, etc.	**1. Data backup plan** **2. Disaster recovery plan** **3. Emergency mode operation plan** 4. Testing and revision procedures 5. Applications and data criticality analysis
8. Evaluation	Episodic evaluation of safeguards to ensure policy in place meets the standards set forth by the security rule	None provided
9. Business associate contracts	Ensure written contracts exist between covered entities and third party contractors who will have access to PHI	None provided

bold indicates “required” implementation specifications

for technical protection, but of these only two, “Unique User Identification” and “Emergency Access Procedure,” are deemed mandatory. The former instructs covered entities to ensure that each employee and administrator have a unique identification within the electronic information system, both for access security and auditing purposes. The second demands that in an emergency setting (power outage, natural disaster, etc.), access to the electronic PHI is maintained (Services DOHAH 2003).

Table 17.2 Physical safeguards for digital health

Physical safeguards	Description	Implementation specification
Facility access controls	Ensure physical access to HER storage facilities is limited to only those with authorization	1. Contingency operations 2. Facility security plan 3. Access control and validation procedures 4. Maintenance records
Workstation use	Control over the physical properties of a workstation where the EHR is accessed from	None specified
Workstation security	Ensure physical access to workstations is restricted to only those with authorization	None specified
Device and media controls		**1. Disposal** **2. Media Re-use** 3. Accountability 4. Data backup and storage

bold indicates "required" implementation specifications

Table 17.3 Technical safeguards for digital health

Technical safeguard	Description	Implementation specification
Access control	Technical policies that allow PHI access only to those allowed	**1. Unique user identification** **2. Emergency access procedure** 3. Automatic logoff 4. Encryption and decryption
Audit controls	Software that is able to routinely examine activity of an EHR	None specified
Integrity	Prevent unwanted manipulation or destruction of data	1. Mechanism to authenticate electronic protected health information
Person or entity authentication	Verification of employees attempting to access EHR	None specified
Transmission security	Prevent unwanted access to PHI during transmission over an "electronic communications network"	1. Integrity controls 2. Encryption

bold indicates "required" implementation specifications

17.3 How Do We Use Digital Health to Enhance Clinical Performance?

The use of digital health in modern medicine goes beyond the use of technology in medical record keeping. While the EHR has revolutionized modern medicine, there is a multitude of other ways to deploy technology in order to improve our healthcare delivery. According to Eric Topol, author of *The Creative Destruction of Medicine*, digital health is the "…digitization of humans," and through the use of wireless devices, social media, and computer power, we are "…illuminating the human black box" (Topol 2012). In essence, as technology evolves, we are able to capture human metrics in more detail than ever before.

Many examples of how digital healthcare can improve a patient's life are self-evident, from cochlear implants that facilitate hearing, to robots that assist in patient rehabilitation after stroke. We have discussed the EHR and its integral role in modern healthcare, giving stakeholders the ability to rapidly collate large sums of data for quality improvement research. In this chapter however, we will focus on the use of digital data collection in surgery and its use in optimization of healthcare delivery. This is an underexplored field, with recent advances having sent far-reaching ripples through the academic community.

Technology needs to be at the center of quality improvement in surgical care. The most direct way this can be accomplished is through direct improvement of surgeon skill. There are multiple ways in which this can be achieved. As surgery moves from the traditional "open" approach to minimally invasive surgery (MIS), there are more and more procedures being performed with the use of a laparoscope, a small fiber-optic camera that allows the surgeon to see inside a body cavity through an incision only a couple centimeters in width. This use of video-assisted surgery allows for capture of intraoperative, intra-corporeal video. Recording footage from the operating room gives rise to many methods of analysis, from direct assessment and feedback, to tele monitoring and surgical coaching.

