Access and Disclosure of Personal Health Information: A Challenging Privacy Landscape in 2016-2018

Linda L. Kloss[1], **Melanie S. Brodnik**[2], **Laurie A. Rinehart-Thompson**[3]

[1] Kloss Strategic Advisors, Vero Beach, FL USA

[2] Emeritus Health Information Management and Systems, The Ohio State University, Columbus, Ohio, USA

[3] Health Information Management and Systems, The Ohio State University, Columbus, Ohio, USA

Summary

Objectives: To assess the current health data access and disclosure environment for potential privacy-protecting mechanisms that enable legitimate use of personal health information while preserving the rights of individuals. To identify the gaps and challenges between increasing requests and expanding uses of such information and the regulations, technologies, and management practices that permit appropriate access and disclosure while guarding against harmful misuse of such information.

Methods: A scoping literature review focused on (1) regulations affecting access and disclosure of personal health information, (2) the uses of health information that challenge access and disclosure boundaries, and (3) privacy management practices that may help mitigate gaps in protecting patient privacy.

Results: Countries and jurisdictions are developing laws, regulations, and public policies to balance the privacy rights of individuals and the unprecedented opportunities to advance health and health care through expanded uses of health data. Regulations and guidance are evolving, but they are outpaced by the increasing demand for and the challenges of managing access and disclosure. Mechanisms such as consent and authorization may not always be adequate. Mechanisms that advance principled stewardship are more important than ever.

Conclusions: Access and disclosure management are important dimensions of privacy management practices. This is a volatile period in which diverging public policies may reveal how best to balance access and disclosure of personal health information by individuals and by institutional custodians of the information. Approaches to access and disclosure management, including the roles of individuals, should be a focus for research and study in the years ahead.

Keywords

Privacy; health data access; disclosure; Health Information Portability and Accountability Act; General Data Protection Regulation; information governance

Yearb Med Inform 2018:60-6
http://dx.doi.org/10.1055/s-0038-1667071

Introduction

The current health data access and disclosure environment can be characterized by various attempts to develop privacy-protecting mechanisms that enable the legitimate use of personal health information while preserving the rights of individuals. A person's right to control access to, and the disclosure of, his or her personal information is the crux of the right of privacy anchored in law, regulation, and principles of fair information practices. Individuals exercise their right to control access by being afforded "notice" of information collection and how it is to be used and "choice" about whether to permit such collection and use.

While the principles underlying the privacy of personal health information are nearly universal, their implementation varies greatly depending on applicable law and regulation, the digital environment, the lifecycle of the information, personal preferences, and rapidly changing uses. Countries and jurisdictions are grappling with how to craft policies that balance the rights of individuals and the unprecedented opportunities to advance health and health care through expanded uses of data [1]. Digitization of health data is unleashing a range of transformative uses contributing to improved design and delivery of health care, better personal health choices, and healthier communities. These uses include population health improvement, medical registries, biomedical devices, and research analytics. Overall, more health information is being created about individuals and individuals are creating more health information about themselves [2].

This paper summarizes recent challenges confronting the privacy landscape as demands for access and disclosure of personal health information have increased. In today's dynamic information environment, it appears to be more difficult for individuals to exercise their rights and more challenging for policymakers and those responsible for stewardship of personal health information.

Methods

A scoping literature review was conducted that included sources from the US and EU regulatory agencies, articles found through PubMed, CINAHL (Cumulative Index to Nursing and Allied Health Literature), Embase, MeSH (Medical Subject Headings) databases, and other sources including policy papers and environmental scan documents from a variety of govern-

mental and industry sources focusing on privacy protection trends. Literature was reviewed from 2016 through early 2018 with some earlier seminal articles cited. The literature review was broad in order to identify the changes in regulation and the expanded uses of information in order to capture challenges in access and disclosure management. The US Health Information Portability and Accountability Act of 1996 (HIPAA) definitions for the key concepts of access and disclosure have been used [3, 4].

