

Distribution Agreement

In presenting this report as a partial fulfillment of the requirements for an advance degree from Emory University, I agree that the School of Public Health shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to copy from, or to publish this report may be granted by the professor under whose direction it was written, or in his/her absence, by the Director of Career Education, when such copying or publication is solely for scholarly purposes and does not involve potential financial gain. It is understood that any copying from, or publication of this report, which involves potential financial gain will not be allowed without written permission.

Nikki Williams Sebastian

Date:

UNIQUE PATIENT IDENTIFIERS AND
IMMUNIZATION INFORMATION SYTEMS:
BENEFITS TO CONSIDER

BY

Nikki Williams Sebastian
Degree to be Awarded: MPH
Executive MPH

Frederick Grant PhD, MPH, MBA, Chair

Date:

Janet Fath, PhD, Committee Member

Date:

Laura Gaydos, MPH, PhD
Associate Chair for Academic Affairs, Executive MPH Program

Date:

UNIQUE PATIENT IDENTIFIERS AND
IMMUNIZATION INFORMATION SYTEMS:
BENEFITS TO CONSIDER

BY

Nikki Williams Sebastian
M.P.H., Emory University, 2017
B.A., Tulane University, 1995

Thesis Committee Chair: Frederick Grant PhD, MPH, MBA

An abstract of

A Thesis submitted to the Faculty of the
Rollins School of Public Health of Emory University
in partial fulfillment of the requirements of the degree of
Master of Public Health in the Executive MPH program
2017

Abstract

INTRODUCTION: Currently, the United States is not developing a unique patient identifier (UPI) to use as a singular key to accurately link, file, and retrieve individual health records. Although the existing Congressional prohibition against using federal funds to develop UPIs remains, in early 2017, a House committee advised it does not prohibit the examination of ways to effectively and accurately identify patients.

AIM: The purpose of this research is to 1) examine existing legal framework surrounding why UPIs are currently banned for use in the U.S. healthcare system 2) perform a literature review of current methodologies of identifying patients 3) review existing UPI proposals and the feasibility of UPI implementation into existing IIS.

METHODS: The research performed in this thesis takes place in three stages: 1) An analysis of federal legislation and private industry publications to examine the Congressional ban on the use of unique patient identifiers in the U.S. healthcare system. 2) A comprehensive review of public health literature to identify patient-matching protocols and investigate how patient identities are determined without the accuracy and stability provided by unique identifiers. 3) A general review of publications that detail IIS data quality challenges resulting from the lack of UPIs.

RESULTS: The results of this thesis are organized into three stages, 1) Legislative analysis results, 2) Systematic literature review results, and 3) IIS data analysis results.

DISCUSSION: Evidence suggests that UPIs would improve efficiency and data quality of IIS by eliminating duplicate records and by allowing for accurate data exchange to facilitate more efficient tracking of immunization histories. This can only be achieved through federal legislation that addresses confidentiality, privacy, and security concerns of sharing data across nationally distributed electronic health information networks. Public education, engagement, understanding and acceptance of UPIs will also be required in order to realize their full potential. Informed by the literature, a clear case exists that IIS would benefit from the implementation of UPIs.

Acknowledgements:

The author would like to acknowledge:

Sylnice Williams, MAEd,
Deidre Griffith, M.P.H,
Lauren Drummond, M.T.S,
Del Jupiter, M.S.L.S.,
Janet Fath, PhD,
and Frederic Grant, PhD, MPH

for their continued inspiration, support and encouragement.

TABLE OF CONTENTS

Chapter I: INTRODUCTION	1
1.1 Background	1
1.1.1 Immunization Information Systems	1
1.1.2 Challenges with IIS Data Quality	3
1.1.3 Patient Identification in the U.S. Healthcare System	3
1.1.4 Inefficiencies in the Healthcare System	5
1.1.5 Unique Patient Identifiers (UPIs)	6
1.2 Purpose	7
1.2.1 Thesis Organization	7
1.3 Research Questions	9
1.4 Table 1: Definition of Key Terms	10
Chapter II: REVIEW OF THE LITERATURE	13
2.1 Introduction	13
2.1.1 Literature Review Strategy	13
2.2 Summary	14
2.2.1 Table 1: Literature Review Search Terms	14
2.2.2 Healthcare Privacy Legal Framework	17
2.2.3 Impact of HIPAA on State and Local laws	18
2.2.4 HIPAA’s Impact on the Implementation of UPIs	18
2.2.5 Patient Identification Methodologies	21
2.2.6 IIS	21
Chapter III: METHODS	24
3.1 Introduction	24
3.2 Procedures	25
3.2.1 Stage 1: Systematic Review of Federal Legislation	25
3.2.1.1 Stage 1: Summary	30
3.2.2 Stage 2: Systematic Review of Patient Matching Methods	30
3.2.2.1 Master Patient Indexes (MPIs)	31
3.2.2.2 Statistical Matching	32
3.2.2.3 Biometrics	34
3.2.2.4 Social Security Numbers (SSNs)	34
3.2.2.5 Stage 2 Summary	36

3.2.3	Stage 3: General Analysis of IIS Data	37
3.2.3.1	Stage 3: Summary.....	39
3.3	Procedures Summary	40
Chapter IV:	RESULTS	41
4.1	Introduction	41
4.2	Findings	41
4.2.1	Stage 1: Legislative Analysis Results	41
4.2.2	Stage 2: Systematic Literature Review Results	45
4.2.2.	Analysis of UPI Proposals	45
4.2.2.1	Data Encryption Proposals	46
4.2.2.2	National ID Cards.....	47
4.2.2.3	Private Sector UPI Initiatives.....	48
4.2.3.	Stage 3: IIS Data Analysis Results	49
4.2.3.1	Pharmacies and IIS	52
4.3	Chapter IV Results Summary	54
Chapter V:	DISCUSSION.....	57
5.1	Discussion of Research Questions	57
5.2	Key Findings	58
5.2	Recommendations.....	58
5.3	Conclusions.....	59

List of Figures

- Figure 1 Recommended Immunization Schedule for Children and Adolescents Aged 18 Years or Younger, United States, 2017
- Figure 2 Recommended Immunization Schedule for Adults Aged 19 Years or Older by Age Group, United States, 2017
- Figure 3 UPI Legal Framework Timeline

Chapter I:

INTRODUCTION

1.1 Background

The purpose of this thesis is to discuss why unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research will review the reasons why UPIs have not been implemented into the United States healthcare system and this research will also investigate how patients are commonly identified without the benefit of UPIs.

This chapter will provide an overview of immunization information systems (IIS) and discuss their important role in the US healthcare system and will introduce a common challenge across IIS; how to accurately identify patients. This chapter will also provide an overview of UPIs and explain why they are the solution to a more modern, robust, and reformed healthcare system.

1.1.1 Immunization Information Systems

Current up-to-date immunizations protect individuals, families and communities from disease. Since patients often receive vaccinations from multiple providers who may not communicate with each other, it is challenging to achieve a consolidated record that contains patient vaccination and also patient demographic data. A consolidated patient record is necessary to document the vaccinations received and to determine vaccinations that are still needed.

In order for immunization records to remain current, healthcare providers must record each immunization in their organization's internal proprietary database system and then report

the event to their local immunization information systems (IIS), also known as vaccine registries. The Centers for Disease Control and Prevention (CDC) defines IIS as confidential, population-based, computerized databases that record all immunization doses administered by participating providers to patients residing within a given geopolitical area. IIS help to eliminate and control the spread of vaccine preventable diseases listed in Figure 1.

A patient could request a healthcare provider also update his own personal immunization record that he maintains for himself, which he can share with other providers. Patients today have different types of providers with expertise in specific areas of healthcare. Each healthcare provider operates and maintains their own unique and disparate patient identification methods for use within their own practices and within their healthcare systems. When patients change providers, pharmacies, or laboratories due to changes in employment or relocations, or as they transition into adulthood, their patient records must travel with them to ensure they receive appropriate care and treatments. Complete patient records ensure providers have the information they need to make informed clinical decisions. (Greenberg, 2009)

Providers that administer vaccines typically do not exchange patient immunization data with other providers outside of their network. Instead, they may or may not participate in a formal IIS which are responsible for tracking immunization information for particular jurisdictions. As a public health concern, it is the responsibility of federal, state and local authorities, in conjunction with healthcare providers and community partners to prevent and control diseases. (Johnson Foundation, 2013). As a result, immunization information systems serve vital roles in the US healthcare system. IIS link health care delivery with population-based data. IIS provide a logical basis for the establishment of National Health Information Networks (NHINs) which link electronic health records (EHRs) and other health information systems.

Because of NHINs, patient records, including immunization records, can be electronically transmitted through electronic data exchanges.

1.1.2 Challenges with IIS Data Quality

Accurate patient identification is a critical component of IIS. These systems consolidate immunization records from multiple data sources; providers, schools, pharmacies, for example, for multiple vaccines and for a series doses for the same vaccines. The duplication of immunization records is a concern of many IIS managers. Duplicate records undermine credibility of IIS data which is used to establish policies and make financial decisions. Duplicate records make it difficult to determine the needed vaccinations for an individual patient. When an IIS patient has at least one additional immunization record that is identical, it then becomes logically impossible to distinguish that patient's record from another patient's whose immunization record also contain the same data elements.

To a lesser extent, duplicate immunization records affect usage reporting and therefore negatively impact vaccine forecasting abilities as well. Accurate immunization histories are needed to effectively manage vaccine purchases for annual immunization spend plans. (MIROW, 2006)

1.1.3 Patient Identification in the U.S. Healthcare System

IIS do not exist in isolation. In the U.S., each state or local government operates its own system which may be developed and maintained by their own employees or the IIS may be developed through contracts with 3rd party vendors. Due to the variety of platforms used for IIS development and maintenance, organizations such as the American Immunization Registry Association (AIRA) and the CDC develop and promulgate guidelines for functional standards,

guidelines, and best practices. (AIRA, 2017) But even with their guidelines, the lack of an UPI inhibits the accuracy of matching patient records.

IIS are participants in the overall U.S. healthcare system and are subject to local, state, and federal legislation. Overall, how is other non-immunization patient information collected and tracked for over 320 million Americans? Common methods for identifying patients includes master patient indexes, statistical matching, biometric data, and the use of social security numbers. (Arzt, 2017)

Master patient indexes are medical database that contains information on every patient registered at a particular healthcare organization. Different healthcare organizations use their own MPIs as there is no national MPI available to all healthcare providers. Statistical patient matching involves the use of algorithms of patient demographic data fields to match patients to their medical records. (Hillestad, 2008) Biometric identifiers are personal attributes such as fingerprints and retinal scans, for example, that are not prone to keying or data entry errors. Social security numbers, typically combined with other data fields, are by default the most commonly used method to identify patients.

Patient records collected over the course of one's lifetime are not tracked on a national cohesive scale. A national patient identification strategy would ensure the accurate, timely, and efficient matching of patients to their lifetime healthcare information. (Leonard, 2009) UPIs could accurately link of all patient information from a variety of healthcare settings including hospitals, schools, universities, the armed forces, employer sponsored occupational health programs, insurance companies, pharmacies, laboratories, dentist offices, public health clinics, correctional facilities, and nursing homes, and other healthcare systems. (White, 1997) Each of

these healthcare organizations implement and maintain their own unique proprietary patient identification methods. Typically, these systems are not integrated with other organizations regardless of the fact that they, over time, can very likely share the same patients. Sometimes these healthcare providers are business competitors vying to provide treatments and procedures for the same patients.

Correctional facilities for example, face unique patient matching challenges. Every year, approximately ten million individuals are incarcerated in 3,300 local and county U.S. jails. These inmates eventually become patients in these facilities which typically health care to a highly mobile, largely uninsured populations with higher-than average rates of mental illness, substance abuse, and chronic diseases. (Butler, 2014) Correctional facilities often provide care without access to their patient's complete healthcare or immunization records accumulated outside of the correctional systems. Only four states, Florida, New York, Massachusetts and Oregon, out of 62 states and territories, have implemented electronic health record (EHR) systems that interface with correctional facilities, pharmaceutical systems, and the electronic medication administration records. (Butler, 2014)

1.1.4 Inefficiencies in the Healthcare System

Mergers and acquisitions in the healthcare industry have resulted in fragmented and incompatible IT systems. Patient-matching methodologies become more complex with each new merger and acquisition. (AIRA, 2013) Multiple patient records can exist within a single institution. Multiple patient records may exist across several institutions within the same healthcare system. Some healthcare software vendors have ceased their operations and left their providers with orphaned electronic healthcare (EHR) systems with unsupported data that cannot be easily imported into other systems. (Lumpkin, 2009)

UPIs would improve access to healthcare information and promote efficiencies by eliminating costly redundancies in patient labs, tests, and procedures. (Gliklich, 2014) Health care costs reached \$1 trillion in spending the early 1990s. As of 2016, the Associated Press (AP) claimed healthcare spending reached approximately \$3.35 trillion with growth projected to average 5.8 percent from 2015 to 2025. Blue Cross Blue Shield (BCBS) also reports healthcare spending is currently at three trillion dollars a year. Who currently benefits from the way the healthcare system is currently structured, operated, and maintained, at the current level of expenditures?

In the early 1990s, businesses, consumers, think tanks, and insurers raised the call for mechanisms to manage escalating healthcare costs. A consolidated, integrated healthcare system which includes IIS, that can identify and analyze patient records for accuracy could also be achieved with the implementation UPIs.