Standardized assessment metrics of surgeon technical skill have been used since the mid-1990s. Dr. Richard Reznick's group developed the objective structured assessment of technical skills (OSATS) at the University of Toronto, a simulation-based examination for assessing basic surgical skills (Martin et al. 1997). The introduction of new surgical techniques (laparoscopy, robotics) has demanded the evolution of this type of "global assessment" tool (Vassiliou et al. 2005; Goh et al. 2012). These Likert scale-based assessment instruments allow us to score individual surgeons and trainees in the operating room. Through video analysis, we have moved the arena of surgical assessment from the "bench" to the "bedside." The ability to slow down, stop, or rewind the "game-tape" of a procedure allows for careful analysis of surgeon skill, as well as the use of multiple raters to ensure reliability. The use of video in the operating room also allows for capturing intraoperative errors, defined as …"any deviation from the normal course of a procedure" (Bonrath et al. 2015a). The development of the Generic Error Rating Tool (GERT) allows for a careful *root-cause analysis* of operative near-misses, errors, and most importantly adverse events, which is imperative for improving surgical care delivery. Additionally, efforts are being made to identify whether a surgeons physiological state in the operating room is of importance to optimizing quality care delivery (Moulton et al. 2007; Ahmidi et al. 2010).

Telemonitoring is another emerging way of using technology to enhance patient care and safety. Multiple companies (News 2013; Storz 2014) are currently working on implementing formal intraoperative telemonitoring, as evidence emerges supporting its use (Shin et al. 2015; Moshtaghi et al. 2015). Google, one of the largest IT companies in the world, developed a program for using Google Glass to capture live surgery (Hashimoto et al. 2015).

Another benefit of retrospective review of surgical performance is that is facilitates peer coaching. Learning surgical technical and non-technical skill, which are determinants of patient outcome (Birkmeyer et al. 2013), in real-time during a procedure is often difficult due to external pressures. According to Bonrath et al. (2015b), a way to enhance trainee and surgeon learning is through "… objective assessment, structured debriefing, feedback, behavior-modeling, and guided self-reflection." This is more feasible in a controlled setting, which the post-operative review session provides. In addition to the aforementioned study, there are other groups showing the benefits of surgical coaching through video analysis (Greenberg et al. 2015).

Another way of improving quality through digital data collection in surgery is the identification of training needs and developing "educational interventions" to address them. This process involves understanding which steps of a procedure are prone to surgeon error and designing a targeted program to address the knowledge or technical deficiencies that led to these errors (Bonrath et al. 2013). One way to approach this is by reviewing error-prone steps of a given surgical procedure with trainees in order to ensure they understand the events that led up to error being committed (Bonrath et al. 2015a). A more technologically advanced means of utilizing error-related data to enhance training is through to creation of simulation models that mimic high-risk steps of a procedure (D'Angelo et al. 2015). This allows for trainees to learn the technical skills needed in order to complete high-risk procedures in a safe, low-risk environment.

Other groups have sought to improve surgeon efficiency in the operating room, through a variety of means. Thalmic Labs (Thalmic Labs, Kitchener, ON, Canada) developed the Myo Armband as a way to control electronic devices wirelessly, through an armband that detects muscle movement in the forearm (Labs 2014). They partnered with TedCas (TedCas Medical Systems, Noáin, Spain), and developed a system for surgeons controlling medical devices such as imaging software, wirelessly and while remaining sterile. A similar endeavor is the GestSure system, which uses a Microsoft Kinect© (Microsoft, Redmond, WA) to interpret surgeon movement in order to control medical software. It was developed to fill a similar niche in surgery, to allow surgeons to remain sterile, while interacting with non-sterile equipment (GestSure 2016). These simple adaptations of existing technology are examples of the 'cross-innovation' that can occur when creative minds draw creative inspiration from other realms of technology.

While these described methods can or may enhance surgeon performance in surgery, one must take a real-world approach that synthesizes these principles, without hindering the day-to-day function of the operative environment. The OR Black Box® has been developed in order to facilitate this, through the input of multiple sources of video, audio, and patient physiological metrics. Complete data capture in the operating room allows for a detailed analysis of the events that lead to an adverse outcome, an process developed and employed by the aviation industry. A holistic approach to intraoperative monitoring allows the OR Black Box® system to conduct complex root-cause analyses, with GERT and other assessment metrics. This multimodal data can be used for surgeon/trainee/nurse/anesthesiologist assessment, system-wide quality improvement, coaching, and educational interventions, and most importantly ensure patient safety through the study of intraoperative adverse events, including their causes and consequences.

In the United States, efforts have been undertaken to collate high-fidelity intraoperative data capture from multiple sites. Statewide digital health repositories such as the Michigan Bariatric Surgery Collaborative (MBSC) and the Michigan Urological Surgery Improvement Collaborative (MUSIC) have taken advantage of data collected from multiple hospitals in order to analyze and optimize the quality of care being delivered in the state (Birkmeyer et al. 2013; Ghani et al. 2016). Through high-volume analysis, research questions can be approached with high volume data and sufficient power in order to draw meaningful conclusions at a statewide level. These groups represent a step from *intra*- to *inter*-hospital collaboration and quality improvement initiatives.