Access is the individual's right 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. Access rights extend to individuals or entities authorized by the patient, such as doctors and personal health record services) with an electronic copy of their file.

Disclosure is the release, transfer, provision of *access* to, or divulging in any other manner of *information* outside the entity holding the *information.*

Fig. 1 HIPAA definitions of Access and Disclosure.

Results

The literature review revealed three major themes with accompanying trends, issues, and challenges. The first theme is focused on access and disclosure laws and regulations encompassing privacy regulatory and legal protections. The second theme identified expanding access and disclosure demands for personal health information centered on exchange of health information and data analytics. The third theme presented emerging access and disclosure management practices and tools.

Changing Access and Disclosure Laws and Regulations

As the ability to create, collect, and disseminate vast amounts of health data has evolved, access and protection legislative and regulatory actions have advanced. This section addresses recent legislative and regulatory changes in the EU and the US affecting access, disclosure, use, and data subject empowerment.

In 2016, the EU adopted an updated General Data Protection Regulation (GDPR) that EU countries are gearing up to comply in 2018. By replacing a 1995 directive, the new regulation seeks both to achieve consistency among data privacy laws across Europe and to address the transfer of data to entities outside the EU [5]. GDPR applies broadly to nearly all record keepers, both to those who control and to those who process data about individuals, to all types of personal data that can be used to either directly or indirectly identify the subject, and to the movement of such data [5]. Key provisions apply a greater focus on the rights of data subjects and impose greater jurisdiction and enforcement.

The challenges of protecting the privacy of identifiable health information are universal in the Internet era. Despite similar challenges, both EU and US have very different approaches to regulating access and disclosure. The GDPR is more inclusive in scope than the protections afforded by HIPAA in the US, which limits protections to patient health data (i.e., protected health information, or PHI) in the hands of HIPAA-covered entities and business associates, whose functions center around health-related activities [4]. While applying to all types of personal data, GDPR stipulates that health and genetic information is considered sensitive information. It reinforces the rights of data subjects and the responsibilities of organizations and persons that control and process health and genetic data. Countries outside the EU are reexamining the adequacy of their own privacy laws as compared to the GDPR [6].

GDPR's data subject rights include the right to no-cost access to one's own electronic information from an entity that controls the data, with confirmation about where and for what purpose the data are being processed, and the ability to transmit one's own data to another controller. Rights also include the requirements that consents be unambiguous, accessible, explicit where sensitive information is involved, and easy to withdraw. The purpose of the consent must be attached to each consent that a person is requested to sign. Breach notification to affected data subjects, without undue delay, is also mandatory where the breach results in "risk to the rights and freedoms" of individuals [5]. A unique concept is the "right to be forgotten," a request by a data subject to the data controller to erase and stop further distribution of the subject's information. The controller may balance the request against the relevance of the information and the public interest to the information remaining available [5]. The GDPR's jurisdiction extends to all companies that hold or process personal data of citizens in EU countries, regardless of the company's location. This expands the law's reach to organizations outside the EU who offer goods or services, or monitor the behavior of EU citizens. Tiered penalties are assessed based on the nature of the offense and the organization's revenues [5].

Even as the uses of personal data continue to increase in the era of big health data, there was little change during 2016-2018 in the US to broaden the relatively narrow confines of HIPAA. The Department of Health and Human Services (DHHS) Office for Civil Rights (OCR) has rule making and enforcement authority for health information privacy and security. The US Federal Trade Commission (FTC) enforces the right to privacy beyond HIPAA's limits, to include breach notification requirements for non HIPAA-covered entities such as freestanding personal health record repositories.

In recent years, the US has taken an incremental approach such as issuing guidance on patient access to health records [7], cloud computing [8], and handling specific types of information such as patient safety data and the sharing of opioid data [9, 10]. OCR's venture into the patient access arena in 2016 via guidance regarding the right of individuals or their personal representatives to access their personal health information from healthcare providers, distinct from the authorization process, serves a two-fold purpose. First, it clarified healthcare pro-

viders' responsibilities. Second, it emphasized patient empowerment in healthcare decision-making by simplifying access for patients seeking to either obtain their own information or to direct this information to an individual of their choosing [11]. State laws may add protections for PHI beyond those provided by HIPAA, and other data protection laws may offer recourse when health information is no longer held by organizations subject to HIPAA protections.