1.1.5 Unique Patient Identifiers (UPIs)

Providing an option to link health information in a regional or NHIN of different provider types can only be achieved by the implementation of a national patient identification strategy that is based on unique patient identifiers, where a unique ID is assigned to every patient. A UPI is one identifier assigned to one patient that is used by all types of healthcare systems to ensure the accurate, timely, and efficient matching of patients to their complete healthcare record. UPIs must support 1) Identification of an individual, 2) Identification that individual's health information, and 3) Support patient record management and sharing. (Appavu, 1997) The most commonly exchanged patient information includes laboratory results, prescription information, laboratory, and radiology results. (Hinman, 2010)

But the public health literature indicates concerns with how the emerging NHIN architecture, connectivity, and interoperability impacts patient privacy. NHINs are a centralized means to share electronic health information. NHINs should facilitate the exchange of patient information according to nationally recognized standards, but they do not yet because coordinated national standards for the electronic exchange of patient information do not yet exist.

Nevertheless, although no definitive count exists of the number of NHINs currently in operation, their popularity continues to rise. Nearly half of health information exchanges (71 of 150 exchanges contacted) reported that they are not dependent on federal funding. They reported state or local government involvement in their development efforts. (Martin, 2015)

Congress recognized these types of advances in technology could possibly erode the privacy of health information. In 1999, Congress passed the Privacy Rule, Public Law 105-277, the *Standards for Privacy of Individually Identifiable Health Information*, which prohibited the Department of Health and Human Services (HHS) from using any of its federally appropriated funds to develop a UPI without express Congressional approval.

1.2 Purpose

1.2.1 Thesis Organization

Chapter I presented an overview of the need for UPIs. Chapter II: Literature Review will present analyses in three primary areas 1) Federal legislation that covers patient identification and the use and disclosure of protected health information (PHI) to investigate security and privacy concerns regarding UPIs. 2) Research into patient matching methodologies, and 3) Research into grey literature or non-traditional materials and research produced by organizations outside of the traditional commercial or academic publishing and distribution channels for

discussion implementation of UPIs in IIS. This was necessary because this area of research, UPIs and IIS, is still a relatively new approach to a public health informatics problem.

Chapter III: Methods will explain how the research performed in this thesis takes place in three stages, 1) A systematic review federal legislation pertaining to healthcare privacy with specific emphasis on UPIs. 2) A systematic review of public health literature with emphasis on four popular patient-matching protocols: MPIs, statistical patient matching, biometrics, and social security numbers (SSNs), to examine how patient identities are determined without the accuracy and stability provided by unique identifiers. 3) A general review of grey literature/non-traditional reports and presentations that discuss IIS patient de-duplication problems in order to identify and illustrate specific opportunities for UPI implementation; immunization registries.

Chapter IV: Results chapter will discuss the findings of this research and address the primary research question, “What are the implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system?”

Chapter V: Discussion will report the outcomes of this thesis and will review the implications of the Congressional ban on UPIs to immunization information systems (IIS).

This thesis has three specific objectives, to: 1) Determine why UPIs are currently banned for use in the U.S. healthcare system and 2) Examine benefits, limitations, and privacy and security concerns of four current patient-matching methodologies, and 3) Explain how UPIs would improve the effectiveness and efficiency of one component within the overall U.S. healthcare system, or immunization registries.

This thesis is intended for public health executives and leaders, as well as for readers who are looking for brief high level information on how the implementation of UPIs could provide

benefits to the healthcare system and therefore to IIS as well. Expected benefits of implementing UPIs into immunization information systems are included in this thesis.

1.3 Research Questions

This thesis set out to examine these issues by asking the following three research questions:

- 1) Why are UPIs banned for use in the U.S. Healthcare system?
- 2) With no UPI available, what are the benefits and limitations of the methodologies currently in place to identify patients in the US healthcare system?
- 3) What are some implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system?

1.4 Table 1: Definition of Key Terms

Term	Definition
American Immunization Registry Association (AIRA)	Promotes the development and implementation of immunization information systems (IIS) as an important tool in preventing and controlling vaccine preventable diseases.
American Recovery and Reinvestment Act of 2009 (ARRA)	Economic stimulus package intended to boost the US economy in the wake of the 2008 economic downturn. Provisions included \$19 billion for Health Information Technology (HIT) initiatives including incentive program to encourage eligible providers and hospitals to adopt and use EHR technologies
American Society for Testing and Materials (ASTM)	Standards body in 1995 defined a set of requirements outlining the properties required to create a unique healthcare identifier (UHID) system.
Assistant Secretary for Planning and Evaluation (ASPE)	Principal advisor to HHS Secretary on policy development and is responsible for major activities in policy coordination, legislation development, strategic planning, policy research, evaluation, and economic analysis.
CHIN	Community Health Information Network (of Providers)
Clinical Data Interchange Standards Consortium (CDISC)	Mission is to develop and support global, platform-independent data standards that enable information system interoperability to improve medical research and related areas of healthcare.
Centers for Medicare & Medicaid Services (CMS)	HHS Agency that administers Medicare, Medicaid, the Children's Health Insurance Program (CHIP), and the Health Insurance Marketplace.
Computer-based Patient Record Institute (CPRI)	Workgroup established in 1992 to encourage creation of confidentiality, privacy, and security policies and the implementation of mechanisms that protect patient privacy. Deemed "the focal point" of legislation demanding automated patient records.
Electronic Health Record (EHR)	An electronic version of a patient's medical chart stored within an IT system.
General Practice Immunization Incentives (GPII)	A healthcare not-for-profit company formed in 2008 with a focus on accurately matching patients to their healthcare records and improving patient privacy.

Government Accountability Office (GAO)	An independent, nonpartisan agency that works that investigates how the federal government spends taxpayer dollars.
Department of Health and Human Services (HHS)	Cabinet-level agency responsible for enhancing and protecting the health and well-being of all Americans by providing for effective health and human services and fostering advances in medicine, public health, and social services.
Healthcare Information and Management Systems Society (HIMSS)	Global, cause-based, not-for-profit organization focused on better health through information technology (IT) formed in 1961. HIMSS leads efforts to optimize health engagements and care outcomes using information technology.
Health Information Networks (NHIN)	The ONC has provided funding for a number of health IT programs, including the development of the Nationwide Health Information Network (NHIN)—a set of standards, services, and policies that enable the secure exchange of health information over the Internet.
Health Information Technology for Economic and Clinical Health. (HITECH)	Legislation designed is to spread the use of health IT to achieve five key goals by using incentives to providers.
Health Level 7 (HL7)	Set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers. Messaging standard for EHRs.
Immunization Information Systems (IIS)	Confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area.
Master Patient Index (MPI)	An electronic medical database that contains information on every patient registered at a healthcare organization. An MPI may also include data on physicians, other medical staff and facility employees.
Modeling of Immunization Registry Operations Workgroup (MIROW)	Sponsored by AIRA, An initiative directed at the analysis and improvement of Immunization Information System (IIS) operations.
National Committee on Vital and Health Statistics (NCVHS)	Statutory public advisory body to the Secretary of Health and Human Services on health information policy.

National Health Information Networks (NHIN)	Program within the Office of the National Coordinator for Health Information Technology (ONC), established in 2004 to improve the quality and efficiency of healthcare by establishing a mechanism for nationwide health information exchange.
Office of the National Coordinator for Health Information Technology (ONC), 2004	Supports a Presidential administration's health IT efforts. Resource to the entire health system to support the adoption of health information technology and the promotion of nationwide health information exchange to improve health care. ONC is located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS).
Public Law 104-191 - Health Insurance Portability and Accountability Act of 1996 (HIPPA)	Establishes legal sanctions for wrongful disclosure of individually identifiable health information.
RHIN	Regional Health Information Network (of Providers)
The Family Educational Rights and Privacy Act (FERPA), 1974	Federal privacy law that gives parents certain protections with regard to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules.
Unique Patient Identifier (UPI)	One identifier assigned to one patient to be used by all types of healthcare systems to ensure the accurate, timely, and efficient matching of patients to their complete healthcare record.

Chapter II:

REVIEW OF THE LITERATURE

2.1 Introduction

The purpose of this thesis is to discuss why unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research will review the reasons why UPIs have not been implemented into the United States (US) healthcare system and this research will also investigate how patients are commonly identified without the benefit of UPIs.

Chapter II outlines the literature review strategy which resulted in three primary areas 1) an analysis of pertinent federal legislation that covers patient identification and the use and disclosure of protected health information (PHI) to examine how UPI would fit into the current legal landscape that currently exists. 2) An analysis of previous peer reviewed research into patient matching methodologies, and 3) Materials and research that discuss IIS produced outside of the traditional peer review and governmental publishing and distribution channels such as private industry journals and white papers.

2.1.1 Literature Review Strategy

A review of literature published primarily between 2000 and 2017 was conducted using the search terms contained in Table 1. Research published prior to 2000 but after 1994, included literature that first addressed the need for UPIs that was published in the mid-1990s. This was necessary in order to properly credit organizations that initiated discussions for the need UPIs in healthcare. The literature review included peer reviewed publications, government publications, grey literature.

2.2 Summary

The following terms illustrated in Table 1 were used to conduct the public health literature review:

2.2.1 Table 1: Literature Review Search Terms

MeSH Terms:

1. Consolidate
2. Data
3. Feasibility
Identification
Identifier
Immunization
4. Informatics
5. Patient
6. Record Registry
7. Unique Patient Identifiers
8. UPI
9. UPI Implementation
10. Vaccine Registries
11. Validating

Text Terms:

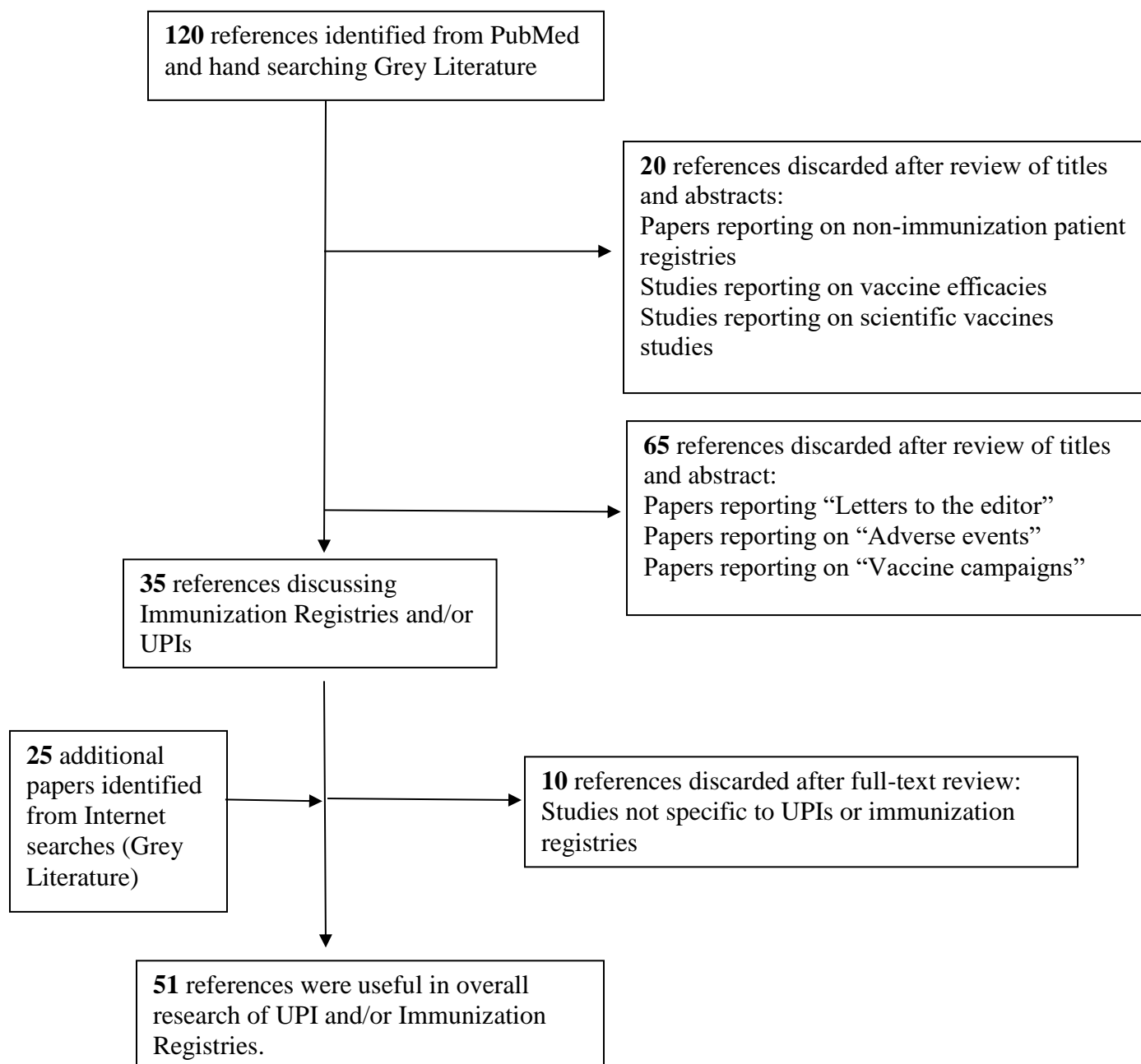
1. "Computer security"
2. "Costs Benefits of IIS"
3. "Data Integration"
4. "Health Reform"
5. "Immunization Programs"
6. "Immunization Utilization"
7. "Lifespan Registries"
8. "Medical Records"
9. "Medical Registries"
10. "Automatic data processing and immunizations"
11. "Computerized Health Identification"
12. "Health Identification Strategy"
13. "Health Identifiers and Registries"
14. "Registry Privacy"
15. "Unique Health Identification"
16. "UPIs and Immunizations"
17. "Unique Health Identifiers and Immunizations"
18. "Unique Health Identifier"
19. "Vaccine Registry Health Identification"

The PubMed MeSH terms search string, "*Registry, Immunization, Informatics*" was most successful and yielded 99 relevant results. With non-traditional sources included, the total starting point was 120 references. Studies that discussed immunization efficacies, scientific vaccines studies, and non-immunization registries were discarded.