Medical education will be revolutionized through the benefits of digital platform development. The shift from the time-base, “Halsteadian” training model (Halsted 1904), to the contemporary Competency-Based Medical Education model (CBME) (Potts 2016) has created a pressing need for robust means of analyzing trainee performance in the clinical environment. Technology such as the OR Black Box® will allow stakeholders to better understand the real-world performance of their trainees, and over time, develop a greater ability to define thresholds for what is deemed “competent” at a given task or procedure (Szasz et al. 2014). We understand that not only is technical skill in surgery is important for high-stakes assessment, but also non-technical skill, and digital platforms that collect both types of data are needed for adequate evaluation of surgical trainees.

17.4 Who Is Ready to Handle Digital Health Information?

As discussed in this chapter, digital health can play a hugely important role in the overall improvement of health care delivery. “Big Data” promises to provide answers for many of the health care challenges we face today. However, it is crucial there is absolute clarity in terms of who has access to this type of data. The legal and ethical implications of allowing open access to patient data are far reaching, and are important to recognize as this field continues to grow. These obstacles may hinder the ability to provide open access to data, and they will be discussed below.

A 2014 systematic review (van Panhuis et al. 2014) describes two types of “legal barriers” that may have implications in data sharing in research. One, “Protection of Privacy,” describes the role of the HIPAA and other government organizations around the world that exist to regulate both PHI confidentiality and sharing. In the article, they cite concerns that the borders between fully de-identified data and that which contains some PHI is not always clear, and that this can limit data which can be shared (Wartenberg and Thompson 2010; Lane and Schur 2010). The other barrier described pertains to ownership and copyright concerns. They site a Canadian example of this (Kephart 2002), where in order to amalgamate a nationally collected health survey with provincially collected patient data, individual approval processes were required, province-by-province. This type of legal obstruction leads to increased effort and expense on researchers. As the methods of collecting patient data expands and diversifies, there will be more and more confusion as to who actually is responsible for guardianship of data sets, and this will discourage organizations from sharing data for fear of legal reprimand (Lee and Gostin 2009). As this review points out, this lack of granularity with regard to data ownership leads to inconsistency in guidelines published (Strobl et al. 2000). In the United Kingdom, there was a great amount of uncertainty regarding PHI use in research, following the Data Protection Act of 1998 (Strobl et al. 2000). This lead to the further legislation around the subject of data sharing (Greenough and Graham 2004), and the process there remains disjointed and controversial (Knapton 2016).

The Propublica's "Surgeon Scorecard" is an example of controversial sharing of "Big Data" with the general public. This is a freely accessible database that published surgeon morbidity and mortality statistics, in an effort to increase the transparency of patient outcomes reporting (Allen and Pierce 2015). While a noble pursuit, recent criticism has called the validity of their outcome reporting into question. In a recent article (Ban et al. 2016), Ban et al. conducted an analysis, comparing Scorecard reported "adjusted complication rate" with traditionally studied outcomes from the NSQIP database. They found that ProPublica's exclusion criteria omitted 84% of postoperative complications and correlated poorly with NSQIP outcomes. This critique, in addition to that of the RAND group (Friedberg et al. 2016), have called into question whether this type of data should have been published without first going through a full assessment of validity. While all agree that the public needs to be privy to this type of information, the means by which it is best delivered remains to be answered.

How should patients be integrated in data sharing strategies? A review by de Lusignan et al. in 2014 examined the effect of patient access to the EHR on patient safety, patient experience and satisfaction, adherence, equity and efficiency (de Lusignan et al. 2014). Their group found that patient EHR access fails to impact patient outcomes parameters, except for a possible decrease in prescribing error regarding drug interactions (Staroselsky et al. 2008). Additionally, they found that the literature points to concerns amongst physicians about patient worry or offense taken when accessing their medical file (Haggstrom et al. 2011). Finally, there is general apprehension amongst health care professionals that allowing patient access to EHR data will limit their productivity due to an increase in patient correspondence around test results (de Lusignan et al. 2013). However, other publications have found the inverse to be true (TSO 2012). In an American pilot study in 2013, the Department of Veteran Affairs (VA) offered its patient's full access to their EHR, and assessed overall patient satisfaction. Nearly all patients in the study (90%) felt that this complete transparency improved their overall care (Nazi et al. 2013). A systematic review of the effect of patient access to EHR found that of all endpoints assessed, the strongest evidence showed an improvement in doctor-patient communication when patients were able to see their medical record (Ross and Lin 2003). They found in their review that important factors such as adherence, patient education and empowerment. They also found that in the non-psychiatric patient population, there was not an increase in anxiety or worry around reading medical notes.