In December 2016, the United States Congress passed the 21st Century Cures Act (Cures Act) [12]. Focused on accelerating medical product development and innovation, as well as advancing research in the areas of opioid abuse, Alzheimer's disease, and cancers [13], it sets the stage to facilitate collaborative data sharing in these priority areas while protecting identifiable sensitive information of research subjects and maintaining compliance with HIPAA. It allows the National Institutes of Health (NIH) to require the sharing of scientific data by recipients of grants [14] and permits the remote access of PHI preparatory to research provided that the required privacy and security safeguards are followed and researchers do not retain the PHI [15]. DHHS must issue guidance pertaining to authorization by an individual to permit the use of his or her PHI for future research [15]. Final revisions to the Common Rule, to go into effect July 19, 2018, require that informed consents contain a concise explanation of information that would be material to potential study subjects' understanding of the study and their participation decisions. Key elements include the purpose of the study, risks and benefits, and alternative treatments [16].

DHHS also finalized changes in 2017 to the longstanding regulations, Confidentiality of Alcohol and Drug Abuse Patient Records [17]. The revisions address the more contemporary needs of seamless health information exchange in integrated treatment systems and enhanced research, while preserving the original intent of the regulations to maintain the privacy and confidentiality of this sensitive information [18]. This type of sensitive information is also addressed in the 21st Century Cures Act, which requires DHHS to address use and disclosure of PHI of individuals either seeking or receiving mental or substance abuse treatment (Title XI, Section 11004) and automatically issues Certificates of Confidentiality to NIH-funded projects that collect or use identifiable sensitive information [19].

Efforts to protect personal information, both health-related and non health-related, are proactive across many jurisdictions. Such efforts should also be persistent and ongoing. Efforts in the EU that paint the privacy landscape with broad legislative strokes may provide blueprints for a legislation that addresses privacy universally rather than compartmentalizing it, as this is currently seen in the United States with the separation of HIPAA from other privacy laws.

Expanding Access and Disclosure for Health Information

Emerging issues regarding access and disclosure are discussed in the context of exchange of health information and data analytics. Exchange of health information requires proactive steps to ensure compliance with regulations and best practices for the disclosure of personal health information. Data analytics involves the use of aggregate health information most often anonymized or de-identified, which presents challenges to safeguard against unauthorized re-identification and re-disclosure.

Exchange of Health Information

Most developed countries have implemented electronic health record (EHR) systems and are working toward the seamless exchange of health information between disparate systems [20]. However, incompatible technology, lack of data standards, variations in state or regional privacy rules, and organizational governance policies impede EHR interoperability [20, 21]. Health information exchange (HIE), whether government-sponsored or private, is also being used to share health data across healthcare settings. The exchange, access, and use of patient health data through HIE may be limited due to exchange partners' concerns about privacy and security practices including protocols whereby individuals exercise consent to what is shared through the exchange process [22, 23]. These issues are under scrutiny in many countries as nationwide efforts to share information continue to evolve [24-27].

In the US, the Office of the National Coordinator for Health Information Technology (ONC) and key partners and stakeholders have assumed responsibility for moving the country toward an interoperable EHR environment. ONC's responsibility is supported through the HITECH Act and the Cures Act that has "set the expectation that all electronically stored patient health information will be exchanged, accessed and used under applicable State or Federal law" [28, 29]. The ONC's *Shared Nationwide Interoperability Roadmap, Proposed Interoperability Standards Measurement Framework* and the recently proposed *Trusted Exchange Framework and Common Agreement* focus on establishing policies, procedures, and technical standards that support interoperability capabilities while also adhering to State and Federal privacy and security rules related to the access, disclosure, and use of patient information [30-33].