"Letters to the Editor" were discarded along with references about adverse vaccine events. References that did not in any way discuss UPIs or immunization registries were also discarded. In the end, 51 peer-reviewed, government published reports, and white papers identified as helpful to this overall research.

One hundred and twenty initial references were analyzed according to their content.

Items were discarded after review of titles, abstracts, and key words determined they did not the desired objectives, discussion of IIS and or UPIs:



The American Society for Testing and Materials (ASTM) first proposed six options for a unique identifier in 1995 in their *Standard Guide for Properties of Universal Healthcare*

Identifiers. (UHIDs) (ASPE, 2012)

1. Social Security Numbers (SSN)
2. Biometric Identifiers
3. A Directory Service
4. Personal Immutable Properties
5. Patient IDs based on existing Medical Record Numbers
6. Public Key-Private Key Cryptography Method.

Currently, the literature review found proposals for unique identifiers generally fall into similar classes based on ASTM's initial recommendations: 1) SSNs 2) UPIs not based on SSNs, 3) A directory service that combines patient characteristics such as social characteristics (name, SSN, address, driver license etc.), biometrics characteristics and other groupings such as sex, and race. 4) Personal immutable properties which are not easily changed such as last name, town, state, or country. (HHS, 1997)

Overall, discussion of UPI in general are well documented. But implementation of UPIs to specific areas of the healthcare system, is not widely available. There should be literature to discuss implementation of UPIs in specific areas such hospital systems or in correctional facilities, to name a few.

The literature also documents the legislation associated with health care privacy and security. Comprehensive Federal legislation is publically available information.

Literature regarding proposals for the use of UPI in IIS is not widely available.

2.2.2 Healthcare Privacy Legal Framework

The United States has no comprehensive federal law governing the collection and use of health information. (AIRA 2016) Several pieces of legislation were reviewed to develop an understanding of the legal framework associated with UPIs. This included the 1996 Health Insurance Portability and Accountability Act (HIPAA), which provides national standards that form the baseline of health information privacy protections. This means in general, an entity covered by HIPAA may not use or disclose protected health information unless authorized by the individual who is the subject of the information. HIPAA does permit the use and disclosure of protected health information without authorization for treatment, payment, health care operations and for public health purposes. (AIRA 2016)

The subsequent Privacy Rule of 2000, clarified who HIPAA covers and what patient information is protected, and also how protected health information can be used and disclosed. The associated Security Rule of 2003, determined what safeguards are to be in place to ensure appropriate protection of electronic protected health information. (HHS, 2017)

The 563-page Omnibus Final Rule of 2013 was implemented to modify the Privacy and Security rules in order to implement the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, created to stimulate the adoption of electronic health records (EHRs). This Omnibus Final Rule strengthened the privacy and security protections for individuals' personal health information by increasing penalties for HIPAA violations, with a maximum penalty of \$1.5 million per violation. The Omnibus rule also, among other things, prohibited the sale of health information without appropriate permissions.

The HIPAA Breach Notification Rule was also implemented in 2009 as part of the HITECH act. This rule states HIPAA covered entities and their business associates must provide notification following a breach of unsecured protected health information.

The Family Educational Rights and Privacy Act of 1974 (FERPA) legislation was analyzed because it covers IIS data. FERPA protects the privacy of student education records and grants rights regarding those education records. It governs school records and also requires that parents or guardians provide consent to release immunization information contained in an education record.

This patchwork of federal, state, and local laws and policies presents challenges for both intra and interstate exchange of immunization information. (Martin, 2015)

2.2.3 Impact of HIPAA on State and Local laws

As federal legislation, HIPAA preempts contrary or any less restrictive state or local laws. But HIPAA does not preempt more restrictive state laws that govern health information privacy. State and local IIS managers have to consult with their own legal representatives to determine the impact of HIPAA on local IIS.

Declaration of an emergency may affect the way that IIS information can be used and disclosed under state, local and territorial laws. An emergency declaration might affect who has access to information under what circumstances and requirements for consent or notification, among other impacts. (AIRA, 2016)

2.2.4 HIPAA's Impact on the Implementation of UPIs

HIPAA governs the activities of HIPAA-covered entities (CEs) and their business associates. CEs are health care providers, health plans and health care clearinghouses that transmit standard transactions electronically. The entity (state or local agency) managing the IIS

may or may not be a CE, depending on the entity's structure. Local health departments (LHDs) are either locally governed, are governed by the state, or they can be governed by both state and local governments. How LHDs are governed typically depends on the size of the population served. Usually small LHDs usually serve less than 50,000 people. Medium LHDs serve between 50,000 and 499,000 people. Large local health departments typically serve over 500,000 people. (NACCHO, 2016)

One study surveyed 49 states, 3 municipalities (New York City, Philadelphia, and San Antonio, each of whom operates an IIS independent of its respective state), and the District of Columbia, for a total of 53 participants. (Martin, 2015) Approximately 45% of IIS consider themselves to be a CE under HIPAA. An entity that submits immunization data to an IIS may or may not be a CE. Immunization providers, hospitals and health insurers are, in general, CEs under HIPAA which considers IIS to be a public health authorities. An IIS must determine for itself if it is governed by HIPAA and if so, whether the use or disclosure of protected information is required or permitted by HIPAA. A 2015 Public Health Informatics Institute (PHII) survey found that twenty-four (45.3%) of IIS were considered by their programs to be covered entities under HIPAA, 25 (47.2%) were considered to not be covered entities under HIPAA, and 4 (7.5%) IIS did not know whether their IIS was considered to be a covered entity under HIPAA. (Martin, 2015)

HIPAA allows CEs the use of a limited data set of protected health information (PHI) which may be used and disclosed for research, health care operations, and for public health purposes. It allows for the use of limited PHI data that excludes specific identifiers of individuals, their relatives, and their employers. This means UPIs would be HIPAA-compliant as long as they do not include the following types of direct identifiers: (AIRA, 2016)

Names	Postal address information	State code
Zip code	Telephone numbers	Medical record (chart) numbers
SSNs	Provider ID numbers	Health plan (insurance) IDs
Medical device IDs	Certificate numbers	License numbers

Publications from the U.S. Department of Health & Human Services (HHS) overall, provided the bulk of federal publications used in this research. HHS would be the federal agency tasked with UPI implementation, should Congress mandate such legislation. HHS' 1997 *Analysis of Unique Patient Identifier Options*, by Soloman Appavu, was the primary reference for HHS' official position on UPIs.

A number of HHS sub-agencies published reports related to the different aspects of UPI development and implementation. The Office of the Assistant Secretary for Planning and Evaluation (ASPE), tasked with advising the HHS Secretary on policy development related to health, disability, and human services, provides analyses on economic policy. ASPE developed a white paper that discusses the requirements for a unique health identifier for individuals. (ASPE, 2012)

The National Committee on Vital and Health Statistics (NCVHS), the statutory public advisory body that advises the HHS Secretary on health information policy, standards, privacy and confidentiality, quality, and data access, recommended in 1997 that it was premature to develop a unique health identifier for individuals because security and confidentiality issues that would be raised by implementing UPIs have not yet been resolved by Congress. (NCVHS, 2000)

HHS' Centers for Medicaid Services (CMS), the agency that provides health insurance through Medicare, Medicaid, the Children's Health Insurance Program (CHIP), and also through the Health Insurance Marketplace, provides healthcare coverage for over 100 million Americans. CMS is a stakeholder in the move towards healthcare administrative simplification, a feature

UPIs would help to facilitate. CMS published Meaningful Use Core guidelines for electronic health records (EHRs), which would be beneficiaries of UPI implementation. (CMS, 2012).

HHS' Centers for Disease Control and Prevention (CDC)'s National Center for Infectious and Respiratory Diseases (NCIRD)'s Immunization Information Systems Support Branch (IISB), provides a number of references related to research into and guidelines for immunization registries. The American Immunization Registry Association (AIRA), a CDC partner organization, provided portals to other publications that also address immunization registry technology related topics.

2.2.5 Patient Identification Methodologies

Several options to identify patients are discussed in public health literature. This research focused on four primary modern methods most often discussed in the literature; master patient indexes, statistical matching methods, biometrics and social security numbers (SSNs). (Arzt, 2017) (Hillestad, 2008)

2.2.6 IIS

Previous Research

One of the more recent IIS studies came from the Public Health Informatics Institute (PHII) in 2015 in their report, "*Immunization Information Systems: A Decade of Progress in Law and Policy*". This paper was helpful in explaining the legislative framework and legal limitations that impact IIS operations.

Alan Hinman's 2010 paper, *Immunization Registries Can Be Building Blocks for National Health Information Systems*, was particularly useful to the immunization registry discussion in Chapter IV, the results section. Hinman described the value to and contributions of immunization registries to the U.S. healthcare system. He mentioned that IIS provide a

comprehensive picture of the health of the US population. He notes IIS link healthcare delivery with population based data. Using Hinman's examples, this research expands his arguments by adding the discussion of UPIs, focusing on how UPIs would specifically benefit IIS in their role as significant components within in the U.S healthcare system.

Another article in the November, 2004 issue of *School Nurse News*, discusses immunization information systems. This resource was also used as a resource to help structure arguments in support of UPIs for use in immunization registries. This article also focuses on the benefits of IIS to patients and providers.

Peer-reviewed, if perhaps dated research into patient matching methods with discussion of UPIs does exist. Some previous research discussed UPI models, proposals, and provided examples, but did not specifically address application to immunization registries.

Of the 50 references selected, two relevant PubMed technical articles specifically addressed unique health identifiers and healthcare. (Netter, 2003) discussed the considerable benefits of UPIs in her 2003 paper, such as mitigating treatment errors and improving administrative efficiencies, but falls short of calling for a national identification number because of the privacy and confidentiality concerns raised by NCVHS. Earlier researchers (Carpenter and Chute, 1994) proposed UPI models based on a series of immutable values but did not address privacy concerns.

A number of references discussed options for improving immunization registry data quality and accuracy. (AIRA, 2017) Duplication of immunization records is a documented problem noted in the literature. Over immunization and the immunization record completeness for low-income, urban children and adolescents was also mentioned.

Suggestions included updating registries at point-of-service. Others addressed vaccine record de-duplication efforts while some discussed mobile technologies that would offer individuals more control of their own immunization records. But no references specifically addressed improving immunization registries using UPIs.

Overall, the literature review included a search for papers that included all of the desired elements,

1. An exploration of UPI models
2. UPI benefits and limitations
3. The legislative framework associated with UPIs
4. Discussion of UPI benefits to public health
5. Benefits to immunization registries.

This literature review did not find any references that addressed all five of these elements. There is a dearth of recent peer-reviewed literature that discusses how UPIs would benefit IIS.

Non-Traditional Literature

The AIRA website, (<http://www.immregistries.org/>), contained a number of relevant resources. Some AIRA references were not peer reviewed. The Healthcare Information and Management Systems Society (HIMSS) resource library (<http://www.himss.org/library>), was also useful in providing a number of references, particularly, their *Patient Identify Toolkit*. (HIMSS, 2011). Another organization, Global Public Inclusive Infrastructure, (GPII), whose goal is to provide cloud-based services to the healthcare industry to accurately link healthcare records, also published a comprehensive list of relevant references related to patient-matching methods, *Patient Matching Literature Review References* at <https://gpii.info/>. The HealthIT.gov website in general, was another government resource that provided general current Health IT related news and updates in the industry.

Chapter III: METHODS

3.1 Introduction

This thesis was developed to investigate how unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research will review the reasons why UPIs have not been implemented into the United States (US) healthcare system and this research will also investigate how patients are commonly identified without the benefit of UPIs.

Chapter III specifically addresses the research question, “What strategies are in place to accurately identify patients in the US healthcare system?” This chapter will analyze the benefits, limitations, and the privacy and security concerns of MPIs, statistical matching, biometrics, and SSNs.

As indicated in Chapter II, a systematic review of public health literature was conducted. That chapter is focused on four popular patient-matching protocols: master patient indexes, statistical patient matching, biometrics, and SSNs, to examine how patient identities are currently determined in today’s healthcare system without the accuracy, stability, reliability, and security that unique identifiers would provide. 3) A general review of reports and presentations that discuss IIS patient de-duplication initiatives to illustrate specific opportunities for how and where UPI solutions could be implemented once valid security and privacy concerns are eventually addressed.

Chapter III details the research performed in this thesis that took place in three stages, 1) The systematic review federal legislation, primarily the Health Insurance Portability and

Accountability Act (HIPAA) of 1996 and the subsequent Rulings that followed as they pertained to healthcare privacy with specific emphasis on the mention of UPIs. 2) This chapter will investigate how patients are identified without the accuracy that UPIs would provide, focusing on master patient indexes, statistical patient matching, biometrics, and SSNs.