The role of robust, highly integrated operative data collection was discussed earlier in this chapter. The OR Black Box® and similar endeavors use real intraoperative footage in its analysis of surgical factors in patient outcomes. This concept of video recording in the operating room comes with some ethical implications that must be addressed. In a recent article from Prigoff et al. (2016), multiple steps are outlined to ensure that video recording is carried out in a way to addresses issues like patient consent and confidentiality. In addition to straightforward concepts, such as ensuring the patient gives *informed* consent and de-identification of video data, the article touches on the important topic of data ownership. If the video is created to be stored in the EHR, then it is considered part of the medical record and is fully accessible to patients. However, if the video is created as part of a quality improvement initiative, then it is considered separate from the medical record (Makary 2013). The legal implication here is that it is considered inadmissible in cases of litigation, unless the court deems its inclusion is necessary for the purposes of discovery. Finally, the article stresses the importance of maintaining security practices that ensure the upholding of patient confidentiality.

17.5 Conclusion

Emerging technologies in data capture and sharing in the medical field open the door for advances in our understanding of healthcare and disease. Big Data has become the mantra of many healthcare researchers who have been tasked with answering the key questions of our day. The use of digital health datasets require highly robust methods of ensuring data security, as well as innovative methods for optimizing patient safety. In this chapter, the concepts of data privacy were covered, focusing on the key aspects of the HIPAA regulations. In addition, novel use of digital health technologies was discussed, highlighting recent innovations in surgery in particular. Finally, the legal and ethical barriers that stakeholders face when interacting with healthcare data was discussed, outlining the roles that both healthcare professionals and patients play as we move further into the era of digital health.

References

Ahmidi N, Hager GD, Ishii L, Fichtinger G, Gallia GL, Ishii M. Surgical task and skill classification from eye tracking and tool motion in minimally invasive surgery. Med Image Comput Comput Assist Interv. 2010;13(Pt 3):295–302.

Allen M, Pierce O. Making the cut. ProPublica Patient Safety. https://www.propublica.org/article/surgery-risks-patient-safety-surgeon-matters. Published July 13, 2015. Accessed July 25, 2106.

Ban KA, Cohen ME, Ko CY, et al. Evaluation of the ProPublica Surgeon scorecard "adjusted complication rate" measure specifications. Ann Surg. 2016;1 doi:10.1097/SLA.0000000000001858.

Berwick DM. Measuring surgical outcomes for improvement: was Codman wrong? JAMA. 2015;313(5):469–70.

Birkmeyer JD, Finks JF, O'Reilly A, et al. Surgical skill and complication rates after bariatric surgery. N Engl J Med. 2013;369(15):1434–42. doi:10.1056/NEJMsa1300625.

Bohnen JD, Chang DC, Lillemoe KD. Reconceiving the morbidity and mortality conference in an era of big data. Ann Surg. 2016;263(5):857–9. doi:10.1097/SLA.0000000000001508.

Bonrath EM, Zevin B, Dedy NJ, Grantcharov TP. Error rating tool to identify and analyse technical errors and events in laparoscopic surgery. Br J Surg. 2013;100(8):1080–8. doi:10.1002/bjs.9168.

Bonrath EM, Gordon LE, Grantcharov TP. Characterising "near miss" events in complex laparoscopic surgery through video analysis. BMJ Qual Saf. May 2015a:1–7. doi:10.1136/bmjqs-2014-003816.

Bonrath EM, Dedy NJ, Gordon LE, Grantcharov TP. Comprehensive surgical coaching enhances surgical skill in the operating room. Ann Surg. 2015b;262(2):205–12. doi:10.1097/SLA.0000000000001214.