Health Data Analytics

Analysis of aggregated health information is advancing population health management, performance improvement outcomes, and clinical medicine; however, the expanding ways in which health data are collected and used pose the potential for individual harm [34]. Issues related to the combinations of vast amounts of data, the use of advanced algorithms and artificial intelligence, and the lack of regulation mean "in many respects, anything goes" [35]. The range of these issues is well documented in seminal reports by the EU, the US President's Council of Advisors on Science and Technology, and the US Federal Trade Commission [34, 36, 37].

Data release policies that address control, transparency, and accountability when entities share aggregate health data may offer some privacy protection. De-identification of data is another form of protection that refers

to a "process that is applied to a dataset with the goal of preventing or limiting informational risks to individuals, protected groups, and establishments, while still allowing for the production of aggregate statistics" [38]. The US HIPAA Privacy Rule identifies circumstances when de-identified PHI may be disclosed. However, once disclosed, the de-identified data are no longer protected by the HIPAA. The EU GDPR places stricter controls on de-identified data use than what the HIPAA Rules provide by requiring that data subjects consent for data use unless other circumstances are documented. The GDPR approach is intended to help inform data subjects of how their information in aggregate form is being used and the circumstances under which they may give or withhold consent [39].

This brief discussion about access and disclosure issues relating to the exchange of health information and data analytics reveals some of the gaps in US regulatory controls. It remains to be seen how GDPR once implemented will protect the privacy of data subjects while advancing important uses for health and other types of information.

Governance and Management of Access and Disclosure

The volume of requests for disclosure of health records is increasing. For example, an eleven-hospital health system in the US Midwest processes 30,000 requests for health record disclosure per month [40]. Requests for de-identified health datasets are also on the rise. Healthcare organizations are improving the reliability of access and disclosure governance and management to improves against unauthorized access or disclosure of PHI [41].

Information Governance

Information governance (IG) is a management practice that makes explicit the framework under which information is processed, accessed, disclosed, protected, and used. Underlying IG decision-making are the Fair Information Practices (FIPs), a set of internationally recognized core information stewardship policies that embody time-tested ethical practices [42]. As a set of high-level policies, FIPs shape public policy and can also guide stewardship decisions where laws and regulations are silent [43]. IG translates principles into policies and ensures that policies are well executed. Today's complex access and disclosure challenges require enterprise-wide vigilance regarding individually identifiable and aggregated information across the lifecycle of that information.

IG is a voluntary function for health care organizations in the US and awareness is growing as health care organizations report benefits from formalizing access to analytic data and standardizing disclosure practices across the healthcare organization [44]. The UK's National Health Service uses IG as an organizing vehicle for various data protection and information handing requirements [45]. Adapting IG guidance from cross industry records management, the American Health Information Management Association (AHIMA) advocates for voluntary adoption in the US [46]. The voluntary multi-stakeholder organization, Integrating the Healthcare Enterprise (IHE), promulgates governance as the framework for information technology standards for health information management practice [47]. International health information management communities are likewise calling for more robust IG [48, 49].

Management Practices

Reliable process-based routines are foundational to effective access and disclosure management.

Sound access and disclosure management requires policies, procedures, technologies, and management tools to support the range of functions identified in Figure 2.

Informed consents and informed authorizations for the release of information are core issues in managing access and disclosure and remain an acknowledged weak link because it can be difficult to judge whether consent is informed and whether an authorization is authentic [43]. The EU GDPR includes explicit Rules for Consent to strengthen citizen's rights regarding an informed consent process for the collection, use, and sharing of personal data. In addition, patients must be informed about how to withdraw consent. Data controllers must be able to demonstrate that a person has given consent [50].