Since each of these patient matching methods have limitations as to how well they can accurately and securely identify patients, Chapter III will also 3) Analyze proposals for how to better identify unique patients. Chapter IV will discuss whether or not IIS are preferable options for testing the theory, concepts and eventual implementation of UPIs into the U.S. healthcare system. Chapter V will conclude this thesis with discussion of the research questions and provide recommendations for UPI implementation.

3.2 Procedures

3.2.1 Stage 1: Systematic Review of Federal Legislation

The Department of Health and Human Services (HHS) has not funded any projects to develop UPIs since the late 1990s. No funding has been appropriated despite the fact that Congress passed the Health Insurance Portability and Accountability Act (HIPAA) which calls for, among things, the creation of a unique patient identifier:

(b) UNIQUE HEALTH IDENTIFIERS.—“(1) IN GENERAL.—The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers. (2) USE OF IDENTIFIERS.—The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.
(Public Law 104–191).

HIPAA established requirements for unique identifiers for health plans and for employers through EINs, issued by the Internal Revenue Service (IRS). It also established requirements for

National Provider Identifiers, (NPI) for providers. NPIs and EINs must be included on all HIPAA transactions to satisfy HHS' Center for Medicaid Services' (CMS) healthcare administrative simplification initiatives. But at the same time, UPIs for patients were not mandated.

Privacy and security concerns stalled the development of a UPI for individuals in the United States. Some privacy activists believed UPIs would empower government and corporations to exploit individuals and profit from their consolidated, easily available and complete health record. Other fears are that government officials or other nefarious individuals might sell patient data to the highest bidder, despite the fact that healthcare privacy legislation already currently exists to protect patient information. (Peel, 2012)

Privacy activists have spoken in favor of patients enduring a maze of different healthcare records from different offices, hospitals, pharmacies, labs, treatment facilities, government agencies and health plans, etc., because they believe obscurity would provide safety and anonymity. (Peel, 2012) Privacy activists are concerned with UPIs, the same reason proponents are for them, because they believe they would easily link patient information across providers. (Peel, 2012)

As a result, there is currently no adopted national standard for unique patient identification. (AMIA, 2001) There are no UPIs despite the fact that HIPAA recognized that UPIs for individuals are an essential component of healthcare administrative simplification. UPIs have not been implemented despite evidence that UPIs would have many cost reducing benefits by reducing redundancies from repeated tests, procedures and from over immunizations to name a few examples. (Gliklich, 2014)

Yet while some progress in addressing privacy concerns has been made since 1996, as with the HIPAA *Security* and *Privacy* rules, the National Center for Vital and Health Statistics (NCVHS) believes barriers to an effective and beneficial national health information infrastructure are primarily legal, societal, organizational, and cultural in nature versus technical barriers. NCVHS stresses privacy, confidentiality, and security concerns, primarily that;

1. Confidentiality safeguards be in place for UPI standardization efforts move forward.
 2. Security and confidentiality protections serve as preconditions for UPI implementation.
 3. Protections extend across all the users, technologies, and functions.
 4. National data standards be established for data exchange between healthcare providers.
 5. Equitable online health information services across all communities.
- (NCVHS, 2000)

HIPAA does not specifically address these concerns first raised by NCVHS back in 2000. Congress has yet to provide federal legislation for HIPAA to be modified in order to explicitly cover NHIN architectures. In 1998, perhaps hoping to table the matter for further investigation, Congress prohibited the federal government (HHS) from adopting a national strategy to implement UPIs. Before this prohibition though, Congress did commission HHS to provide a comprehensive analysis of UPI options. The 1997 report, mentioned earlier, provided a number of general findings, primarily that,

A unique patient identifier is an integral part of patient care and information...Its strengths include accurate identification without the repetitive use and disclosure of a patient's personal identification information. A UPI preserves anonymity, protects privacy, and prevents unauthorized access to health information. (Appavu, 1997)

Around the same time also in 1997, the Institute of Medicine (IOM) presented the case for computer based patient records, (CPRs) based on unique health identifiers, referred to as Universal Health Identifiers (UHIs) that would “*accurately and reliably link all health related data for a single individual*” (IOM, 1997) Since the early 1990s, researchers have acknowledged that the current patient identification system, based on proprietary IDs, social security numbers,

driver's licenses and signatures, and other demographic data is outdated and over all inadequate because these methods do not provide sufficient security and are often targets for identity theft.

In 1999, three years after HIPAA was enacted, Congress passed the Privacy Rule, Public Law 105-277, the *Standards for Privacy of Individually Identifiable Health Information*, which prohibited HHS from using any of its appropriated funds to develop a UPI without express congressional approval:

None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C. 1320d-2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.

This new *Privacy Rule* was enacted in December 2000. It was later modified in August, 2002 to clarify, among other things, that covered entities may disclose protected health information to public health entities, without patient authorization, for the conduct of public health surveillance, investigations, or interventions, as well as for the purpose of preventing or controlling diseases. (HHS, 2002)

HHS also published a *Security Rule*, *The Security Standards for the Protection of Electronic Protected Health Information*, in February 2003. This rule set national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. (HHS, 2017)

The *Privacy Rule* established national standards for the protection of certain health information. The *Security Rule*, established a national set of security standards for protecting certain health information that is held or transferred in electronic form. (HHS, 2017)

In 2004, President Bush, after observing electronic health infrastructures first hand while travelling in Europe, established the Office of the National Coordinator for Health Information Technology (ONC) within HHS. ONC's mission is to advance broad adoption of electronic health records. The ONC's strategic framework included interoperability of IT systems as a key component. ONC pushed for the development of national health information networks (NHINs) to enable disparate health care information systems across the United States to be linked so that authorized users could share clinical information in real time. (Kuperman, 2011)

But the legal patchwork of legislation complicates the full implementation of NHINs. For example, a state may have a law that mandates provider reporting of pediatric immunizations to an IIS without need for parental consent, but the laws for health information exchange require written patient consent for participation. (Martin, 2015)

Further legislative progress for a national electronic health network was made with the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act that provided \$750 million in grants and contracts towards building the nation's health information infrastructure.

Another recent piece of legislation, the 2016 *21st Century Cures Act*, directs the Government Accountability Office (GAO) to conduct a study to review methods for securely matching patient with their records:

HHS shall consult with [healthcare] stakeholders and standard setting organizations such as CDISC that have experience working with Federal agencies, to standardize health data submissions. (Public Law 114-255, 2016)

And most recently, in early 2017, the U.S. House of Representatives' Committee on Appropriations recently revisited and clarified Congress' position on UPIs:

...Although the Committee continues to carry a prohibition against HHS using funds to promulgate or adopt any final standard providing for the assignment of a unique health

identifier for an individual, this limitation does not prohibit HHS from examining the issues around patient matching. Accordingly, the Committee encourages the HHS Secretary, acting through the Office of the National Coordinator for Health Information Technology and CMS, to provide technical assistance to private-sector led initiatives to develop a coordinated national strategy that will promote patient safety by accurately identifying patients to their health information. (Public Law 115-31, 2017)

Despite some legislative progress, the effect of the congressional prohibition against UPI implementation means individual private proprietary statistical matching models were made the default method to identify over 320 million unique patients in the U. S. As health care information is now electronically distributed across city, county, regional, national health networks, and also across international healthcare systems, the need for the development of a more accurate, more reliable patient identification method remains a significant public health informatics problem.

3.2.1.1 Stage 1: Summary

HIPAA legislation of 1996 and the subsequent Security and Privacy rules that followed provide a legal basis for a establishment unique patient identifier. UPIs could be HIPAA compliant as long as they meet specific conditions and do not contain certain personally identifiable characteristics. Although the legal basis exists, security and privacy concerns prompted Congress to halt funding for UPI development initiatives until this issue once again becomes a priority on the legislative agenda.

3.2.2 Stage 2: Systematic Review of Patient Matching Methods

Introduction: A Definition of a Unique Key

Set Theory is a branch of mathematical logic that studies sets, better known as collections of objects. It is a theory on how to describe distinct objects or groups of objects. In the relational database model for example, data is organized into one or more tables (or relations), a

collection of columns and rows. Each table contains keys that uniquely identify each row within a table. Each table name is unique. Every data object within a database, such as queries must also have unique names or identifiers. Relational database systems may contain hundreds, thousands, or millions of unique rows, called records. Unique keys are necessary in order to eliminate redundancy, or the duplication of data.

A unique key is the most accurate identifier of a record across multiple linked databases and systems. A unique patient is counted once in the denominator to be measured, e.g., the number of patients in a hospital, the number of patients registered with a specific provider, or the number of patients covered by an insurer. Using a UPI, all patient data from multiple providers would be linked into one health record.

The Healthcare Information and Management Systems Society (HIMSS) defines patient matching as identifying, matching, and/or merging records, stored in multiple applications or databases, belonging to the same patient. Three primary benefits of UPIs are accurate patient matching, increased privacy and security and reduction of costs and wastage resulting from duplicate tests and procedures ordered. Several options to identify patients are in use today in the healthcare marketplace. One option is the master patient index.

3.2.2.1 Master Patient Indexes (MPIs)

Healthcare organizations participate MPIs in order to assist them in accurately identifying their patients. MPIs are databases of patient information populated from EHRs that are only provided to participating healthcare providers who subscribe to the MPI. Providers or larger healthcare systems that do not participate in a particular MPI do not have access to, nor do they share their information with one MPI, but may do so with another. Since the healthcare organizations that do participate in MPIs typically use their own proprietary EHR systems, data

exchange problems may occur between users of the same MPI when synchronizing database changes to patient records because although the providers may subscribe to the same MPI, they may use different EHR platforms. (Arzt, 2017)

As a result, with MPIs, not all participating systems can automatically correct records from another organization's software vendor. Data irregularities do occur within MPIs. This familiar problem is traced back to the lack of a national patient identification strategy that provides standards, guidelines and procedures for all healthcare providers in the United States to identify their patients (Arzt, 2017)

Privacy and Security Concerns

MPIs are limited because there is no single unique identifier across all MPIs available to be used to connect the records for one patient across multiple providers, regions, and states. Without UPIs, MPIs actually rely on statistical matching which is often prone to errors.

3.2.2.2 Statistical Matching

Statistical matching involves the use of algorithms to identify and match patients. Statistical matching models attempt to string together multiple patient data fields into one unique and accurate identifier or record. These algorithms use patient demographic data such as SSNs, last name, first name, birth date, ethnic background, blood type, address or zip code, and gender. Statistical matching models are the most widely used patient matching options available today. (Hillestad, 2008)

But the literature suggests that statistical matching has flaws and operational impediments. The literature suggests statistical patient matching is not the best option to uniquely identify patients. Accuracy is increased by making the algorithm more complicated, by increasing the number of data elements used in the search.

Data can be categorized and prioritized for more efficient statistical searches. But the problem with personal attributes such as name and address is that they are usually not unique to the individual, they change over time, and are often entered into systems in different formats by data entry clerks. Data-entry errors, such as misspellings, add to the difficulties with statistical matching methodologies.

Privacy and Security Concerns

Statistical matching is often faulty because results can include positives and false negatives, thus reducing user confidence in these methods. False positives occur when different patient records are incorrectly declared to be for the same person. False negatives occur when records for the same patient are thought to be for different people. These mistakes may lead to serious medical errors such as wrong treatments resulting from incorrect diagnoses, and also in surgeries intended for one patient being performed on another. They may also lead to wasted expenditures in the forms of repeated tests and procedures. (Hillestad, 2008)

Cultural and regional differences in naming conventions also serve as potential sources of errors with statistical matching algorithms. Common names have various spellings. Data entry clerks in provider offices have the power to decide how to enter information that will be imported into an IT systems and databases. The name Ashely is an example of a name with multiple spellings: Ashleigh, or Ashlee with surname Kelly, Kelley, O'Kelly, O'Kelley).

Demographic attributes used to identify patients are not usually unique. Attributes can change over time. Patients can decide to change their names and/or perhaps their gender identities. Patients and move away between jurisdictions. The repeated collection, distribution, edit, storage, and use of patient data fields by multiple healthcare providers results can in data quality challenges. (Hillestad, 2008)

3.2.2.3 Biometrics

Biometric identifiers typically include personal attributes that are not prone to keying or data entry errors. Biomarkers such as retinal scans, fingerprints, facial analysis, voice patterns, vein patterns, and also DNA samples, are not easily forged. Some advantages of biometric identifiers are that they are specific to an individual and they can identify patients without the need documentation that may be lost, stolen, destroyed, forgotten, or altered. Disadvantages of biometric identifiers include their relatively expensive implementation, equipment, and maintenance costs which make them unsuitable options for financially strapped state, local health departments, and smaller providers.

Privacy and Security Concerns

Although biometric identifiers generally remain stable over a patient's lifetime, there are instances where, with fingerprints for example, where biomarkers may degrade in time. Fingerprints may degrade due to exposure to latex gloves. Some medical treatments like chemotherapy can also degrade biomarkers. Voice patterns as well may also gradually change with age. (Arzt, 2017) (Grannis, 2009)

3.2.2.4 Social Security Numbers (SSNs)

Social Security Numbers (SSNs) are default patient identifiers. With their existing administrative and technology infrastructures and operating procedures already in place, SSNs are logical options to identify patients. But at the same time, SSNs are problematic for the exact same reasons, their existing administrative and technology infrastructures, and operating procedures. (Appavu, 1997) Therefore, SSNs are flawed for use in healthcare because they link patients to information outside of the healthcare system. SSNs are targets for identify theft, and financial fraud and abuse.

