An Evaluation of the Socio-Political Interactions of Health Data Architecture to Inform Ethical Data Governance

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Luke McPhillips

4/12/2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: Luke McPhillips

Approved: _____ Date _____
Rider Foley, Department of Engineering and Society

Introduction

Examining security and privacy issues with the collection of health data, Patil and Seshadri (2014) cite a study from the Ponemon Institute, an organization conducting independent research on data privacy, that concludes 94% of hospitals had one or more security breaches in the past year. Data is now a core component of modern medical care. It enables hospitals to track long-term health trends, recognize and respond accurately to the individuality of personal health and view progress towards public health goals. As the prevalence of data in healthcare continues to increase, there is a critical need to implement robust structures of data governance. Governments and healthcare systems around the world are increasingly seeking to explore public policy options to protect patient privacy but also support the usage of data for improved care. A clear example of this in the United States is the Health Insurance Portability and Accountability Act, a United States law which sets standards for the protection of data throughout the healthcare system.

Data-intensive healthcare solutions are not a trend just for the high-income world. Stakeholders in low- and middle-income countries (LMIC) also seek to build systems for collecting, storing, and analyzing data for improved patient outcomes. But the barriers to success are significantly harder to navigate, Tuti et al. (2015) provides a non-exhaustive list of challenges faced in clinical data management in Kenya:

1. Resource context: There is shortage of staffing, limited funds, unreliable power sources.
2. IT infrastructure: Non-comprehensive electronic health record systems, poor internet connectivity, complex data storage and access procedures.
3. Pre-existing reporting structures: existing national health information system requirements on data capture and storage, designed to address stakeholder needs.

4. Data collection tools: Non-standardized collection protocols, usage of paper records. (p. 185)

My capstone team is taking on a small portion of this challenge. Under our advisor, Doctor Donald Brown, we will develop an algorithm deploying image capture and optical character recognition techniques to scan perioperative (surgical data) flowsheets from medical centers in Rwanda. This data will be captured and transferred securely to the University of Virginia for storage and further research, with remote access provided to physicians in Rwanda. Our goal is a system to facilitate the growth of a stronger, independent data infrastructure built out within Rwanda. The client is a UVA anesthesiologist who travels through Doctors Without Borders each year to the University Teaching Hospital of Kigali, which will be the partner site for this project.

Complications arise with the existence and storage of private, personal health data. Wyber et al. (2015) cite work from a study completed at the London School of Economics, writing:

> The risk of accidental or intentional breaches of data security may be particularly high in settings with high levels of illiteracy and corruption that are undergoing rapid technological transition. In many such settings, legislation supporting the privacy and security of information services is frequently underdeveloped and rarely enforced. (p. 205)

The authors call attention to the complexity of technological advancement, and the difficulty of maintaining a power equilibrium that shines light on the array of stakeholders that comprise data systems. The increasing complexity of medical care and patient needs shapes policy development to guide growing human-centered health data systems in low- and middle-income countries.

Analyzing health data governance using techno-politics and social construction of technology

Delving deeper into the data accessibility and protection component of my capstone project, I will leverage two frameworks towards analysis of the socio-technical development of data applications and governance in LMIC. Large-scale health data systems are inherently political, the risks and opportunities associated with the storage of private data naturally associate with centralized political systems that leverage strong institutional structures to protect individual liberties. Winner (1980) references Plato as evidence for his claim of inherent techno-politics:

> Plato goes on to suggest that governing a state is rather like being captain of a ship or like practicing medicine as a physician. Much the same conditions that require central rule and decisive action in organized technical activity also create this need in government. (p. 129)

The reference towards practice of medicine holds incredible relevance, implying the political connotations of medical care provision have prevailed for 1500+ years. Medical environments continue to lend themselves to the same centralized power structure and hierarchical order of command for the support of decisive, safe actions.