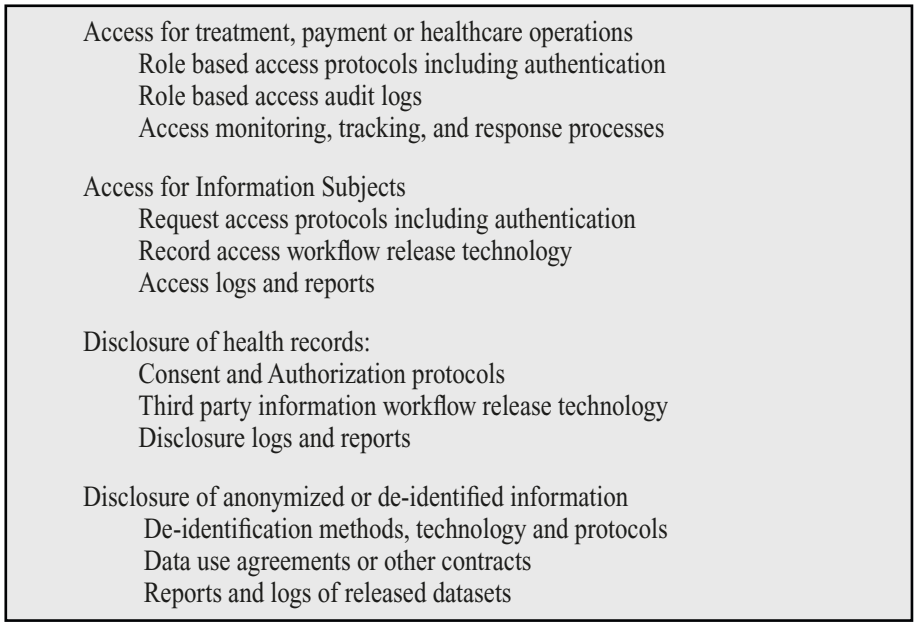

Fig. 2 Access and Disclosure Management Functions.

Disclosure of de-identified datasets is included in Figure 2 because effective management of aggregate data sets includes understanding intended uses and safeguarding against inappropriate uses that could bring harm to individuals. Rubenstein and Hartzog concluded "perfect anonymization has failed. Currently the law is focused on whether an individual can be identified within a set. We argue that the better locus for data release policy is on minimizing the risk of re-identification and sensitive attribute disclosure" [51]. The US National Committee for Vital and Health Statistics (NCVHS) the federal advisory committee on health data policy including HIPAA, recommended process-based guidance to reinforce best practices such as data sharing agreements, business associate agreements, consent and authorization practices, encryption, security and breach detection in the context of the management of de-identified data sets [52]. Guarding against re-identification of previously de-identified data is an important area where more advanced approaches need to be more widely used [53].

Technologies to support access and disclosure management continue to improve in areas such as role and attribute-based access, sensitive information segmentation, managing patient privacy preferences, and electronic request and distribution of authorized copies of medical records. Privacy engineering and privacy by design approaches have the potential to improve privacy systems thinking in technology development and process design [50, 53].

Health information stewards are responsible for sound policy governance and process management of access and disclosure functions. Technology advancements can support stewards in meeting these responsibilities regarding digital information management and can support data subjects in the exercise of their rights.

Discussion

Access and disclosure of health information is an important policy issue and a management challenge. Exploring recent public policy developments and the rapidly changing information environment reveals gaps that impact how access and disclosure functions are managed. Examples of such gaps include lack of meaningful notice, consent and authorization practices, weak data release policies for sharing aggregate health data, immature information governance and interoperability capabilities. The line between privacy protection of personally identifiable information and aggregate data is blurring as risks of re-identification increase. This review of the literature related to access and disclosure supports three conclusions:

1. There is much to be learned from further study of the impact of recent policy developments in the EU, US, and in other countries. For example, in 2017, Australia enacted more stringent breach notification requirements when a breach is likely to result in serious harm [54]. The UK will soon update its Information Governance requirements, a cornerstone for various data protection and information handing requirements including access and disclosure [55]. Jurisdictions are on different paths and the experiences over the next several years are likely to help inform future policy.
2. The management of access and disclosure processes is no longer a fragmented set of back office functions. As health systems become more complex and access and disclosure volumes increase, these functions like other aspects of information management are being centralized and standardized to improve reliability, mitigate risk, and control operating costs. Proactive access and disclosure management is a cornerstone of privacy management and effective governance of information [56].
3. There is potential to improve access and disclosure management with technology that will, for example, capture requests and authorizations, authenticate those authorizations, and disclose records using e-fulfillment. Technology can improve access management, monitoring, and control. It can also improve the de-identification of personal health information and help assess and mitigate the risk of re-identification [57].