Privacy and Security Concerns

As a result, several states prohibit the use of the SSNs as patient identifiers. Alaska, Kansas, Maine, New Mexico, and Rhode Island restrict the solicitation of SSNs or prohibit denying goods and services to an individual who decline to provide their SSNs.

The demand for SSNs and other personal information has not abated. In February, 2016, Hollywood Presbyterian Medical Center in Los Angeles, California regained access to their computer systems only after paying a ransom to hackers who infected their system with malware which prevented staff from accessing the computer networks which included labs, pharmacies, and emergency room data.

The year before, in 2015, hackers stole names, birthdates, medical IDs, social security numbers, mailing addresses, electronic-mail addresses and employment information, including income data from the insurance giant Anthem, Inc., the second-largest health insurer in the United States. Anthem maintained records for over 80 million patients.

These are only two examples where healthcare data breaches involving SSNs occurred. This illustrates the dangers and risks of relying on SSNs for use in unencrypted electronically dispersed healthcare systems. (Orstein, 2015) Since 2010, at least 158 healthcare institutions, including medical providers, insurers and hospitals, have reported being hacked or having information technology issues that compromised patient records. (Winton, 2016)

In February 2013, President Barack Obama issued an executive order calling for the establishment of voluntary standards and guidelines to help organizations prevent and avoid cyberattacks. The Cybersecurity Act of 2015 includes a specific section focused on cyber security in health care. It called for the creation of a task force to develop best security practices for the health care industry. But the 2009 Health Information Technology for Economic and

Clinical Health Act, known as the HITECH Act, had already called for cyberattack protection standards. HITECH required healthcare organizations to publicly report data breaches involving at least 500 patients.

Another problem with SSNs are that they not automatically updated as names change. Multiple people with the same name may be born on the same day. It is insufficient to accurately identify a patient using only the last four digits of the SSN. The cards contain no picture or biometric identifiers. SSNs have been recorded incorrectly in health care systems because they do not have check digit, a form of redundancy check used for error detection in identification numbers. This means providers do not run SSNs against a national system to verify and validate the numbers they have are accurate.

Furthermore more, about 10 million individuals residing in the U.S. do not have the SSNs. Illegal aliens and visitors who need healthcare are not issued SSNs. They were not mandatory until 1936 and therefore anyone born prior to that year, may or may not have been issued a SSN. (McKinley, 1970)

3.2.2.5 Stage 2 Summary

None of the contemporary methods to identify patients, MPIs, statistical patient matching, biometrics, and SSNs, provides the cost savings, accuracy, stability, reliability, and security that unique patient identifiers would provide. Each of these methods has limitations and drawbacks and none provides the scalability required for national patient identification strategy. These difficulties also exist with patient matching in IIS systems and underscores the need for UPIs in immunization registries.

3.2.3 Stage 3: General Analysis of IIS Data

In *Figure 1, CDC's Routine Recommended Immunization Schedule for Children and Adolescents Aged 18 Years and Under*, currently includes 15 vaccines. Immunizations are usually given in a series, depending on age. Combined together, these vaccines require at least 37 doses to be administered over the years from birth to 18 years of age. The schedule recommends at least 20 shots before 24 months of age. Sometimes more doses are recommended depending on specific health conditions. Five doses of the Diphtheria, Tetanus, and Pertussis (DTaP) vaccine alone are recommended for children by the age of six. (CDC)

Figure 2, The U.S. Recommended Immunization Schedule for Adults Aged 19 Years or Older by Age Group, in 2017 currently recommends over 25 doses of multiple vaccines, or boosters, by the age of 65. More doses for adults as well are recommended depending on specific health conditions. Combining the childhood totals and the later adult total recommended doses, this equals to at least 62 immunization doses recommended be administered over a lifetime. Children will change providers, hospitals, pharmacies, and healthcare systems as they age. So too will adults due to changes in employment or relocation. UPIs can help address the need for long term national patient identification strategies needed to track this type of long term patient information.

Fifty-one (96.2%) of 53 IIS programs surveyed are now authorized to collect lifetime immunization records for children and also for adults. (Martin, 2015). When patients change providers, the account numbers and/or IDs assigned to them become obsolete. With each new provider, patients are assigned new identification and account numbers. (Leonard, 2009) This change in providers is repeated throughout patient's lifetime as medical information is collected from birth, until death and sometimes also after death from autopsies.

Many IIS receive their data through EHR interfaces rather than through direct-entry or paper record submissions. (Martin, 2015) UPIs could help resolve IIS data problems of accurately linking individuals to multiple vaccination records submitted by different providers over time. UPIs would be able to uniquely identify hundreds of millions of patients when each of these 62 recommended doses of multiple vaccines are administered.

Duplicate immunization records have increased with the electronic transmission of vaccine records. A 2016 AIRA survey of immunization programs showed that vaccine event duplications tend to be a particular problem from Medicaid. Others noted that certain EHR systems send complete vaccination history each time a new vaccine is administered, resulting in data duplication. (AIRA, 2016) Duplicate immunization records consume significant system processing time, reduce data quality, and reduce the ability to accurately report immunization status.

The New York City health department defines duplicate immunization clusters as instances where there are two or more immunizations appear to be administered on same day, or within 1-2 days apart for same individual. Patient age is also used to identify appropriate immunization records since some vaccines are developed for pediatric or for adult usage. With their proprietary immunization de-duplication algorithm, New York City's first data de-duplication efforts in 2010 resulted in the removal of 1.5 million records from their IIS system. By 2012, 2.9 million duplicate vaccination records were eliminated. (Ternier, 2012) This de-duplication effort is one example, in one city, in one state out of 62 U.S. states and territories.

One problem with this process of eliminating data, is that at least one of these multiple immunizations could have in fact actually occurred and the records needed to be tracked and

maintained. Over immunization errors need to be tracked and monitored to help improve processes. UPI would help to prevent and reduce the over immunizations as well.

Arizona documented data quality issues where 15% of their immunization records did not include gender. Without gender in immunization records, accurate gender specific reporting was impossible. That type of reporting is critical when tracking human papillomavirus vaccine (HPV) uptake as an example because HPV was initially targeted towards girls.

Arizona also saw large amounts of duplicate immunization data which resulted in lower actual dosage series completion rates. They noticed in some instances, immunization record counts were higher than the actual population of certain jurisdictions. All of these examples resulted in the unreliability of their IIS data. After their de-duplication initiatives, Arizona noted several positive outcomes including increases in immunization series completion rates and in influenza coverage and an overall improvement in data quality. (Ruiz, 2012)

3.2.3.1 Stage 3: Summary

The adoption of a single unique patient identifier, used to access patient information across all healthcare settings, including immunization registries, will help facilitate a national patient data matching strategy. Since eventual UPI development and implementation would likely occur in stages, immunization registries should be the first public health systems considered for testing and implementation of the concept because they are relatively stable and have a long history of development and standardization. (Hinman, 2010)

The lack of a national patient identification strategy explains some of the underlying data problems generally found in IIS. Vaccine registries illustrate specific examples for the need for UPIs in the U.S. healthcare system.

3.3 Procedures Summary

The purpose of this thesis is to discuss why unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research reviews the reasons why UPIs have not been implemented into the U.S. healthcare system and this research investigates how patients are commonly identified without the benefit of UPIs.

Chapter III specifically addressed the research question, “What strategies are in place to accurately identify patients in the US healthcare system?”, by analyzing the benefits, limitations, and also the privacy and security concerns of MPIs, statistical matching, biometrics, and SSNs.

This chapter also addressed the research question, “What are some implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system? The primary implication is that there is no national strategy in place to track all of the 62 recommended doses of vaccines that should be administered over a lifetime, in order to protect communities from vaccine preventable diseases.

Chapter IV:

RESULTS

4.1 Introduction

The purpose of this thesis is to discuss why unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research reviews the reasons why UPIs have not been implemented into the U.S. healthcare system. This research will also investigate how patients are commonly identified without the benefit of UPIs.

This chapter will describe the findings of the Chapter III research in stages. The first stage will provide analysis of federal legislation regarding patient privacy. Stage two will review results of the systematic literature of patient matching protocols and also review UPI proposals. Stage three will further address the primary research question, “What are the implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system?”

Based upon a review of the literature in Chapter II, it is clear that UPIs could facilitate a national patient identification strategy with IIS used as the initial building blocks a national public health informatics system. This thesis includes research into the rationale for the legislation that prevents the implementation of UPIs and research into the impacts of that decision on the U.S. healthcare system.

4.2 Findings

4.2.1 Stage 1: Legislative Analysis Results

Security, privacy, and confidentiality concerns of UPI could be resolved by federal legislation and oversight. Security and privacy concerns have more to do with how data are

accessed, managed, and controlled rather than with how patient records are stored, maintained, retrieved and distributed. In 2008, The Rand Corporation proposed that UPIs, once implemented, should immediately become federally protected sensitive health information. They acknowledge UPIs likely will still become targets for hackers. However, unlike the SSNs, they also proposed that UPIs should not link to financial or any other non-healthcare records in accordance to HIPAA guidelines. (Hillestad, 2008)

Criticisms with HIPAA and its associated privacy and security rules and with similar state privacy laws are that they archaic, implemented prior to the widespread development of electronically distributed patient record systems. (Greenberg, 2009) Networked healthcare systems offer many benefits such as greater efficiencies, but they do invoke privacy issues that some critics believe the current HIPAA framework fails to address.

It should be noted that HHS invested nearly six years into creating the HIPAA standards. HHS held hearings, proposed rules, reviewed and responded to public comments. At 1,500 pages long, HIPAA legislation is a clear set of rules about the accepted use of protected health information. HIPAA legislation relied on the best information available at the time of its passage. (McDonald, 2009)

Furthermore, HIPAA Section 1177, “The Wrongful Disclosure of Individually Identifiable Health Information” describes penalties for the misuse of PHI. The problem is the lack of clear federal guidelines on the electronic exchange of protected health information in NHINs.

HIPAA does govern the electronic exchange of financial and administrative information in the health care industry according to its own administrative simplification provisions. An electronic transaction involves information exchanges between two parties to carry out financial

or administrative activities related to health care. Transactions subject to this administrative simplification rule include, healthcare claims, plan enrollments, payments, claim status, and coordination of benefits, to name a few. These electronic transactions are expected to take place without the implementation of UPIs in the healthcare system. This decentralized approach to health information exchange in the United States is in contrast to other high-income countries. (Hinman, 2010)

More concerns with UPI implementation include institutional privacy and fear of monopolies. Commercial private institutions may be tempted to block access to their patients' information and keep them returning for more treatment and services rather than to share their information with competing hospital and providers. The highly competitive nature of the health care industry encourages the use of proprietary systems also to limit providers' mobility and to make it easier for their employers to control their movements. Federal legislation in this area, that designated patients, not providers, as owners of healthcare records, would resolve this potential problem of monopolies.

This type of anticipated monopolistic provider behavior can also be addressed with federal incentives. Incentive structures would guide how health information would be used and shared. Federal legislation could support incentives for sharing and coordinating care and penalties could be assessed for withholding patient information. Evidence suggests that incentives could motivate and encourage reciprocity among healthcare providers which would put patients' needs first and also strengthen the data quality of NHINs. (Brailer, 2012)

Based upon a review of the literature, it is clear that federal leadership is required to ensure that standards and legislation are implemented to preserve and enhance national NHINs which should be supported with UPIs. HHS noted in its 1997 report that until national standards

exist for uniquely identifying patients, the value from capturing, storing, aggregating, and analyzing data from local, regional and national health information networks will go unrealized.

ASTM, in their *Standard Guide*, called for the establishment of a Central Trusted Authority (CTA) to issue and manage UPIs. This CTA could preferably be a government agency, or perhaps an independent semi-government entity, or a private non-profit organization entrusted with developing UPI models. This might satisfy critics' concerns about having one all-powerful government authority being responsible for issuing UPIs and then controlling access to electronic healthcare information.

The 1997 HHS report explained that no legitimate scientific or technical concern lies with UPI implementation. The concerns expressed are with the lack of legal standards to mitigate the potential for UPI theft, fraud and abuse.

Barriers to UPI implementation arise from a lack of awareness and understanding of their actual capabilities and benefits. The intellectual understanding of the work required, how to do perform what needs to be done, and for whom the work will be done, for patients, is often ignored in the overall privacy debate. Surveys of U.S. patients indicated they are more concerned that their private healthcare information might be accessed by their employer and used to limit job opportunities. Hillestad in their 2008 paper reviewed survey results and found 80% of Americans said that they are very concerned about identity theft or fraud. Seventy-seven percent are very concerned about marketers gaining access to their data; 56 %, about employers gaining access; and 53 %, about insurance companies.

UPIs will need public engagement for successful implementation in the U.S. There is an urgent need for policymakers to revisit and strengthen privacy laws due in response to constant high-tech innovations in healthcare. The Office of the National Coordinator for Health IT noted

in a 2015 data brief that provider electronic health record (EHR) adoption rates are steadily increasing, with a 27% increase noted from 2013 to 2014.

The IOM noted back in 1996, “*there has yet been no agreement on how best to establish the balance between appropriate use of health care data and the individual patient's rights to privacy*”.

4.2.2 Stage 2: Systematic Literature Review Results

Based upon the evidence provided in Chapter III, it is clear that UPIs would reduce dependencies on private personal information that is used outside the healthcare system. UPIs would be restricted to healthcare identification and tracking purposes only. Unlike SSNs which are currently used in credit, financial systems, schools and a myriad of other non-healthcare related systems, encrypted UPIs would preserve patient anonymity, protect privacy, and would mitigate unauthorized access to health information.