Tiffin, George and Lefevre (2019) draw on their personal experiences operating with health data in South Africa and India to support this, calling for the establishment of strong data governance procedures to mitigate potential power imbalances. Two pillars of data governance they define are ethics/informed consent and legal frameworks. Without regulation, data systems can instead be used as a tool to perpetuate the inequities that health systems aim to reverse through improved care. It is the opportunity for misuse that therefore makes data political, and inherently requires transparency and centralized management.

This framework for analysis is not complete without the complementary consideration of the rapidly evolving nature of health innovation. While I will argue the above point that technical health systems maintain inherent politics, the procedures, methods and basis of care is evolving according to the needs of diverse social groups. Consider the framework illustrated by Pinch and Bijker (1987). The needs of social groups such as patients, providers, and other vested system interests are constantly being re-defined by expanding data capabilities. Reciprocally, the functionalities of medical systems are simultaneously evolving in response to those needs. Our capstone team's client (Dr. Marcel Durieux) briefly discussed a program in Rwanda where blood is flown by drone to regional medical centers. In this example, the needs of patients and rural medical providers are defining the construction of this technical system and in response the needs of those individuals and organizations are evolving to higher orders of complexity. Providers may soon need to use data to predict required blood types and quantities.

The capstone project itself supports similar interpretation. Hospitals in LMIC are seeking to use health data to provide more customized patient journeys and improve doctor training programs. As they develop their capabilities, the needs of patients evolve to now include data rights. The technology must now respond and this need is the genesis of our work. The necessity for using a two-pronged framework of analysis is driven by the increasingly complex profiles of stakeholder groups. In his article on techno-politics, Winner (1980) references Engels' examples of railroads and shipping as inherently political technologies:

> Similar lessons are adduced in Engels's analysis of the necessary operating conditions for railways and ships at sea. Both require the subordination of workers to an "imperious authority" that sees to it that things run according to plan. (p. 129)

These traditional systems are either publicly owned by shareholders or privately controlled. Ownership of capital is clear, and there is a clear organizational structure from those who conduct business strategy to those who perform field work. In contrast, debate exists over who actually owns data and whether that is the right question to truly frame the conversation of societal power. Rosner (2014) argues:

> However, there is a great deal of evidence for citizen concern with control of information about them. Perhaps, then, ownership is not the appropriate framework from which to address people's anxieties and the broader rights of data protection and privacy. Control regimes and rights are better perspectives from which to consider the state of personal data. (p. 627)

It is this notion of centralized control versus private ownership which requires the usage of two frameworks. In the technical dimension of this paper I discuss the privacy of HIV data, a clear example of how human identity is tied to personal health data. Drilling deeper into this relationship, I will argue that the play of this notion of self-ownership against the larger notion of "control" is what must drive a human-centric development of the societal framework of values within which the requisite political hierarchies and governance systems of data operate.

Flowsheet digitization to support improved care in low- and middle-income countries

The technical project can be broken into three segments: image classification, data storage and data protection and access. Surgical data at the University Teaching Hospital of Kigali is collected in handwritten flowsheets. Our team's goal is to develop an end-to-end system for the scanning, upload, and analysis of these flowsheets. Similar data collection work has been done electronically in Kenya through REDCap, a proprietary Vanderbilt clinical software.

Sileshi et al. (2017) implemented a simple electronic data collection system to digitize a 132-field form of surgical data and conduct statistical tests on surgical outcomes. This collection was done in real-time using tablets and did not include a means for digitizing data stored in older paper records. Our project will take a two-pronged approach, providing a means for the automated digitizing of both current and older surgical records.

Scanned flowsheet images require the construction of deep learning algorithms to extract data that can be stored in a structured manner. The images in Appendix A display the pre/perioperative flowsheet (Durieux, 2019). The record contains an array of information types that can be categorized into three analytical bins:

1. Graphical: Graphical data will require building an algorithm that recognizes the spatial relationships of points on the graph to assign values to locations. The data will be stored as a time series.
2. Structured handwritten text: Includes fields on the form with finite options for entries. Examples include types of surgical procedures, medications, dosages. Our team will utilize a classification algorithm to match handwritten words against a set library of potential terms.
3. Checkboxes: We will use optical mark recognition techniques analyzing light patterns to predict whether a box is empty or filled.

