A Primer on the **Privacy, Security**, and **Confidentiality** of **Electronic Health Records**

Manish Kumar, Samuel Wambugu
MEASURE Evaluation

February 2016

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation

A Primer on the **Privacy, Security,** and **Confidentiality** of Electronic Health Records

Manish Kumar, Samuel Wambugu
MEASURE Evaluation

February 2016

SR-15-12 ISBN: 978-1-943364-25-1

MEASURE Evaluation is funded by the U.S. Agency for International Development (USAID) under terms of Cooperative Agreement AID-OAA-L-14-00004 and implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International, John Snow, Inc., Management Sciences for Health, Palladium, and Tulane University. The views expressed in this presentation do not necessarily reflect the views of USAID or the United States government. SR-15-128

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation

ACKNOWLEDGMENTS

The authors thank Shannon Salentine for her useful suggestions and initial reviews of the document, Debbie McGill for editing, Denise Todloski for creative direction, and Sue Pace for design and formatting.

Suggested Citation

Kumar, M. & Wambugu, S. (2015). A primer on the security, privacy, and confidentiality of electronic health records. Chapel Hill, NC: MEASURE Evaluation, University of North Carolina.

ABBREVIATIONS

ANSI	American National Standards Institute
CEN	European Committee for Standardization
EHR	electronic health record
ePHI	electronic protected health information
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
PHI	protected health information
PII	personally identifiable information

CONTENTS

BACKGROUND

The use of electronic health records (EHRs) is widespread in developed countries but is only gradually displacing the use of paper records. Advocates of health information technology promote EHRs, because they improve quality of care, reduce cost, enhance patient mobility, are more reliable, and enable evidence-based medicine.[1] However, the transition from paper-based to EHR systems in low- and middle-income countries poses some unique challenges for privacy and confidentiality, security, and data integrity and availability[2] that can outweigh the benefits. For example, fragmented health information systems create barriers to improvements in quality of care, efficiency, and patient safety. Moreover, the growing use of mobile devices to capture and exchange electronic health information[3] presents complex security and confidentiality problems. From the health systems perspective, addressing security and privacy issues is critical not only for clinical care but also for public health and health systems research,[4] because data from patient encounters are used in routine health information systems for program monitoring and assessment.[5] Additionally, security breaches[6] of health information systems have economic, social, ethical, and legal implications, as evidenced by lawsuits arising from such incidents.

All of these challenges become more pressing with the rapid uptake of Internet services to share and access health information. Threats to the integrity of health information systems and the data they contain are real. Cyber security is required to prevent, detect, and act on unauthorized access to a health system and its information.[7] Therefore, ensuring privacy, security, confidentiality, integrity, and availability of protected health information (PHI) in EHRs is absolutely necessary.

> Electronic health records improve quality of care, reduce cost, enhance patient mobility,are more reliable, and enable evidence-based medicine.

Regardless of the format of patient health information—EHR, paper, mobile devices, or other media—healthcare providers and organizations must put safeguards in place to protect patient health information and comply with regulations.[8] With the growing need for healthcare providers to share and access health information across diverse and dispersed information systems and organizational boundaries, the interoperability of information systems has assumed greater significance for

---

[1] Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. A., and Toval, A. 2013. "Security and Privacy in Electronic Health Records: A Systematic Literature Review." *Journal of Biomedical Informatics*, 46(3), 541-562.

[2] Harman, L. B., Flite, C. A., and Bond, K. 2012. "Electronic Health Records: Privacy, Confidentiality, and Security." *The Virtual Mentor*: VM, 14(9), 712-719.

[3] Kotz, D., Fu, K., Gunter, C., and Rubin, A. 2015. "Privacy and Security: Security for Mobile and Cloud Frontiers in Healthcare." Communications of the Association for Computing Machinery (ACM), 58 (8):21-23. Available at: http://www.cs.dartmouth.edu/~dfk/papers/kotz-frontiers.pdf.

[4] Zou, X., Liu, P., and Chen, J. Y. 2011. "New Threats to Health Data Privacy." *BMC Bioinformatics, 12 Suppl 12*, S7-2105-12-S12-S7.

[5] Baker, Dixie B. 2010. "Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety." Chicago, IL: Healthcare Information and Management Systems Society (HIMSS). Available at: http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=7506.

[6] Iron Mountain. n.d. "Electronic Health Records Security and Privacy Concerns." Available at: http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/E/Electronic-Health-Records-Security-and-Privacy-Concerns.aspx.