Bova C, Drexler D, Sullivan-Bolyai S. Reframing the influence of the health insurance portability and accountability act on research. Chest. 2012;141(3):782–6. doi:10.1378/chest.11-2182.

D'Angelo AL, Law KE, Cohen ER, et al. The use of error analysis to assess resident performance. Surgery. 2015;158(5):1408–14. doi:10.1016/j.surg.2015.04.010.

de Lusignan S, Morris L, Hassey A, Rafi I. Giving patients online access to their records: opportunities, challenges, and scope for service transformation. Br J Gen Pract 2013.

de Lusignan S, Mold F, Sheikh A, et al. Patients' online access to their electronic health records and linked online services: a systematic interpretative review. BMJ Open. 2014;4(9):e006021. doi:10.1136/bmjopen-2014-006021.

Firm WKLB. *Modifications to HIPAA privacy, security, and breach notification rules*. 2013.

Friedberg MW, Pronovost PJ, Shahian DM. A methodological critique of the ProPublica surgeon scorecard. Santa Monica. Rand Health Q. 2016;5(4, 1)

GestSure. Product information for management. July 2016:1–3. http://www.gestsure.com/product-information-for-management/.

Ghani KR, Miller DC, Linsell S, et al. Measuring to Improve: peer and crowd-sourced assessments of technical skill with robot-assisted radical prostatectomy. Eur Urol. 2016;69(4):547–50. doi:10.1016/j.eururo.2015.11.028.

Glenn T, Monteith S. Privacy in the digital world: medical and health data outside of HIPAA protections. Curr Psychiatry Rep. 2014;16(11):494–11. doi:10.1007/s11920-014-0494-4.

Goh AC, Goldfarb DW, Sander JC, Miles BJ, Dunkin BJ. Global evaluative assessment of robotic skills: validation of a clinical assessment tool to measure robotic surgical skills. J Urol. 2012;187(1):247–52. doi:10.1016/j.juro.2011.09.032.

Greenberg CC, Ghousseini HN, Pavuluri Quamme SR, Beasley HL, Wiegmann DA. Surgical coaching for individual performance improvement. Ann Surg. 2015;261(1):32–4. doi:10.1097/SLA.0000000000000776.

Greenough A, Graham H. Protecting and using patient information: the role of the Caldicott Guardian. Clin Med (Lond). 2004;4(3):246–9.

Haggstrom DA, Saleem JJ, Russ AL. Lessons learned from usability testing of the VA's personal health record. J Am Med Inform Assoc. 2011;18(Suppl 1):i13–7.

Halsted WS. The training of the surgeon. JAMA. 1904;XLIII(21):1553–4.

Hashimoto DA, Phitayakorn R, Fernandez-del Castillo C, Meireles O. A blinded assessment of video quality in wearable technology for telementoring in open surgery: the Google Glass experience. Surg Endosc. 2015:1–7. doi:10.1007/s00464-015-4178-x.

Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. Business Associates. April 2003:1–6.

Kephart G, Canadian institute for health information, initiative CPH. Barriers to accessing and analyzing health information in Canada. Ottawa: Canadian Institute for Health Information; 2002.

Knapton S. Controversial £7.5 million NHS database scrapped quietly on same day as Chilcot Report. *The Daily Telegraph*. http://www.telegraph.co.uk/science/2016/07/06/controversial-50-million-nhs-database-scrapped-quietly-on-same-d/. Published July 6, 2016.

Labs T. See the Myo armband in surgery. November 2014:1–7. http://blog.thalmic.com/myo-armband-surgery/.

Lane J, Schur C. Balancing access to health data and privacy: a review of the issues and approaches for the future. Health Serv Res. 2010;45(5 Pt 2):1456–67. doi:10.1111/j.1475-6773.2010.01141.x.

Lee LM, Gostin LO. Ethical collection, storage, and use of public health data: a proposal for a national privacy protection. JAMA. 2009;302(1):82–4. doi:10.1001/jama.2009.958.

Makary MA. The power of video recording: taking quality to the next level. JAMA. 2013;309(15):1591–2. doi:10.1001/jama.2013.595.

Martin JA, Regehr G, Reznick R, et al. Objective structured assessment of technical skill (OSATS) for surgical residents. Br J Surg. 1997;84(2):273–8.