Our team is leveraging open source code to perform these tasks.

The data extracted from the medical record will be stored in a relational database at the University of Virginia for further academic research both in the United States and Rwanda, and our team will look to integrate our results with the data systems that do already exist in Rwanda. Verbeke et al. (2012) discuss this in their use of OpenClinic, an opensource software, at The

University Teaching Hospital of Kigali. In a 2010 survey, they found that nearly 70% of patients could be identified by electronic record (p. 11). Our team will map the data stored at UVA through our project back to these records using patient identifiers. This will best support further analytics and extraction of information.

The final component of the project is the definition of database accessibility guidelines. We will address this step after successful development and testing of our technical system. Our team will seek to answer the following questions:

- Who should have access to this data?
- What are potential use cases for how the data will be used?
- What legal requirements surround the international transfer of patient data?
- How do we anticipate the needs of this infrastructure to evolve?

These questions will be the foundation for our team's exploration of open source software's impact. While the example discussed at the beginning of this section utilized proprietary software (REDCAP), Kanter et al**.** (2012) discuss what social and technical advantages have led to the download of opensource medical data platforms in over 50 countries for efficient and ethical data storage:

> Open source platforms were preferred over proprietary products…(They) require no license fees, can be tailored to fit the needs of the project, and have support from the development community contributing to and using the particular product…This includes cost, flexibility, ownership, and the benefit of a large passionate, and involved developer and implementer community. (p. 193-194)

These benefits have been clear to our team, it is what has supported all our work so far and enabled us to build code we could not understand ourselves. The definition of accessibility

guidelines will mark a shift in thinking, where our team will examine the system we build and try to identify risks that come with using open source software with patient medical data.

Research question and methods for case analysis

How are governments of low- and middle-income (LMIC) countries responding to the challenge of protecting patient data rights as they move to quickly build digital health ecosystems? Data is an irreplaceable component of the human future, but considering the barrage of data breaches in the past decade, it is clear that a culture of safe and ethical usage has not yet permeated any corner of the globe. Underprivileged populations are at most risk. Beck, Gill & Lay (2016, p. 2) conducted focus groups across LMIC with medical field stakeholders and found that, "Of the 49 countries claiming to have developed (data) privacy laws, 55% reported that they had not developed any guidelines for the implementation of such laws." The concerns raised by this finding are the basis for my research question and the examination of the nuances of data governance in LMIC, and how it is shaped by institutions, people, and data systems themselves.

I used a case-study approach to provide a review of the cultural and political complexities that can inform the development of cohesive health data systems. Examining four LMIC across the globe (including Rwanda), I leveraged a multi-directional set of techniques to provide just support for the bilateral framework outlined above. Policy analysis drove the evaluation of how data systems have altered the public space and pervaded political dialogue. I used the four pillars for ethical data governance outlined by Tiffin, George, and Lefevre (Ethics and Consent, Data access, Sustainability and Legal Frameworks) to examine how the existence of data presents the same challenges to governments building health data infrastructure across the world. Table 1

below shows the sub-criteria Tiffin, George and Lefevre define for each pillar. These sub-criteria were the basis for assessing country policy.

Table 1. Sub-criteria of the pillars for ethical data governance

Ethics and consent	Data access	Sustainability	Legal framework
• Vulnerability • Potential harms • Confidentiality • Informed Consent • Beneficence • Return of results	• Procedural oversight • Structural control	• Documentation • Back-ups • Metadata • Accessibility • Fidelity	• Right to privacy • Data repurposing • Data security • Third-party access

An evaluation of health data systems in the selected countries grounded the conversation for how the needs of individuals, medical groups, international NGOs and the like are shaping the construction of data systems. The referencing of the drone system and my capstone project above are two examples. Binagwaho and Scott discuss crucial characteristics of health data application, and call attention to the intertwining of politics with socially defined health goals:

> Each country should promote policies that foster synergies across sectors. The health sector cannot achieve health-related goals as an isolated, stand-alone system. For example, it needs the involvement of local leaders who govern by proximity and ensure the implementation of social policies… (p. 204)

To understand how the data landscape is changing in each country, I evaluated strategic plans for health care sector innovation along three dimensions: a clearly articulated policy goal, breadth of collaborators in constructing the plan, and clear specification of initiatives to improve health data

systems. This portion of the analysis enables a review of whether health sectors are effectively engaging with their stakeholders to advance data systems with clear, actionable goals. The four pillars outlined by Tiffin et. al. frame a view of whether systems are enacting needed change, the three dimensions informed by Binagwaho and Scott examine how that change is pursued.

Case results for India, Poland, Rwanda and Malaysia

Governments of LMIC are looking to establish and improve policy to articulate patient data protection standards and create strong data governance systems, but are struggling to keep pace with the rate of innovation in data usage and their own public health objectives. In the four countries examined only Malaysia and Poland have published data protection laws robustly outlining the rights of individuals to control the data they generate, and only India has published healthcare sector specific guidelines that recognize the unique, deep implications of vulnerable health data and the complexity of interactions between state and non-state agents. Malaysia and Poland have outlined clear and relatively complete policy for procedures and legal frameworks. India is the only country to take a clear focus to the notion of data sustainability, pushing towards a defined notion of interoperability. Other countries are focused on physical sustainability, maintaining the physical infrastructure to service data initiatives. Table 2, at the top of the next page, summarizes the performance of each country against the four pillars. Of significant note is that the two countries with more resources per capita to leverage (Malaysia and Poland) have the most comprehensive coverage of the four pillars.

Table 2. Evaluation of countries against four pillars of ethical data governance

	Ethics and consent	Data access	Sustainability	Legal framework
India		✓	✓	
Poland	✓	✓	✓	✓
Rwanda		✓	✓	
Malaysia	✓	✓		✓

Case study: India

Policy overview

India is rapidly transitioning towards digital health systems, recognizing the value in efficient technological systems in providing care to a large and growing population. The Indian Ministry of Health and Family Welfare defined an objective to construct a seamless health information system in coordination with public and private healthcare providers in their latest National Health Policy (2017). The main documents pertaining to health data governance are titled Health Domain Metadata and Data Standards (HDDS) and EMR-EHR Standards for India. HDDS outlines the technical construction of integrated information technology systems and the EMR-HER Standards for India provides a more holistic direction towards human interaction with data.

Drafted and published for review are India's Personal Data Protection Bill (PDPB) and the Digital Information Security in Healthcare Act (DISHA). These documents are widely viewed as potentially lifting data policy in India up to the standards set in the European Union with the General Data Protection Act and in the United States with HIPAA. Together, they will

give both comprehensive cover of data-related concerns and targeted policy for health care stakeholder needs.

Ethics and consent

The EMR-EHR Standards for India includes a strong structure for personal data rights. The section clearly articulates that data is owned by the patient, and specifies forms of protected information such as biometric data.. Data is held in trust on behalf of the patient, the patient has the right to access their data and to prevent access to unauthorized parties. While medium of obtaining consent is not described, the document clearly outlines what practices require patient consent. While policy is drafted (PDPB, DISHA), there is no comprehensive patient-centric policy in place.

Data access

The EMR-EHR Standards for India describe the technological steps to be taken to ensure data security, stating "The security standards require healthcare provider to implement reasonable and appropriate administrative, physical, and technical safeguards…" (p. 24). These standards include identity authentication to access data networks, forced log-off from electronic sessions and the distinction of access scope depending on a physician's clinical practice type. Further, all actions related to electronic health information must be recorded for audit.

Sustainability

The HDDS of India specifies much of the technological implementation of sustainability goals. The document focuses on the notion of interoperability, stating:

> One of the key challenges is to provide the information architecture for the increasingly large and growing complexity of information needs … Establishing nationwide

> interoperability … is one of the key steps in the endeavor to better manage this complexity. (HDDS, YEAR, p. 9)

The document defines database architecture standards, how tables should be organized and connected to facilitate data sharing across systems. It pursues a notion of system sustainability different than other countries, focusing more so long-term usability than physical integrity.