[7] HealthIT.gov. n.d. "Cybersecurity: A Shared Responsibility." Available at http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility.

[8] Health Insurance Portability and Accountability Act (HIPAA). 2015. "Guide to Privacy and Security of Electronic Health Information." Available at: https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information.

improved quality of care, efficiency, and patient safety.[9]

Data privacy and security and patient confidentiality are two important dimensions of interoperability.[10] Achieving them requires countries and organizations to adopt health informatics standards, to help define the fundamental concepts associated with electronic health information. The International Standards Organization (ISO) has developed standards to enable health information security, privacy, and confidentiality. Many developed countries, such as the United States, the United Kingdom, and Canada are using standards and regulations extensively to meet security, privacy, and confidentiality needs in healthcare settings. For example, the Health Insurance Portability and Accountability Act (HIPAA)[11] and the Health Information Technology for Economic and Clinical Health Act[12] are two key pieces of U.S legislation addressing privacy and security in the transmission of data.

With rapid proliferation of EHRs, protecting and securing patient health information has become an important priority for healthcare providers.

This primer aims to describe basic concepts, outline global standards, and propose steps for organizations to protect and manage access to and use of individual health information in EHRs. We conducted a literature search in the PubMed database, using MeSH (medical subject headings) for **electronic health records** together with such key words as **privacy, security, confidentiality, protected health information,** and **personally identifiable information**. MeSH is a controlled vocabulary thesaurus of the National Library of Medicine used to index articles for PubMed. Selected literature from PubMed was used in writing this primer. The literature search also yielded an annotated bibliography. In addition to the PubMed search, the primer took into account pertinent gray literature available in the public domain on the websites of the ISO, healthit.gov, the U.S. Department of Health and Human Resources, the American Health Information Management Association, and others.

What do privacy, security, and confidentiality mean in the context of EHRs?

With rapid proliferation of EHRs, protecting and securing patient health information has become an important priority for healthcare providers. Countries have implemented policy and regulatory frameworks to guide and monitor implementation of laws and procedures to safeguard patient health information. In this context it is useful to understand the key concepts related to data security, privacy, and confidentiality.

The first important concept to understand is what EHR implies. The ISO 18308:2011 standard defines an EHR as

> *one or more repositories, physically or virtually integrated, of information in*

[9] HIMSS. n.d. "Interoperability 101." Available at: http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/Ambulatory%20Practices%20and%20the%20Importance%20of%20Interoperability.pdf.

[10] HIMSS. "Interoperability 101."

[11] HIPAA Act of 1996. n.d. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

[12] Health Information Technology for Economic and Clinical Health Act. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.

> *computer processable form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users, represented according to a standardized or commonly agreed logical information model. Its primary purpose is the support of life-long, effective, high quality and safe integrated healthcare.*

Another important concept related to EHR systems is **personal health information**. According to ISO 27799, this is information that relates either to the physical or mental health of an identifiable person or to the provision of health services to that person.[13] It may include information about patient registration, payment, or eligibility for healthcare; a unique patient identifier; disease and diagnostic details; and provider identification.

People have the authority to determine what information to share, with whom, and how.

In the United States, the 1996 HIPAA defines individually identifiable health information as

> *information, including demographic information, that relates to a) the individual's past, present, or future physical or mental health or condition, b) the provision of healthcare to the individual, or c) the past, present, or future payment for the provision of healthcare to the individual.*

HIPAA identifies 18 data elements that can identify a patient and thus constitute PHI. For example, if a diagnostic report includes the patient's name, Social Security card number, and/or zip code, it is considered PHI.

The U.S. National Institute for Standards and Technology (NIST) has also published guidance for protecting the confidentiality of personally identifiable information (PII).[14] Even though American health regulations are meant to protect PII, they do not prevent identification of individuals by use of publicly available PII shared through various web-based applications.[15]

Privacy in healthcare settings refers to people's right to control access to their personal information. People have the authority to determine what information to share, with whom, and how.[16] The HIPAA Privacy Rule protects the privacy of individually identifiable health information[17]; it does not apply to the use or disclosure of "de-identified health information," which implies that the data do not contain PHI.

Security refers to the protection measures and tools that safeguard health information and health information systems from any unauthorized access to or modification of information, denial of service to authorized

---

[13] U.S. Department of Health and Human Services. 2000; as amended April 17, 2003. "Standards for Privacy of Individually Identifiable Health Information." Available at: http://www.hhs.gov/ocr/privacy/hipaa/news/2002/combinedregtext02.pdf.