In today’s healthcare environment, a team of healthcare professionals from different disciplines and institutions, can be responsible for providing healthcare services for a single patient. This requires a high level of data integration, data interoperability, and data sharing. Proper delivery of patient care is critical and is dependent on the ability to retrieve accurate patient information as accurately and quickly as possible. (Leonard, 2009)

The costs of developing and deploying a national UPI standard has been estimated at between \$4.9 billion and \$12.2 billion (Grannis, 2009) Others say the cost of developing patient identifiers actually depends on the approach and on the specific technical architecture to be used.

4.2.2. Analysis of UPI Proposals

Due to the problems with accuracy, privacy and security concerns with MPIs, statistical matching, biometrics, and also SSNs and despite the prohibition of UPI implementation into the

U.S. healthcare system, research into UPI proposals continues. The need for more secure and efficient options to identify patients still has not been resolved.

4.2.2.1 Data Encryption Proposals

In the hacking examples mentioned earlier, identify thieves have already demonstrated that encryption is an effective method for protecting patient information. One UPI proposal includes a set of unique characters based on complex mathematical formulas where two encryptions keys are used to authenticate users. One public key is for the sender, the other private key is intended for the receiver of the encrypted healthcare information. With encryption, patient data would be electronically locked or scrambled, and if anyone gained unauthorized access to the data, the encryption process would render the information unreadable to unauthorized users, and therefore unusable and unsellable. (White, 1997) Had Hollywood Presbyterian officials established policies that required patient data to be encrypted, they could have mitigated the damage and fallout from that data breach.

There are various types of data encryption services depending on at what point the data is secured. Data can be encrypted when it is stored in databases. Data can be encrypted as it travels through the internet. With encryption, data cannot be accessed or utilized without the required private unique keys.

Some healthcare organizations now use Direct Project protocols to transmit healthcare information. Direct Project is a secure email service designed for healthcare providers and other participants to send encrypted health information directly to trusted recipients over the Internet. (Brailer, 2012) Secure processes for data transmission already exist. What is lacking is the ability to accurately identify patients on a national scale.

One of the first UPI proposals was published in 1994 by Mayo Clinic researchers. They suggested a UPI based a series of personal immutable properties or codes that included dates and geographic information. Their complex and therefore unlikely proposal was eventually pushed to 19 digits. (Carpenter, 1994) HHS, in contrast, recommended a simple user friendly UPI that is suitable for use by both humans and computers as an ideal choice.

Other models consisted of the seven-digit date of birth field, a six-digit place of birth code, and a five-digit sequence code, to identify the individual born on the same date in the same geographic area. (HHS, 1997)

4.2.2.2 National ID Cards

Health ID cards with unique identifiers similar to state issued driver's licenses are another option. The 2005 Real ID Act, requires improved security for driver's licenses and other personal identification cards. Similar legislation could also mandate national healthcare ID cards that could be encrypted like federal employee ID badges. Health ID cards contain chips that store encrypted healthcare information which could only be read by designated card readers. (Public Law 109-13, 2005)

Decades ago, according to a 1996 study by Privacy International, around 100 countries had already enacted laws making identity cards compulsory for their citizens. Recently, in 2016, India began implementing a 12-digit unique identification (UID) numbering system, Aadhaar, to Indian residents. Managed by the Unique Identification Authority of India (UIDAI), the Aadhaar is now required for access to certain government subsidies, benefits and services. The Aadhaar card can be used as a single identification document for healthcare institutions but unfortunately it can also be used by government bodies and for other financial transactions.

News reports noted that representatives from the US National Cancer Institute observed India's new system and commented that, "India's Aadhaar program is further ahead of many other countries, including the United States in terms of being able to link records from the doctor's offices, hospitals, laboratories and the pharmacies." (Srivastava, 2016)

4.2.2.3 Private Sector UPI Initiatives

Public and private sector partnership recommendations for establishing UPIs have not yet been harmonized with the privacy, security and confidentiality concerns that were raised decades ago by organization such as ASTM, NCVHS, and the IOM. This impasse is a result of the lack federal UPI guidelines and standards.

A number of disparate private Sector UPI development proposals are currently underway. The CHIME National Patient ID Challenge, launched in January 2016, was open to individuals or groups to identify the best plan, strategies and methodologies that would easily and quickly identify patients, while at the same time, achieving 100% accuracy. The four finalists, as of May 2017, proposed to identify patients by 1) Using biometric technologies, 2) Analyzing a combination of behavioral and biometric information. 3) Implementing encryption/hashing technologies, a method of recognizing fingerprints while at the same time, hiding the private information related to the fingerprint. The fourth finalist proposed combining photos and biometric markers. The CHIME grand prize winner was announced on November 3rd, 2017, but the details of which proposal achieved 100% accuracy was not made publically available on their website.

In 2016, Pew Charitable Trust also called for proposals for research in three areas related to patient matching: patient matching safety implications, patient matching cost implications, and EHR usability safety implications. As a result of no federal guidance or official

recommendations, these initiatives and others like them, are working separately and independently and have no standards by which to develop cohesive models for possible nationwide integration and implementation, across all types of healthcare organizations.

4.2.3. Stage 3: IIS Data Analysis Results

The Office of the Surgeon General's 2011 national strategy included disease control and prevention. The full national strategy, published to their website in June of 2011, by the National Prevention, Health Promotion and Public Health Council (NPHPPHC), said, "*Prevention policies and programs often are cost-effective, reduce health care costs, and improve productivity*". NPHPPHC's report notes less than half of older adults are up-to-date on the core set of clinical preventive services including immunizations. This problem exists despite the fact that vaccines are one of the safest and most effective tools in managing the fight against infectious diseases.

IIS are leaders in health information data exchange. The 2015 PHII survey determined that thirty-six (67.9%) IIS programs had authority to transmit or allow access to immunization data across state borders. Of the 36 IIS programs with authority to transmit information across state borders, in 15 (41.7%), the authority was only obtained by data exchange agreements. Eleven IIS (30.6%) reported their authority was derived from general public health laws, and 10 other programs (27.8%), reported their authority was derived from a specific statute or regulation. (Martin, 2015)

Two (3.8%) IIS programs reported that they did not know whether they had authority to transmit or allow access to data across state borders. New York State, for example, has legislative authority to transmit or allow access to data across state borders and also required a

data-sharing agreement. Twenty-nine IIS programs (54.7%), responded they currently transmit or allow access to data in the IIS across state borders and 24 (45.3%) reported they do conduct transmission or access across state borders. (Martin, 2015)

Immunization information systems serve vital roles in responding to pandemic influenza and other public health emergencies. Immunization data are imported from disparate sources, electronic health records, pharmacies, Medicaid, and other systems that support and inform public health immunization activities. It is imperative that IIS control the quality of data in their systems because policy makers depend on the information from IIS to make evidence-based decisions. (AIRA, 2014)

Each healthcare provider, depending on the age and type of population served, is expected to administer vaccines according to specific schedules. Patients that visit more than one provider can generate more than one immunization record for a single office visit. Due to the growing number of health care providers who submit data to IIS, it is important for immunization information systems (IIS) to monitor and control the quality of data in their systems.

De-duplication of immunization records is a two-fold problem that includes de-duplication at the patient level (e.g. two records describe the same patient) and de-duplication at the vaccination event level (e.g. two records describe the same immunization). IIS must decide how to identify and process duplicate immunization records. They must determine which records represent the same vaccination event. (MIROW, 2006)

In connection with these findings, the Modeling of Immunization Registry Operations Workgroup (MIROW), developed a vaccine de-duplication guide to provide guidance to IIS managers. The major focus of the guide was to address issues of vaccination level de-

duplication for lifetime immunization records. The guide includes discussion of rules and procedures that promote accurate and complete immunization records compiled over time from multiple data sources.

No national immunization registry exists in the United States, nor are there plans in place to develop one. Instead, focus is on the public health community to create a national network of immunization information systems. (CDC) To achieve that goal, individual IIS must be able to exchange data unambiguously. To facilitate that, UPIs are needed.

Hinman in his 2010 paper, noted the immunization status and records of nearly 95 million patients are already included in immunization registries across the country. But out of 325 million, 95 million individuals is roughly only 29% of the U.S. population. How are immunizations tracked for the remaining 70% of the U.S. population, if at all?

Some Americans self-track their immunization histories using the yellow multi-fold cards provided by the United States Public Health Service (USPHS) by bringing those cards with them to different providers. Most individuals do not self-track their immunization histories, as they move between jurisdictions throughout their lifetimes.

As previously noted, (Hinman, 2010, Martin, 2015) IIS have been in existence over 20 years and are more mature and have a long history of development and standardization compared to other population-based health information systems. In connection with this finding, it is noted that IIS could be fully integrated with EHRs to facilitate effective public health information exchanges. But that would require significant long range planning and effort. This means, on a national scale, federal legislation and guidance is needed.

By contrast, other high-income countries have implemented national IIS. Singapore, for example, has a national registry for persons born January 1, 1996 or later. (see

<https://tinyurl.com/y75qvw2x>). In Australia, immunization tracking was traditionally the responsibility of local states and territories, until the federal government noticed a range of disparities between states and territories regarding the funding of and access to vaccines for their populations. As a result, Australia developed their National Immunization Strategy in 1993 and subsequently implemented a national immunization registry. (Australia, 2013)

Canadian provinces and territories are currently working towards the development of a national network of immunization registries. Currently, as in the U.S., each Canadian province and territory maintains its own system for tracking immunization coverage. (Canada, 2017)

As with adults, in some areas, certain children are still not receiving recommended routine vaccinations. Many preschool children (aged 19 to 35 months) and also teens do not receive all of the routinely recommended vaccinations. (Stockwell, 2016) If de-duplicated data for these children were in all IIS, reminders could be sent to them to receive the recommended vaccinations. Because of this problem, states have expanded immunization efforts to include urgent care facilities and local pharmacies to help close these immunization gaps.

4.2.3.1 Pharmacies and IIS

In 2014, AIRA studied the immunization efforts of pharmacies. In general, each of the major chains interviewed, Walgreens, CVS, Rite Aid, Safeway, and Kroger reported that they aggregate immunization data from each store site into a data warehouse and modify the information to meet state specific IIS reporting requirements. The AIRA report noted each pharmacy site is identified with a unique ID and in some cases, the IDs also tracks back to a specific pharmacist. The greatest challenges cited by the pharmacies that report IIS data included data quality issues, specifically those associated with demographic data. The greatest concerns were the lack of unique patient identifiers, variations in patient's name, and the lack of patient

address which all led to patient matching and duplication issues in the IIS. This resulted in inappropriately merged records or creation of a completely new IIS record.

The implementation of UPIs should prevent these pharmacies from submitting incorrect patient information and gradually reduce the problem of reporting fragmented IIS records because these providers would gradually report data to IIS using a unique ID.

Accurate information is needed in order to identify patients involved with vaccine recalls, which may occur for a short time or for vaccines that may be withdrawn from the marketplace permanently. Specific batches, or lots, can also be withdrawn or recalled. In order to notify providers and patients about recalls, accurate patient identification strategies are needed.

UPIs can help provide IIS managers with insight into immunization patterns of community health centers, public health clinics and tracking trends of sociodemographic characteristics of geographically dispersed populations, UPIs can help facilitate the development accurate immunization histories for all patients.

UPIs should help providers comply with federal and state vaccine registry recording requirements. UPIs would help in reducing providers' reporting burdens and also help them to better manage their vaccine inventories in real time. (Reed, 2004) UPIs would offer improvements to billing services by allowing providers to accurately identify those who have payments due and to know how much exactly to bill them. They would help providers accurately locate and seek payments from the correct individuals. A consolidated complete patient record would also eliminate duplication of efforts in tests, in procedures, and in the prescribing of medications among different providers and facilities.

It is a complex process to identify patients using multiple personal attributes within large, ever expanding electronically distributed systems. Ever increasing IIS record volumes coupled

with differences in EHR reporting systems, require solutions to the problem of duplicate patient records. (Grant, 2012)

A national immunization registry with a unique personal identifier would also eliminate the problems associated with MOGEs, or patients who have “moved or gone elsewhere”. The American Medical Informatics Association (AMIA) recommended in their 2001 National Agenda for Public Health Informatics, under their healthcare architecture and infrastructure category, the establishment a UPIs to facilitate integration of data from multiple sources. That recommendation fed into their next one, an interface between public health and medical care.

4.3 Chapter IV Results Summary

The purpose of this thesis is to discuss why unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research reviewed the reasons why UPIs have not been implemented into the U.S. healthcare system. This research also investigated how patients are commonly identified without the benefit of UPIs.

Three stages of analysis were performed: The first stage provided analysis of federal legislation regarding patient privacy. Stage two reviewed results of the systematic literature of patient matching protocols. Stage three addressed the primary research question, “What are the implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system? The major findings were as follows:

Federal legislation regarding patient privacy has yet to provide guidance and more specific legislation that addresses electronically distributed patient record systems. HIPAA does govern the electronic exchange of financial and administrative information, but critics say

HIPAA, passed 1996, in the dawn of the internet age, failed to anticipate and plan for the development of an electronically distributed national health information network.

HIPAA does address the traditional model of medical communications where providers communicate directly with another in the sharing health records, tests results, etc., to fulfill specific requests for information exchanged through oral and through written communication channels. But with the transition away from oral and written communication between providers towards the more seamless electronic exchange of health information across ever expanding computer networks, this raises questions about how to authenticate legitimate, authorized users and receivers of patient health information.