Legal framework

The Information Technology Act, last updated in 2011 with latest security provisions, outlines the legal guidelines for the storage and handling of personal data. The act is not specific to the health sector. The upcoming policies discussed above will greatly enhance India's legal framework, establishing specific regulatory bodies and procedures for handling violations of data usage practices.

Digital health strategy: Policy goal

In 2019, the Indian national government published a National Digital Health Blueprint for public review. The document identifies the power of digital technologies in achieving better, more inclusive health care. Recognizing the breadth of lived experience in a country of over one billion**,** data-driven care is an opportunity to provide equitable care to all communities.

Digital health strategy: Plan collaborators

The Blueprint was published by a Commission established by the Indian national government. The committee included stakeholders from the Ministry of Health and Family Welfare and other Ministries, non-profit groups informing the development of health sector policy and related government ministries. Input was not gained from parties holding specific technological expertise.

Digital health strategy: Initiatives

The Blueprint identifies four core areas of focus for investment, a clear identification method for ensuring that each person maps to a unique identifier to support expansion of electronic health records, empowerment of the citizen to control the security and permissions for their data, simple and clear mediums for delivering care through digital services, and interoperability – the construction of an integrated network of data platforms to serve as a basis for all other efforts to ensure equitable care. The Blueprint breaks these down further and identifies specific action items that build towards accomplishing them.

Case study: Poland

Policy overview

Poland benefits from EU resources dedicated to policy development, the General Data Protection Regulation (GDPR) passed by the EU in 2016 provides comprehensive coverage with regards to data handling in the EU across economic sectors. As a regulation, all members of the EU are required to implement its guidelines. Poland has been amending data security policy across its departments. This analysis will evaluate the standards of the GDPR Poland is in the process of implementing. Of note is the Act on the Protection of Personal Data, the Polish policy on protection of person's and their data. Looking forward, Poland is looking to an EU communication on digital transformation of health and care and a report titled Computerization Trends for E-Health Poland for direction in improving digital health systems.

Ethics and consent

Well outlined in the GDPR and the Act on the Protection of Personal Data, consent is outlined by rights of the data subject. The GDPR outlines 11 rights of the data subject including right to access, right to information system transparency, and the right to be forgotten.

Data access

Data access procedures are fully outlined in both the GDPR and the Act on the Protection of Personal Data. Individuals have the right to claim their data and robust procedures are in place for practitioners to access patient's data. Practitioners can only see data that is directly relevant to providing care and patients are given full authority to determine whether more information should be provided. Poland has also established a Personal Data Protection Office to supervise compliance.

Sustainability

The GDPR details procedures for maintaining the integrity of data, Poland's efforts to update legislation across the various impacted sectors of the economy represent work to improve data sustainability. This includes emergency standards in case of failure of physical infrastructure as well as organization and interoperability standards.

Legal framework

As a regulation, the GDPR does not have legal authority. The various updates to current law enacted by Poland do. As displayed in the Act on the Protection of Personal Data, a clear legal framework has been put in place for handling misuse of health data. Supervisory authorities are established and fines/punishments are in place.

Digital health strategy: Policy goal

The document Computerization Trends details the efforts of the Polish government to create a unified health information technology system. The government aims to provide a streamlined experience for its citizens, and to leverage data to improve patient engagement with provision of care.

Digital health strategy: Plan collaborators

The Computerization Trends document represents the perspectives of health industry professionals at both the national level and the EU level. It does not discuss technical input sources, leaving an assumption that strategies to improve information and communication technologies are completely independent of digital health development.

Digital health strategy: Initiatives

The Computerization Trends document details efforts to improve citizen access to health information as well as establishing good practices for collection and sharing of data. These efforts are jointly defined by Poland and the EU, and represent a collaborative effort to uphold the goals of the EU in practice in Poland.