Moshtaghi O, Kelley KS, Armstrong WB, Ghavami Y, Gu J, Djalilian HR. Using Google glass to solve communication and surgical education challenges in the operating room. *The Laryngoscope*. March 2015: n/a–n/a. doi:10.1002/lary.25249.

Moulton C-AE, Regehr G, Mylopoulos M, MacRae HM. Slowing down when you should: a new model of expert judgment. Acad Med. 2007;82(10 Suppl):S109–16. doi:10.1097/ACM.0b013e3181405a76.

Murdoch TB, Detsky AS. The inevitable application of big data to health care. JAMA. 2013;309(13):1351–2. doi:10.1001/jama.2013.393.

Naam NH, Sanbar S. Advanced technology and confidentiality in hand surgery. J Hand Surg. 2015;40(1):182–7. doi:10.1016/j.jhsa.2014.03.011.

Nass SJ, Levit LA, Gostin LO, Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. Beyond the HIPAA privacy rule: enhancing privacy, improving health through research. 2009. doi:10.17226/12458.

Nazi KM, Hogan TP, McInnes DK, Woods SS, Graham G. Evaluating patient access to electronic health records: results from a survey of veterans. Med Care. 2013;51(3 Suppl 1):S52–6. doi:10.1097/MLR.0b013e31827808db.

News HI. Innovation in telemedicine technology: an entrepreneur's perspective. May 2013:1–19. http://www.healthcareitnews.com/news/innovation-telemedicine-technology-entrepreneurs-perspective.

Potts JR. Assessment of competence: the accreditation council for graduate medical education/residency review committee perspective. Surg Clin North Am. 2016;96(1):15–24. doi:10.1016/j.suc.2015.08.008.

Prigoff JG, Sherwin M, Divino CM. Ethical recommendations for video recording in the operating room. Ann Surg. 2016;264(1):34–5. doi:10.1097/SLA.0000000000001652.

Register OOTF. *Code of Federal Regulations Title 45*. Government Printing Office; 2010.

Ross SE, Lin C-T. The effects of promoting patient access to medical records: a review. J Am Med Inform Assoc. 2003;10(2):129–38. doi:10.1197/jamia.M1147.

Services DOHAH. The security rule. February 2003:1–49.

Services DOHAH. ONC Data Brief Number 1, 2012 Electronic health record systems and intent to attest to meaningful use among acute care hospitals in the U S 2008–2011. February 2012:1–7.

Services UDOHAH. *Summary of the HIPAA Security Rule*. 2013.

Shin DH, Dalag L, Azhar RA, et al. A novel interface for the telementoring of robotic surgery. BJU Int. 2015;116(2):302–8. doi:10.1111/bju.12985.

Staroselsky M, Volk LA, Tsurikova R. An effort to improve electronic health record medication list accuracy between visits: patients" and physicians" response. Int J Med Inform. 2008;77(3):153–60.

Stevens GM. *Compliance with the HIPAA medical privacy rule*. 2003.

Storz K. VISITOR1® from KARL STORZ–TELEMEDICINE EVOLVES into REMOTE PRESENCE. August 2014:1–3. https://www.karlstorz.com/ca/en/visitor1-telemedicine-evolves-into-remote-presence.htm.

Strobl J, Cave E, Walley T. Data protection legislation: interpretation and barriers to research. BMJ. 2000;321(7265):890–2.

Szasz P, Louridas M, Harris KA, Aggarwal R, Grantcharov TP. Assessing technical competence in surgical trainees: a systematic review. Ann Surg. 2014;261(6):1–1055. doi:10.1097/SLA.0000000000000866.

Topol EJ. The creative destruction of medicine. Basic books; 2012.

TSO. The power of information: putting all of us in control of the health. May 2012:1–119.

van Panhuis WG, Paul P, Emerson C, et al. A systematic review of barriers to data sharing in public health. BMC Public Health. 2014;14(1):1144. doi:10.1186/1471-2458-14-1144.

Vassiliou MC, Feldman LS, Andrew CG, et al. A global assessment tool for evaluation of intraoperative laparoscopic skills. Am J Surg. 2005;190(1):107–13. doi:10.1016/j.amjsurg.2005.04.004.

Wartenberg D, Thompson WD. Privacy versus public health: the impact of current confidentiality rules. Am J Public Health. 2010;100(3):407–12. doi:10.2105/AJPH.2009.166249.