Because of space constraints there are some limitations to this review. The very important topic of whether individuals know their information rights and how to access their own health information was not explored in this paper. Attitudes and understanding regarding uses of digital information for research, public health, and other uses were also not explored. However, because the Fair Information Practices ground public policy and information governance, the individuals' perspective is embedded in any discussion of access and disclosure.

Conclusions

Like other aspects of information management, access and disclosure of personal health information is in a volatile period. Recent policy advancements offer new opportunities to adapt, enhance, and improve practices and identify and apply practical lessons about what is required to raise the level of practice. Additional research and development is needed about workable solutions supported by privacy-enhancing technologies. More mature solutions need to be mainstreamed. Education of data stewards about best management and governance practices is indicated. There is an opportunity to deliver real value by making it easier for individuals to exercise their rights and for stewards to help them do so.

References

1. Van Staa T-P, Goldacre B, Buchan I, Smeeth L. Big health data: the need to earn public trust. BMJ 2016 July 14; 354 Available from: http://www.bmj.com/content/354/bmj.i3636
2. Wang Y, Kung L, Byrd T. Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technological Forecasting and Social Change. 2018 Jan 126; 3-13. Available from: https://www.sciencedirect.com/science/article/pii/S0040162516000500
3. 45 CFR 164.524. Security and Privacy; Access of individuals to protected health information. 2013. Available from https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-524.pdf
4. 45 CFR 160.103. General Administrative Requirements; Definitions. 2013. Available from https://www.gpo.gov/fdsys/pkg/CFR-2013-title45-vol1/pdf/CFR-2013-title45-vol1-sec160-103.pdf