Case study: Rwanda

Policy overview

Rwanda is pioneering information technologies in Africa, specifically investing heavily in health data systems. Three policies outline the countries progress on establishing effective digital health programs. The last policy for the health sector was published in 2015. It identifies integration of data platforms, data collection and digitization (data was/still is collected on paper flowsheets during surgical events) and data quality as three significant challenges for the sector in the next decade. It advocates for further development of data sharing protocols and more strengthened efforts to improve the quality of data that is stored digitally. The Health Sector Information and Community Technology Security Policy (ICT) describes security practices to be taken by health sector professionals to ensure data is stored, accessed, and protected.

The Data Revolution Policy describes Rwandan efforts to transition to an information-based economy. It references legal frameworks in place currently and identifies the priorities of

the Rwandan government in building a data-centric economy. The policy is not directly defined for the health sector. The country is working on a personal data protection law to cover the rights of individuals to control their own data. There is not currently a draft of this legislation published. Of note is the jointly produced Personal Data Protections for Africa document, a collaborative effort of the Internet Society (an American non-profit dedicated to best technological practices) and the African Union. This document states the challenges faced by African countries in implementing individual-centric privacy standards and requirements of effective legislation.

Ethics and consent

Without publication of the mentioned personal data protection law, Rwandan policy is sparse on consent practices. Current policies relevant to the health sector do not provide a full overview of what identifying patient information is considered private, and what procedures are used for obtaining consent for data usage. The Data Revolution Policy makes mention of personal data protection, but only cites laws pertaining to business transactions and the use of digital signatures. The Personal Data Protections document provides a robust coverage of the challenges African countries face in generating effective policy towards data consent, this should provide a baseline towards the work Rwanda is doing towards a personal data protection bill.

Data access

Data access procedures are clearly defined in the health sector ICT policy. It provides an extraordinarily in-depth coverage of protection practices including log-in practices, use of internet connections, construction of an information security implementation team and security auditing. The policy provides a technician perspective towards data security, defining practices

for information technology services. It does not provide a description for how patients/those who generate data can access their information.

Sustainability

The health sector ICT policy discusses processes for backing up data and ensuring the physical integrity of operating systems. The policy outlines procedures for handling excessively humid weather and power outages, as well as procedures for filing change reports (descriptions of changes taken to modify technology) and where to store back-up data.

Legal framework

The health sector ICT policy outlines compliance practices expected by information technology users, specifying areas where legislation is in place. The policy identifies four areas where legislation is already in place:

- Documentation steps towards implementing the defined data system controls
- Process of changing software systems
- Protection of confidentiality of records
- Process for advising third-party data owners on procedures for secure data storage

There is no accessible, published legislation on legal practices for data mis-use or breach of privacy.

Digital health strategy: Policy goal

The current Rwandan strategic plan for the health sector was published in 2018 for a six-year period. It is titled The Fourth Health Sector Strategic Plan, and was drafted to recognize the evolving health needs of the Rwandan populace and economic conditions continue to strengthen. The overall objective is to push for universal access to care regardless of background.

Digital health strategy: Plan collaborators

The strategic plan identifies five main stakeholders: national government, local government, private actors, development partners and international organizations. It emphasizes collaboration recognizes core competencies based on positioning in the system. The plan designates multiple working groups to carry forward the work outlined through continued coordination of stakeholder groups. The plan does not inclusion of including technical experts.

Digital health strategy: Data Initiatives

The plan defines the strategic direction of health information systems, identifying interoperability and data quality as two key areas for improvement to support data-driven care. Policy for data security, improving best practice for integrated information systems and expanding usage of electronic medical records are cited as key strategies in accomplishing health sector objectives.

Case study: Malaysia

Policy overview

As an upper-middle income country, Malaysia does not fit into the typical categorization of a low- or middle-income country. But the nation has moved between middle- and upper-middle classification, and has been discussed as a subject of the middle-income trap. While not the subject of this paper, the middle-income trap is the concept that a country can get stuck as middle-income. This occurs because the country loses its ability to compete in the global marketplace as wages rise but the economy remains dependent on low-margin manufacturing markets. As such, the country provides an intriguing comparison case to the others selected.