[14] McCallister, E., Grance, T., and Scarfone, K. 2010. "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." Washington, D.C.: National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=904990.

[15] Zou, X., Liu, P., and Chen, J. Y. 2011. "New Threats to Health Data Privacy." *BMC Bioinformatics*, 12 Suppl 12, S7-2105-12-S12-S7. Available at: http://www.biomedcentral.com/1471-2105/12/S12/S7.

[16] Johns, Merida L. 2008. "Privacy and Security of Health Information." In *Electronic Health Records: A Guide for Clinicians and Administrators*, edited by Jerome H. Carter. Philadelphia, PA: American College of Physicians.

[17] HIPAA, 2015.

users, and provision of service to unauthorized users. It has two components:

- Data security encompasses measures to safeguard data and computed programs from undesired occurrences and exposures
- System security covers safeguards associated with hardware, software, personnel, and enterprise-wide institutional policies[18]

The HIPAA Security Rule ensures the security of electronic protected health information (ePHI). NIST sets the following standard:

> *Security should be appropriate and proportionate to the value of and degree of reliance on the computer system and to the severity, probability and extent of potential harm. Requirements for security will vary depending on the particular organization and computer system.*[19]

The concept of **confidentiality** is intertwined with privacy and security and has been defined as either a tool to protect privacy or an act limiting disclosure of private matters.[20] The intent is to ensure that individual health information is used for the intended purpose only, and that patient consent is required for any disclosure.

Clear articulation of privacy, security, and confidentiality is foundational to the development and adoption of health informatics standards to prevent disclosure of PHI.

Confidentiality ensures that individual health information is used for the intended purpose only, and that patient consent is required for any disclosure.

What global standards guide the privacy, security, and confidentiality of health information in EHRs?

Standards are published documents that establish specifications and procedures designed to ensure the reliability of the materials, products, methods, and /or services that people use every day. Health informatics standards are set by both international and national standards organizations. For instance, ISO is the global authority for standards and ISO/TC215 is the ISO technical committee responsible for the standardization of health and medical informatics. The European Committee for Standardization (CEN) is the European authority for standards and CEN/TC251 is the technical committee responsible for standardization of health and medical informatics in Europe.[21] The American National Standards Institute (ANSI), a private nonprofit membership organization, approves official national standards in the United States.

These organizations inform and influence one another. For example, the ISO/TC 215 technical committee has adopted many CEN/TC 251 standards.[22] A systematic review of

---

[18] Johns, 2008.

[19] NIST, U.S. Department of Commerce. 1995. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12. Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

[20] Johns, 2008.

[21] European Committee for Standardization (CEN). 2015. "CEN/TC 251—Health Informatics." Available at: http://standards.cen.eu/dyn/www/f?p=204:7:0:::FSP_ORG_ID:6232&cs=18CA078392807EDD402B798AAEF1644E1.

[22] CEN. n.d. "Business Plan 2015–2018: CEN/TC 251, Health Informatics." Available at: http://standards.cen.eu/BP/6232.pdf.

privacy and security in EHRs found that the most widely used regulations are HIPAA and the European Data Protection Directive 95/46/EC.[23]

The draft of an international standard on health informatics—ISO/DIS 27799:2014(E)—identifies the following areas for ensuring information security: information security policies; organization of information security; human resources security; asset management; access control; cryptography; physical and environmental security; operations security; communications security; system acquisition; development and maintenance; supplier relationships; information security incidence management; information security aspects of business continuity management; and compliance.[24] In other words, the adoption and implementation of standards and compliance with those standards in a healthcare system are closely linked to political leadership and governance, laws and regulations, information technology and physical infrastructure, financial capacity, intra-and interorganizational relationships, and awareness of and education on privacy and security. The scope and operational details of these standards will vary with the healthcare setting. For example, implementing these standards within a hospital's pediatric department will require different levels of effort and resources than implementing them across all the departments or units.[25] The design and development of an international health information system enabling data exchange among country systems will not implement ISO standards in the same way that the design and development of in-country systems would implement them.[26]

> Having international and national health informatics standards in place is essential, but healthcare organizations must translate them into security and management practices for people's health information to be protected.

The International Information Systems Security Certification Consortium has created 10 security domains. The consortium's purpose is to provide common knowledge and define key terms for information security professionals. These domains are valid for all industries, including healthcare. They are:

- Security management practices
- Access control systems and methods
- Telecommunications and networking security
- Cryptography
- Security architecture and models
- Operations security
- Application and systems development security
- Physical security
- Business continuity and disaster recovery planning
- Laws, investigation, and ethics[27]

---

[23] Fernández-Alemán, J.L., et al. 2012. "Security and Privacy in Electronic Health Records: A Systematic Literature Review." *Journal of Biomedical Informatics* 46(3): 541–562. Available at: http://www.sciencedirect.com/science/article/pii/S1532046412001864.