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENGwww.eugdpr.org
6. Robertson SK. Calls grow for Canada to modernize privacy laws amid EU changes. The Globe and Mail. July 12, 2017. Available from: https://www.theglobeandmail.com/report-on-business/industry-news/marketing/calls-grow-for-canada-to-modernize-privacy-laws-amid-eu-changes/article35778176/
7. US Department of Health and Human Services, Office for Civil Rights. Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524, February 25, 2016. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
8. US Department of Health and Human Services, Office for Civil Rights. Guidance on HIPAA & Cloud Computing, June 16, 2017. Available from: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
9. US Department of Health and Human Services, Office for Civil Rights. Guidance on HIPAA & Cloud Computing, June 16, 2017. Available from: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
10. US Department of Health and Human Services, Office for Civil Rights, How HIPAA Allows Doctors to Respond to the Opioid Crisis. Available from: https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdfprofessionals/privacy/guidance/access/index.html
11. US Department of Health and Human Services. Individuals' Right under HIPAA to Access their Health Information. 45 CFR 164.524, February 25, 2016. Available from: https://www.hhs.gov/hipaa/for-
12. Public Law 114-255. Available from: https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf
13. Steinhauer J, Tavernise S. $6.3 Billion Measure Aims to Cure Ailing Health Care Policies. November 28, 2016. Available from: https://www.nytimes.com/2016/11/28/us/politics/congress-cures-cancer-moonshot-alzheimers.html
14. Majunder M, Guerrini C, Bollinger J, Cook-Deegan R, McGuire A. Sharing Data under the 21st Century Cures Act. Genet Med 2017;19(12):1289-94.
15. H.R. 34 21st Century Cures Act. Section 2063. Available from: https://www.congress.gov/bill/114th-congress/house-bill/34/
16. Federal Policy for the Protection of Human Subjects. Federal Register. 82 FR 7149. Jan. 19, 2018. https://www.federalregister.gov/documents/2017/01/19/2017-01058/federal-policy-for-protection-of-human-subjects
17. 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. Available from: https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=b7e8d29be4a2b815c404988e29c06a3e&rgn=div5& view=-text &node=42:1.0.1.1.2&idno=
18. Substance Abuse and Mental Health Services Administration. 42 CFR Part 2 Confidentiality of Substance Use Disorder Patient Records. January 9, 2018. Available from: https://www.samhsa.gov/health-information-technology/laws-regulations-guidelines
19. National Institutes of Health Certificates of Confidentiality (CoC) Kiosk. Certificates of Confidentiality for Research Funded by Non-HHS Federal Agencies. December 29, 2017. Available from: https://www.samhsa.gov/health-information-technology/laws-regulations-guidelines
20. Fradidis L, Chatzoglou P. Development of Nationwide Electronic Health Record (NEHR): An international study. Health Policy and Technology. 2017 6, 124-133.
21. Schmit C, Wetter S, Kash B. Falling short: how state laws can address health information exchange barriers and enablers. J Am Med Inform Assoc 2018;25(6);635-44.
22. Moon L. Factors influencing health data sharing preferences of consumers: A critical review. Health Policy Technol 2017;6;169-87.
23. HealthIT.gov. Computable Privacy. 2016. Available from: https://www.healthit.gov/policy-researchers-implementers/computable-privacy
24. Nohr C, Parv L, Kink P, Cummings E, Almong H, Norgarrd J, et al. Nationwide citizen access to their health data: analyzing and comparing experiences in Denmark, Estonia and Australia. BMC Health Serv Res 2017;17:534. Available from: https://bmchealthservres.biomedcentral.com/articles/10.1186/s12913-017-2482-y
25. Pietro C, Francetic I. E-health in Switzerland: The laborious adoption of the federal law on electronic health records (EHR) and health information exchange (HIE) networks. Health Policy 2018 Feb;122(2):69-74. Available from: http://www.healthpolicyjrnl.com/article/S0168-8510(17)30317-2/pdf
26. Séroussi B, Bouaud J. Adoption of a Nationwide Shared Medical Record in France: Lessons Learnt after 5 Years of Deployment. AMIA Annu Sym Proc 2016;2016:1100-9.
27. National Committee on Vital and Health Statistics (NCVHS). Recommendation on the HIPAA Minimum Necessary Standard. 2016. Available from: https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2016-Ltr-Privacy-Minimum-Necessary-formatted-on-ltrhead-Nov-9-FINAL-w-sig.pdf
28. Health Information Technology for Economic and Clinical Health Act. 2009. PubLaw 111-5(123 STAT. 226, et seq.) Feb. 17, 2009. Available from: https://www.healthit.gov/policy-researchers-implementers/select-portions-hitech-act-and-relationship-onc-work
29. Office of the National Coordinator for Health Information Technology. Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process. January 2018. Available from: https://www.healthit.gov/sites/default/ files/draft-uscdi.pdf
30. Office of the National Coordinator for Health Information Technology. Connecting Health and Care for the Nation A Shared Nationwide Interoperability Roadmap. 2015. Available from: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf
31. Office of the National Coordinator for Health Information Technology. Proposed Interoperability Standards Measurement Framework. 2017. Available from: https://www.healthit.gov/sites/default/files/ONCProposedIOStandardsMeasFrameworkREV.pdf
32. Office of the National Coordinator for Health Information Technology. Draft Trusted Exchange Framework. 2018. Available from: https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf
33. Morris, G. Trusted Exchange Framework and Common Agreement: A Common Sense Approach to Achieving Health Information Interoperability. 2018. Health IT Buzz. Available from: https://www.healthit.gov/buzz-blog/interoperability/trusted-exchange-framework-common-agreement-common-sense-approach-achieving-health-information-interoperability/
34. President's Council of Advisors on Science and Technology. Big Data and Privacy: A Technological Perspective. 2014. Available from: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf
35. Pasquale F. Virtual hearing of the NCVHS Privacy, Confidentiality, and Security Subcommittee. Nov. 28, 2017. Available from: https://www.ncvhs.hhs.gov/transcripts-minutes/transcript-of-the-november-28-2017-meeting-of-the-privacy-confidentiality-and-security-subcommittee/
36. European Commission Data Protection Working Party. Statement on Statement of the WP29 on the Impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU. Sept 2014. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf
37. Federal Trade Commission. Big Data A Tool for Inclusion or Exclusion? Understanding the Issues. 2016. Available from: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf
38. Garfinkel S. De-identifying Government Datasets, National Institute of Standards and Technology 800-188 (2d DRAFT)(Dec. 2016), p. 8. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-188/draft/documents/sp800_188_draft2.pdf
39. European Patients Forum. The New EU Regulations on the protection of personal data: what does it mean for patients? A guide for patients and patients' organizations. 2016; Available from: http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf
40. Hale H. St. Luke's Health System: Transforming ROI From Siloed to Enterprise-Wide Function. AHIMA Annual Convention and Exhibit; 2017 October 8-12; Los Angeles CA.
41. Vayena E, Gasser U, Wood A, O'Brien DR, Altman M. Elements of a New Ethical Framework for Big Data Research. Washington and Lee Law Review [Internet] 2016; 72(3) Available from: http://