HIPAA does not explicitly detail the responsibilities of healthcare providers to ensure that their requests for patients' private health information through NHINs are legitimate and secure. The Congressional response to these concerns, raised by a number of healthcare think tanks, was to prohibit the development of UPIs which would exacerbate these concerns with their implementation into the U.S. healthcare system. The implementation of UPIs in essence, would be putting the cart before the horse, in the management and electronic exchange of patient health information.

In response to the lack of federal support for unique patient identifiers in the electronic exchange of health information, other methods were developed and used to identify patients. MPIs, statistical matching, biometrics, and SSNs. Each method has their own merits, but none of them, alone, can serve as the backbone of a national patient identification strategy.

The implications to IIS of not having UPIs in the U.S. healthcare system are that duplication of immunization records continue to affect IIS data quality, which affects immunization usage reporting, which in turn affects the ability to accurately forecast vaccine

purchasing needs. The degree to which IIS are able to develop solutions to these problems, seem to depend on their size and the resources available to them.

Some IIS are able to hire staff to develop de-duplication algorithms or others hire temporary consultants to assist them. There is guidance for IIS managers to help them mitigate duplicate immunization records, but the ultimate solution would be a unique patient identifier which would be the same identifier used across all immunization information systems as they exchange patient information across the United States.

Chapter V:

DISCUSSION

5.1 Discussion of Research Questions

The purpose of this thesis is to discuss why unique patient identifiers (UPIs) could help resolve common data quality problems with immunization information systems (IIS). This research reviewed the reasons why UPIs have not been implemented into the United States (US) healthcare system and this research also investigated how patients are commonly identified without the benefit of UPIs.

Three stages of analysis were performed: The first stage provided analysis of federal legislation regarding patient privacy. Stage two reviewed results of the systematic literature of patient matching protocols. Stage three addressed the primary research question, “What are the implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system?”

Additionally, a by-product of this research resulted in information relevant to understanding 1) Why UPIs are currently banned for use in the U.S. healthcare system. 2) What patient identification methods are currently used to identify patients and to investigate how well they are working. 3) Determining the implications to immunization information systems (IIS) of not implementing UPIs into the U.S. healthcare system.

Major findings were as follows:

5.2 Key Findings

The use of appropriated federal funds to develop UPIs is prohibited by Congress because privacy, confidentiality and security concerns raised by a number of organizations have yet to be fully addressed with the advent of the electronic exchange of patient records. As result, instead of UPIs, healthcare providers currently rely on MPIs, statistical patient matching algorithms, biometrics and SSNs to identify patients. Each of these methods has benefits and limitations. But none can provide the security, privacy, and scalability features that UPIs would provide.

As a result, being subject to overall health care privacy legislation, IIS must rely on these common patient identification methods as well to track immunization histories of multiple patients who receive multiple vaccines, often in series, throughout their lives. Since none of these methods are 100% accurate in correctly identifying patients, IIS can often experience the duplication of immunization records over time.

This thesis found that despite the federal ban on UPI development, research into UPI proposals continue out of necessity because of the problems with accurately identifying patients continues to exist. A national patient identification strategy is needed.

5.2 Recommendations

The overall goal of developing UPI standards and guidelines should be prevention of disease, which is the most cost effective approach to managing escalating healthcare costs. UPIs would help reduce costs by reducing the duplication of patient records and therefore the number of treatments prescribed.

As UPI development progress is made in public health informatics, due to their maturity, existing saturation in the healthcare system, and their relative stability, IIS should be considered

the public health informatics systems best suited for the initial testing, development, and eventual implementation of one of the most technologically innovative advancements to come, the implementation of UPIs into the U.S. healthcare system.

Suggestions for UPI implementation include, in order of priority:

1. Provide federal guidance, incentives and funding to implement UPIs at the provider level and for each IIS because implementation will take several years to match new UPIs with existing patients.
2. Declare UPIs as protected health information (PHI), making them subject to existing HIPAA regulations and protections.
3. Assign UPIs from a neutral 3rd party entity composed of federal and state government leaders, private-sector partners, non-profit participants, and community oversight participants, in order to foster public engagement and support in the UPI development process. Public buy-in, understanding, and acceptance is needed for successful UPI implementation.
4. Add UPIs as a new data fields in EHRs. This new data field would be included in data submissions to state and local IIS systems, who would also update their data architecture with this new UPI data field.

UPIs will enable families to better consolidate immunization records for each family member. UPIs will help immunization registries be better prepared to respond to outbreaks, pandemics, and vaccine recalls.

5.3 Conclusions

UPIs are required to reform the U.S. healthcare system to make it more efficient, more secure, and more responsive to its customers by reducing the damage from data breaches and in order to place the U.S. healthcare system more in line with how other high-income countries around the world exchange patient information. UPIs would help to improve the security of patient information by eliminating the need to transmit sensitive, personally identifiable information across electronic networks in order to identify patients.

Should UPIs be developed to support “lifespan” registries, or medical records established at birth and ending at death, to better track patients’ complete medical history throughout their lives? Currently, the only option for a complete lifetime medical record is to remain with healthcare providers from birth and stay until to death. But, of course, that is impossible. Obstetricians are not pediatricians and pediatricians are not primary care providers, who in turn are not gerontologists. As patients grow, develop and age, they require different provider types who will need access to their complete medical histories in order to make appropriate clinical decisions.

The goal of developing a comprehensive NHIN composed of provider EHRs, IIS, food inspection systems, traveler’s health systems, urgent care facilities to name a few public health systems, would require UPIs in order to fully integrate these systems with hospitals, schools, correctional facilities, insurance companies, pharmacies, laboratories, nursing homes, dentist offices, public health clinics, the armed forces, and employer sponsored occupational health programs. A unique patient identifier will be the most effective tool to integrate these healthcare systems into a reformed national health information infrastructure.

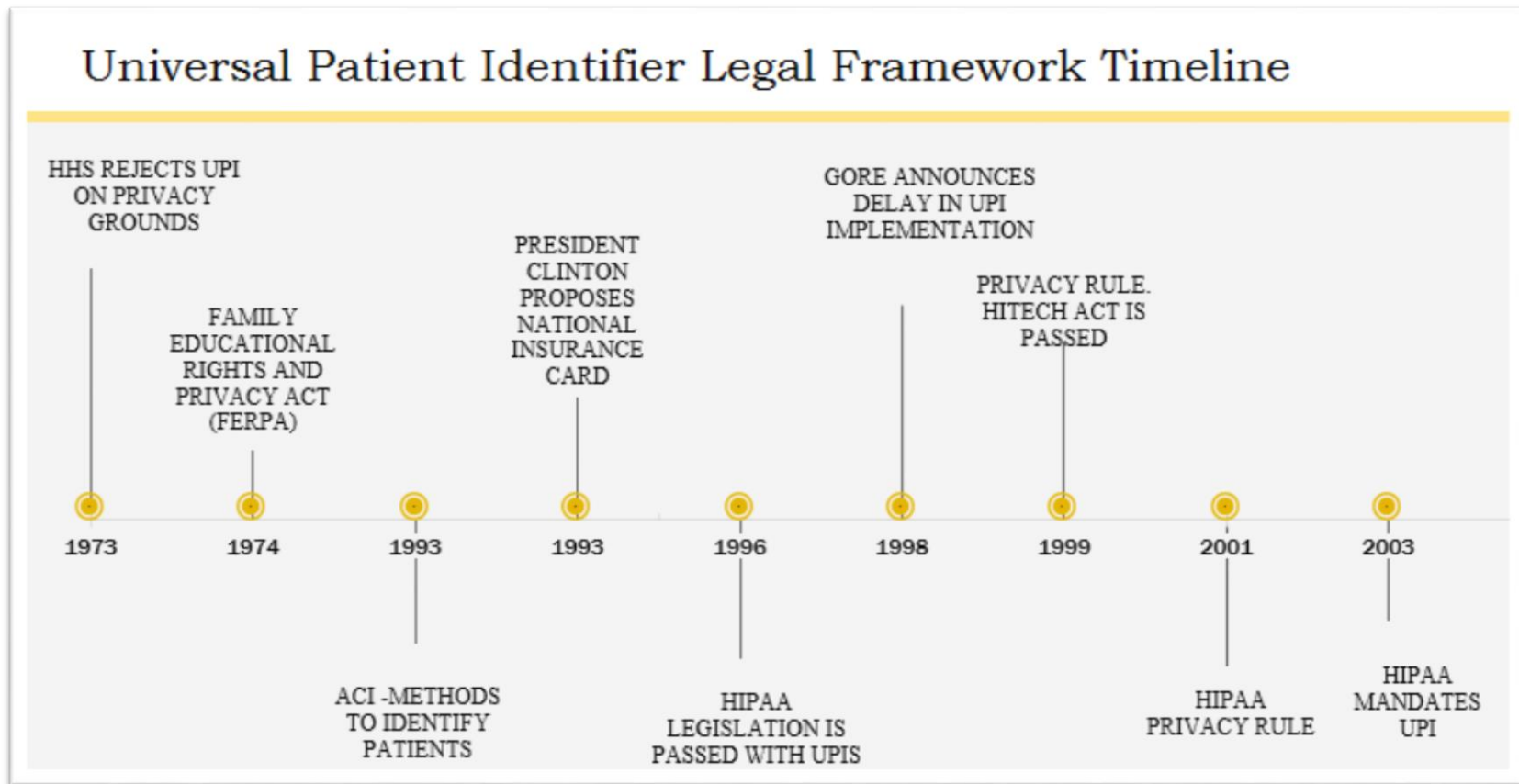
Figure 1: Recommended Immunization Schedule for Children and Adolescents Aged 18 Years or Younger, United States, 2017. See full schedule at <https://www.cdc.gov/vaccines/schedules/downloads/child/0-18yrs-child-combined-schedule.pdf>

Vaccine	Birth	1 mo	2 mos	4 mos	6 mos	9 mos	12 mos	15 mos	18 mos	19-23 mos	2-3 yrs	4-6 yrs	7-10 yrs	11-12 yrs	13-15 yrs	16 yrs	17-18 yrs
Hepatitis B ¹ (HepB)	1 st dose ←.....2 nd dose.....→3 rd dose.....→																
Rotavirus ² (RV) RV1 (2-dose series); RV5 (3-dose series)			1 st dose	2 nd dose	See footnote 2												
Diphtheria, tetanus, & acellular pertussis ³ (DTaP: <7 yrs)			1 st dose	2 nd dose	3 rd dose				←.....4 th dose.....→			5 th dose					
<i>Haemophilus influenzae</i> type b ⁴ (Hib)			1 st dose	2 nd dose	See footnote 4				←.....3 rd or 4 th dose.....→ See footnote 4								
Pneumococcal conjugate ⁵ (PCV13)			1 st dose	2 nd dose	3 rd dose				←.....4 th dose.....→								
Inactivated poliovirus ⁶ (IPV: <18 yrs)			1 st dose	2 nd dose					←.....3 rd dose.....→			4 th dose					
Influenza ⁷ (IIV)					Annual vaccination (IIV) 1 or 2 doses									Annual vaccination (IIV) 1 dose only			
Measles, mumps, rubella ⁸ (MMR)					See footnote 8				←.....1 st dose.....→			2 nd dose					
Varicella ⁹ (VAR)									←.....1 st dose.....→			2 nd dose					
Hepatitis A ¹⁰ (HepA)									←.....2-dose series, See footnote 10.....→								
Meningococcal ¹¹ (Hib-MenCY ≥6 weeks; MenACWY-D ≥9 mos; MenACWY-CRM ≥2 mos)			See footnote 11											1 st dose	2 nd dose		
Tetanus, diphtheria, & acellular pertussis ¹² (Tdap: ≥7 yrs)														Tdap			
Human papillomavirus ¹³ (HPV)														See footnote 13			

Figure 2: Recommended immunization schedule for adults aged 19 years or older by age group, United States, 2017
 Retrieved from: <https://www.cdc.gov/vaccines/schedules/hcp/imz/adult.html>

Vaccine	19–21 years	22–26 years	27–59 years	60–64 years	≥ 65 years
Influenza ¹	1 dose annually				
Td/Tdap ²	Substitute Tdap for Td once, then Td booster every 10 yrs				
MMR ³	1 or 2 doses depending on indication				
VAR ⁴	2 doses				
HZV ⁵				1 dose	
HPV–Female ⁶	3 doses				
HPV–Male ⁶	3 doses				
PCV13 ⁷					1 dose
PPSV23 ⁷	1 or 2 doses depending on indication				1 dose
HepA ⁸	2 or 3 doses depending on vaccine				
HepB ⁹	3 doses				
MenACWY or MPSV4 ¹⁰	1 or more doses depending on indication				
MenB ¹⁰	2 or 3 doses depending on vaccine				
Hib ¹¹	1 or 3 doses depending on indication				

Figure 3: UPI Legal Framework Timeline



References:

- American Immunization Registry Association (AIRA). (2017). *Data Validation Guide for the IIS Onboarding Process* (2017) Retrieved from AIRA website:
http://www.immregistries.org/resources/data/AIRA_Data_Validation_Guide.pdf , 7.
- American Immunization Registry Association (AIRA). (2016, September). *Confidentiality and Privacy: Considerations for Immunization Information Systems*. Retrieved from the AIRA website: http://www.immregistries.org/AIRA_Confidentiality_and_Privacy.pdf , 8.
- American Immunization Registry Association (AIRA) (2014, January). *Survey of Immunization Reporting to Immunization Information Systems by Major U.S. Pharmacies: A Summary of the Methods, Successes and Challenges of Pharmacy-IIS Interfaces*” Retrieved from AIRA website:
http://www.immregistries.org/resources/AIRA_Pharmacy_IIS_White_Paper.pdf, 35.
- American Immunization Registry Association (AIRA). (2013, December). *Patient Identification and Matching Initiative Stakeholder Meeting*”. Authors: Audacious Inquiry Consulting and Lee Stevens. Retrieved from AIRA website:
http://www.immregistries.org/resources/data/Patient_Matching_Mtg_Slides.pdf, 11.
- American Immunization Registry Association (AIRA). Modeling of Immunization Registry Operations Workgroup (MIROW). (2006, December). *Vaccine Level Deduplication in Immunization Information Systems*. Retrieved from AIRA website:
http://www.immregistries.org/resources/aira-bp_guide_vaccine_dedup_120706.pdf, 7.
- American Medical Informatics Association (AMIA). National Agenda for Public Health Informatics. (2001, November). *Journal of Public Health Management and Practice*, 4.
- Appavu, S. I. (1997). Analysis of Unique Patient Identifier Options—Final report. Washington, DC: U.S. Department of Health and Human Services.
- Arzt, A. (2017, March). Is There a National Strategy Emerging for Patient Matching in the US? *Medical Research Archives*, 5(4), 1,2,3,5.
- Australian Government. Department of Health (2013) National Immunisation Strategy for Australia 2013-2018. Retrieved from: <https://tinyurl.com/yaleog5d>
- Berg, N. (2016, March 10). Pay Bitcoin or Else: Hackers Have Figured Out How Easy It Is to Take Down a Hospital. Retrieved from *Fusion.net* website:
http://fusion.net/story/278801/hackers-ransomware-hospital-smart-cities/?utm_source=facebook&utm_medium=social&utm_campaign=realfuture
- Brailer, D. (2012, March). David Brailer And Farzad Mostashari: Two National Health IT Czars Compare Notes. *Health Affairs* 31(3),475-480. doi: 10.1377/hlthaff.2011.1361.