[24] International Organization for Standardization (ISO). 2013. "Draft International Standard ISO/DIS 27799: Health Informatics–Informatics Security Management in Health Using ISO/IEC 27002." Available at: https://www.iso.org/obp/ui/#iso:std:62777:en.

[25] Fernández-Alemán, J.L., et al., 2012.

[26] Li, J. S., Zhou, T. S., Chu, J., Araki, K., and Yoshihara, H. 2011. "Design and Development of an International Clinical Data Exchange System: The International Layer Function of the Dolphin Project." *Journal of the American Medical Informatics Association* 18(5), 683-689. Available at: http://www.ncbi.nlm.nih.gov/pubmed/21571747.

[27] American Health Information Management Association (AHIMA). 2012. "The 10 Security Domains." Journal of AHIMA 83(5): 48–52. Available at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049602.hcsp?dDocName=bok1_049602.

Having international and national health informatics standards in place is essential, but healthcare organizations must translate them into security and management practices for people's health information to be protected.

How can an organization plan and implement processes to ensure the privacy, security, and confidentiality of PHI in an EHR system?

When security- and privacy-related challenges are addressed, personal health records offer numerous benefits to patients.[28] Even though the security and privacy of the health information in any EHR depends on technology and standards, healthcare providers have the prime responsibility to safeguard them.[29] Information security involves a number of nontechnical factors, such as organizational policy; human resources; communication networks, roles, and processes; monitoring; and compliance.[30] A systematic review of the literature on the privacy and security of health information in EHRs found that only 26 of the 49 selected articles considered the use of standards or regulations as tools to protect EHR data. Most of the studies looked at access control issues, but only four mentioned training systems users and/or health staff in security and privacy, even though most HIPAA data breaches are related to theft or loss.[31] One study showed that inadequate identification and authentication of users, unauthorized access by users, inadequate monitoring of user activity, inappropriate disclosure and reporting requirements, and poor security are chief sources of privacy breaches.[32] Implementation of ISO standards can easily address these problems.

In interorganizational healthcare data exchange settings, healthcare providers covered under a PHI law must ensure that their business associates comply with data security provisions. For example, HIPAA's organizational requirements for data security govern business associate agreements. The entities covered under an agreement must obtain a written contract with business associates who handle ePHI, requiring them to implement administrative, physical, and technical safeguards to ensure confidentiality, integrity, and availability of the ePHI that is created, received, maintained, or transmitted on behalf of the covered entity. This contract enforces HIPAA's requirement for business associates to report any security incidents they become aware of to the covered entity. The contract provides for termination of the agreement if a business associate violates one of its material terms.

The HIPAA security guide provides the following sample seven-step process for implementing a security management process:

Step 1: Lead Your Culture, Select Your Team, and Learn
Step 2: Document Your Process, Findings, and Actions
Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis)
Step 4: Develop an Action Plan
Step 5: Manage and Mitigate Risks

---

[28] Carrion, I., Aleman, J. L., and Toval, A. 2011. "Assessing the HIPAA Standard in Practice: PHR Privacy Policies." *Conference Proceedings: Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE Engineering in Medicine and Biology Society. Annual Conference, 2011, 2380–2383. Available at: http://www.ncbi.nlm.nih.gov/pubmed/22254820.

[29] HIPAA, 2015.

[30] Mense, A., Hoheiser-Pfortner, F., Schmid, M., and Wahl, H. 2013. "Concepts for a Standard Based Cross-Organisational Information Security Management System in the Context of a Nationwide EHR." Studies in *Health Technology and Informatics 192*, 548–552. Available at: http://www.ncbi.nlm.nih.gov/pubmed/23920615.

[31] Sade, R. M. 2010. "Breaches of Health Information: Are Electronic Records Different from Paper Records?" *The Journal of Clinical Ethics, 21*(1), 39–41. Available at: http://www.ncbi.nlm.nih.gov/pubmed/20465074.

[32] Neame, R. L. 2014. "Privacy Protection for Personal Health Information and Shared Care Records." *Informatics in Primary Care, 21*(2), 84-91. Available at: http://hijournal.bcs.org/index.php/jhi/article/view/55/84.