openscholar.mit.edu/sites/default/files/dept/files/elements_of_a_new_ethical_framework_for_big_data_research.pdf
42. Organization for Economic Cooperation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980. Available from: theprotectionofprivacyandtransborderflowsofpersonaldata.htm
43. US Department of Health and Human Services, National Committee on Vital and Health Statistics (NCVHS) 2018. Health Information Privacy Beyond HIPAA: An Environmental Scan of Major Trends and Challenges. Available from: https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf
44. American Health Information Management Association. Awareness and Use Growing with Information Governance AHIMA's third IG survey showcases key recommendations for organizations seeking to transform through IG. AHIMA News Oct 17, 2017. Available from: http://www.ahima.org/topics/infogovernance/ignews
45. National Health Service. Information Governance Toolkit. Available from: https://www.igt.hscic.gov.uk/
46. American Health Information Management Association. Information Governance Toolkit 3.0. 2017. Available from: http://bok.ahima.org/doc?oid=302242#.WjAUOEuQxgc
47. Integrating the Healthcare Enterprise (IHE). Health IT Standards for Health Information Management Practices. September 18, 2015. http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_WP_HITStdsforHIMPratices_Rev1.1_2015-09-18.pdf
48. Canadian Health Information Management Association. Information Governance for Canadian Healthcare. May, 2017. Available from: https://www.echima.ca/uploaded/pdf/reports/IG_Paper_summary_Short_Final.pdf
49. International Federation of Health Information Management Associations. 2017. Available from: https://ifhima.files.wordpress.com/2017/10/ifhima-ig-whitepaper-final.pdf
50. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc= OJ:L:2016:119:TOC
51. Rubinstein IS, Hartzog W. Anonymization and Risk. New York University Law School, Public Law & Legal Theory Research Paper Series, Working Paper No 15-36.
52. National Committee on Vital and Health Statistics (NCVHS), 2017 Letter to the Secretary on De-identification of Protected Health Information. Available from: https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf
53. National Institute for Science and Technology An Introduction to Privacy Engineering and Risk Management in Federal Systems. NISTIR 8062 Available from: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf
54. Australian Government. Federal Register of Legislation. 2017. Available from: https://www.legislation.gov.au/Details/C2017A00012
55. NHS, Information Governance Toolkit. https://www.igt.hscic.gov.uk/
56. Kloss L. Implementing Information Governance, Lessons from the Field. AHIMA Press, 2015, p. 111-113.
57. Rubinstein IS, Hartzog W. Anonymization and Risk. New York University Law School, Public Law & Legal Theory Research Paper Series, Working Paper No 15-36.

Correspondence to:
Linda L. Kloss
1101 Baywood Drive
Vero Beach, FL 32963-3997
USA
E-mail: linda@kloss-strategicadvisors.com