- Butler, B. and Murphy, J. (2014, March). The Impact of Policies Promoting Health Information Technology On Health Care Delivery In Jails and Local Communities. *Health Affairs* 33(3),487-492. doi: 10.1377/hlthaff.2013.1125.
- Canada, Government of (2017). National Immunization Strategy: Objectives 2016 – 2021. Retrieved from: <https://tinyurl.com/y7bhh757>
- Carpenter, P. C., Chute, C. G. (1994). The Unique Health Identifier: A Discussion and Proposal. *Proc Annu Symp Comput Appl Med Care*. AIMA, 49-53.
- Hillestad, R et al. (2008). Identity Crisis: An Examination of the Costs and Benefits of a Unique Health Identifier for the US Healthcare System. *Rand Corporation*, xi,xiii,29,33. Retrieved from <http://www.rand.org/pubs/monographs/MG753.html>.
- Gliklich RE, Dreyer NA.(2014). Registries for Evaluating Patient Outcomes: A User's Guide [Internet]. 3rd edition. *Agency for Healthcare Research and Quality (AHRQ)*. Ch. 17 “Managing Patient Identity Across Data Sources”.
- Grannis. S. et al. (2009, June) “Privacy and Security Solutions for Interoperable Health Information Exchange. Research Triangle Institute (RTI), 4-1, 5-2, 5-3, 5-4 Retrieved from: <https://www.healthit.gov/sites/default/files/patient-matching-white-paper-final-2.pdf>
- Grant, F.J., Myerburg, J.D., Wain, J.A., et al. (2012). National Practice Assessment: Immunization Information Systems Patient De-duplication”. Unpublished manuscript, Rollins School of Public Health, Emory University.
- Greenberg, M., Hillestad, R. et al. (2009, March/April). Crossed Wires: How Yesterday's Privacy Rules Might Undercut Tomorrow's Nationwide Health Information Network. *Health Affairs* 28(2), 450-452. doi: 10.1377/hlthaff.28.2.450.
- Hall, J and McGraw, D. (2014).” For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed”. *Health Affairs* 33(2), 216-221. doi: 10.1377/hlthaff.2013.0997.
- Healthcare Information and Management Systems Society (HIMSS). (2011). Patient Identity Integrity Toolkit. Patient Identity Integrity Resources and References. Retrieved from: <http://www.himss.org/library/healthcare-privacy-security/patient-identity>
- Hinman and Ross. (2010). “Immunization Registries Can Be Building Blocks For National Health Information Systems.” *Health Affairs* 29 (4), 676,678.

- Institute of Medicine (IOM) (1997). The Computer-Based Patient Record: An Essential Technology for Health Care, Revised Edition. *The National Academies Press*. Washington, DC: 13, 48. Retrieved from: <https://doi.org/10.17226/5306>.
- Johnson Foundation. (2013) Outbreaks: Protecting Americans from Infectious Diseases. (2013, December). Retrieved from <http://www.healthyamericans.org/assets/files/TFAH2013OutbreaksRpt11.pdf>, 23, 26
- Kuperman, G.J. (2011). Health-Information Exchange: Why Are We Doing It, and What Are we doing?. *J Am Med Inform Assoc*. 18(5), 678. doi: 10.1136/amiajnl-2010-000021.
- Leonard, D.C. and Pons. A. (2009, July). Realization of a Universal Patient Identifier for Electronic Medical Records Through Biometric Technology. *Technology in Biomedicine*. 13 (4), 494, 495.
- Lumpkin, John. (2009). Perspective: E-Health, HIPAA, And Beyond. *Health Affairs* 19(6), 149-151., 4.
- Martin, Daniel W. (2015). Immunization Information Systems: A Decade of Progress in Law and Policy. 2015 *Wolters Kluwer Health, Inc*. 296.
- McKinley and Frase. (1970). Launching Social Security: A Capture and Record Account, 1935-1937, 180-181. *University of Wisconsin Press*, 180-181.
- McDonald, Clement. (2009, March/April). Protecting Patients In Health Information Exchange: A Defense Of The HIPAA Privacy Rule. *Health Affairs* 28(2), 447-449. doi: 10.1377/hlthaff.28.2.447.
- Modeling of Immunization Registry Operations Workgroup (MIROW) Modeling of Immunization Registry Operations Workgroup. (2017, April) Operational Best Practice Guidelines & Related Resources. Retrieved from CDC website: <https://www.cdc.gov/vaccines/programs/iis/activities/mirow.html>
- Modeling of Immunization Registry Operations Workgroup (MIROW). *Vaccination Level Deduplication in Immunization Information Systems*. (2006, December). Retrieved from www.immregistries.org/resources/AIRA-BP_guide_Vaccine_DeDup_120706.pdf
- National Association of County and City Health Officials (NACCHO). (2014, January) “National Profile of local health departments”, 62. Retrieved from: <http://archived.naccho.org/topics/infrastructure/profile/upload/2013-National-Profile-of-Local-Health-Departments-report.pdf>
- National Association of County and City Health Officials (NACCHO) (2016). Electronic Health Information: Local Approaches to Data Sharing. Retrieved from: https://www.networkforphl.org/_asset/2f2sx3/Electronic-Health-Information---State-and-Local-Approaches-to-Data-sharing.pdf

- Netter, W. (2003, Winter) Curing the Unique Health Identifier: A Reconciliation of the New Technology and Privacy Rights. *Jurimetrics* , 43 (2), 165-186.
- Orstein, C. (2015, February 27). Fines Remain Rare Even As Health Data Breaches Multiply Retrieved from *NPR.org* website: <http://www.npr.org/sections/health-shots/2015/02/27/389328345/fines-remain-rare-even-as-health-data-breaches-multiply>
- Peel, D. (2012, January 23). Should Every Patient Have a Unique ID Number for All Medical Records? Retrieved from *WSJ* website: <https://www.wsj.com/articles/SB10001424052970204124204577154661814932978>
- Public Law 104–191. Health Insurance Portability and Accountability Act (HIPAA). 104th Congress. (1996), 110 STAT. 2025.
- Public Law 105–277. Omnibus Consolidated and Emergency Appropriations Bill, Sec. 516, 1998 105th Congress. (1999), 112 STAT. 2681–386.
- Public Law 109-13. Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief”. Division B, Real ID Act of 2005. 109th Congress, Retrieved from: <https://www.congress.gov/109/plaws/publ13/PLAW-109publ13.pdf>, p. 119 STAT. 314.
- Public Law 114-113. Cybersecurity Act of 2015. 114th Congress, Retrieved from: <https://www.congress.gov/bill/114th-congress/senate-bill/754/text#toc-id9d4d6969369a4054a8bb7e0880c6555b>.
- Public Law 114-255. 21st Century Cures Act, HR 6, RFS, 114th Congress. (2016). Retrieved from: <https://www.congress.gov/114/bills/hr6/BILLS-114hr6rfs.pdf>.
- Public Law 115-31. Depts. Of Labor, HHS, and Education and Related Agencies, Appropriations Bill, 2017. HR Committee on Appropriations Report. 114th Congress. Retrieved from: <https://appropriations.house.gov/uploadedfiles/hrpt-114-hr-fy2017-laborhhsed.pdf>, 108.
- Reed, K. (2004, November 19) Immunization Registry Information Systems. *School Nurse News*.
- Ruiz, Michelle. (2012). Arizona Patient Deduplication-Going Beyond the Automated Function. American Immunization Registry Association. Retrieved from: http://repository.immregistries.org/files/resources/5835aded1fa7e/patient_deduplication_-_going_beyond_the_automated_function_.pdf
- Ternier, Alex. Papadouka, Vikki. (2012) Immunization De-duplication: A Program Developed in New York City to Reduce Duplicate Immunizations. American Immunization Registry

Association. Retrieved from: <http://repository.immregistries.org/resource/immunization-de-duplication-a-program-developed-in-new-york-city-to-reduce-duplicate-immunizations/from/iis-data/data-quality/deduplication>

Stockwell, M. et al. (2016) Immunization Data Exchange With Electronic Health Records. *Pediatrics*. 137 (6), 2, 23,26.

U.S. Department of Education. "Parents' Guide to the Family Educational Rights and Privacy Act.pdf". (2007, October). Retrieved from: <https://www2.ed.gov/policy/gen/guid/fpco/brochures/parents.html>

U.S. Department of Health & Human Services (HHS). Centers for Disease Control and Prevention (CDC). National Center for Infectious and Respiratory Diseases (NCIRD). Immunization Information Systems Support Branch (IIS SB). (2013, June). Immunization Information Systems Patient-Level De-duplication Best Practices" Retrieved from: CDC website: <https://www.cdc.gov/vaccines/programs/iis/interop-proj/downloads/de-duplication.pdf>, 0, 9

U.S. Department of Health & Human Services (HHS). Centers for Disease Control and Prevention (CDC)/National Center for Infectious and Respiratory Diseases (NCIRD)/Immunization Information Systems Support Branch (IIS SB). (2012, September) "Meaningful Use and Immunization Information Systems". Retrieved from CDC website: <https://www.cdc.gov/vaccines/programs/iis/meaningful-use/index.html>

U.S. Department of Health & Human Services (HHS). Centers for Medicaid Services (CMS). (2012, October). Eligible Professional Meaningful Use Core Measures. EHR Incentive Program. Retrieved from CMS website: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_MeaningfulUseSpecSheet_TableContents_EPs.pdf

U.S. Department of Health & Human Services (HHS). Centers for Medicaid Services (CMS). (2016, June). Unique Identifiers Overview. Retrieved from CMS website: <https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Unique-Identifier/UniqueIdentifiersOverview.html>.

U.S. Department of Health & Human Services (HHS) (2017, June). HIPAA for Professionals. HHS Health Information Privacy. Retrieved from HHS website: <https://www.hhs.gov/hipaa/for-professionals/index.html>.

U.S. Department of Health & Human Services. (HHS). Office of the Assistant Secretary for Planning and Evaluation (ASPE). (2012, September) White Paper on Unique Health Identifier for Individuals. Retrieved from ASPE website <https://aspe.hhs.gov/white-paper-unique-health-identifier-individuals>

U.S. Department of Health & Human Services. (HHS). (2002). Health Information Privacy. What Were the Major Modifications to the HIPAA Privacy Rule that (HHS) adopted in

August 2002? Retrieved from HHS website: <https://www.hhs.gov/hipaa/for-professionals/faq/192/were-the-major-modifications-to%20the-hipaa-privacy-rule-adopted-in-aug-2002/index.html> .

U.S. Department of Health & Human Services. (HHS). National Committee on Vital and Health Statistics (NCVHS). (2000, June). 50th Anniversary Symposium Report. Retrieved from: <https://www.cdc.gov/nchs/data/ncvhs/nchvs50th.pdf>, 26, 39, 77.

White, A. et al. (1997). Facilitating Linkage Through Unique Health Identifiers: A Difficult Endeavor. *Top Health Inf Manage*. 17 (4) 1997, 32-9.

Winton, R. (2016, Feb. 18). “Hollywood Hospital Pays \$17,000 in Bitcoin to Hackers: FBI Investigating. *LA Times*. Retrieved from: <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>

World Health Organization (WHO). (2007, May) Patient Identification. *Patient Safety Solutions*. 1(2). Retrieved from WHO website: <http://www.who.int/patientsafety/solutions/patientsafety/PS-Solution2.pdf>

Srivastava, Roli (2016, Feb. 27) “Linking Aadhaar to Better Healthcare”. Retrieved from: <http://www.thehindu.com/news/cities/mumbai/news/linking-aadhaar-to-better-healthcare/article8288043.ece>