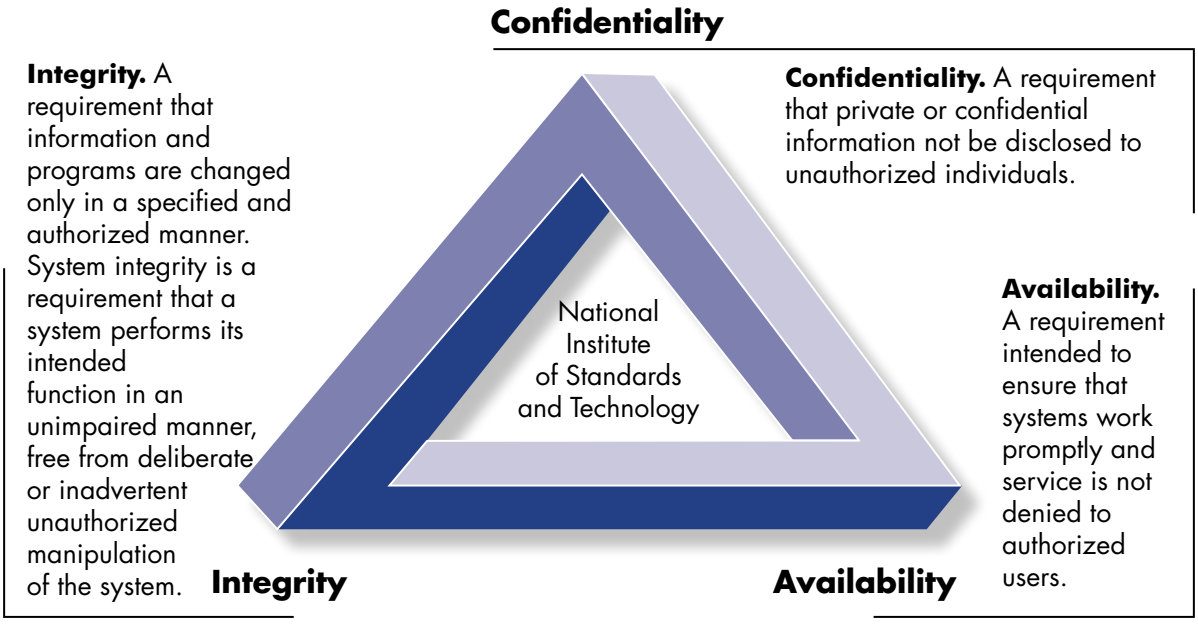
Step 6: Attest for Meaningful Use Security-Related Objective

Step 7: Monitor, Audit, and Update Security on an Ongoing Basis [33]

NIST's "Confidentiality, Integrity, and Availability Triad" (see graphic) is a sound framework with which to analyze an organization's security management practices.[34]

Rapid growth in cloud computing and mobile and wearable devices has enhanced capacity for the virtual exchange of health information but has also increased cybersecurity risks. Mitigating them demands organizational, technological, regulatory, and system user-focused interventions. These can include building a culture that promotes security, protecting mobile devices, limiting physical access, implementing application- and infrastructure-level security measures, and engaging system users.[35] Implementing ISO or national cybersecurity standards to support oversight and accountability mechanisms can address cyber threats in healthcare settings.

CONFIDENTIALITY, INTEGRITY, and AVAILABILITY TRIAD



Source: Adapted from National Institute of Standards and Technology. 1995. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12. Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

[33] HealthIT.gov. 2015. "Sample Seven-Step Approach for Implementing a Security Management Process." Available at: http://www.healthit.gov/providers-professionals/sample-seven-step-approach-implementing-security-management-process.

[34] NIST, U.S. Department of Commerce, 1995.

[35] HealthIT.gov. 2015. "Top 10 Tips for Cybersecurity in Health Care." Available at: http://www.healthit.gov/providers-professionals-newsroom/top-10-tips-cybersecurity-health-care.

MEASURE Evaluation
University of North Carolina at Chapel Hill
400 Meadowmont Circle, 3rd floor
Chapel Hill, North Carolina 27517 USA
measure@unc.edu
www.measureevaluation.org

MEASURE Evaluation is funded by the U.S. Agency for International Development (USAID) under terms of Cooperative Agreement AID-OAA-L-14-00004 and implemented by the Carolina Population Center, University of North Carolina at Chapel Hill in partnership with ICF International, John Snow, Inc., Management Sciences for Health, Palladium, and Tulane University. The views expressed in this presentation do not necessarily reflect the views of USAID or the United States government. SR-15-128

USAID
FROM THE AMERICAN PEOPLE

MEASURE
Evaluation