Three policies outline Malaysia's progress, foremost is the personal data protection act of 2010. The act provides a full structure for classifying sensitive data, detailing access and usage

standards, and defining legal and compliance means. The confidentiality guidelines of the Malaysia Medical Council narrow the scope, looking at data sharing practices and building a patient-centric view on data security rights. Last, the National Cybersecurity Policy of the Ministry of Science, Technology and Information details the high-level objectives of the country in building out secure information systems. This document (as well as the personal data protection act) is not specific to the health care sector. It also does not discuss any form of policy implementation.

Ethics and consent

The Personal Data Protection Act and the confidentiality guidelines lay out the foundation for ethics and consent in Malaysia. The Personal Data Protection Act states the consent requirement for the dissemination of data and defines a data subject's rights to control the storage and movement of their data. The Act gives subject's the right to access and correct their personal data and differentiates between procedures for processing data classified as "sensitive" vs. not. The confidentiality guidelines zoom in on medical relationships, requiring the provider be responsible for the protection of their patient's data in both storage and communication. The section "Disclosure with consent" describes when consent is required, what the limitations are, and how to engage with the data of patient's unable to give consent. In the circumstance that a patient cannot give consent, the confidentiality guidelines require practitioners to place the patient's "care, dignity, and privacy" first.

Data access

The Personal Data Protection Act defines cases for data access under the concept "code of practice". Parties seeking access to utilize data must provide the state with a "code of practice" articulating what data the parties seek to access, security protocols for processing data

and a subjective evaluation of the parties view on ethical usage. The state has the right to issue a code of practice and ensure it aligns with best practices in data access standards. The act imposes a fine on violations of codes of practice.

Sustainability

The confidentiality guidelines offer a high-level statement of handling electronic medical records. Practitioners are to maintain audit logs detailing updates to patient medical records, back-up records in a secure location, protect the integrity of the data from cyber and physical vulnerabilities and outline steps for the data recovery. In neither document is there explicit, detailed coverage regarding the sustainability of the macro-system.

Legal framework

The Personal Data Protection Act appoints a Personal Data Protection Commissioner and Advisory Committee responsible for advocating the policy needs of data subjects, supervising compliance to the act by data users and empowered to take action as needed to enforce the act. The Act permits for the seizure of assets and arrest of violators. The Act appoints an Appeals Tribunal to handle the concerns of any subject that is "aggrieved by the decision of the Commissioner" in matters relating to the Personal Data Protection Act. All three of the above state parties have powers as defined by the act and authorized by the state. This includes power of arrest and power to prosecute.

Digital health strategy: Policy goal

Perceived as being stuck in a middle-income trap, the Malaysian government has developed a strategic plan for the health sector focused on intersectional growth for the digital sector. The country aims to develop a nationalized health data warehouse to serve as a basis for

care. Implementation is under way, and the country's goal is to construct a unified system to serve as a digital base for developing more advanced care.

Digital health strategy: Plan collaborators

The plan does not specifically dictate which parties were consulted in identifying public health objectives and articulating methods of attainment. The national health objectives specify that procedures were formulated in coordination with invested parties, but there is not a clear section outlining who those parties are and what input they had.

Digital health strategy: Initiatives

Malaysia has not identified treatment-specific goals to improve system care. It has dedicated itself to building a health data warehouse, a storage center for all data that informs general care. Development of specific initiatives is expected after a strong basis for data organization is defined and executed. At this point, a strong focus is placed on obtaining the right people and governance systems. This is abstracted out from system implementation and is an initiative to build the infrastructure to support future progress.

Discussion of analysis results

The simultaneous development of healthcare policy and health data information services demonstrates the tensions between socially constructed systems and the policy that must be generated to ensure safe improvement and usage. If people own the data they generate, then they own the ability to inform data utilization. And if policy is designed to respond to the challenges of data existing, it is interconnected with the control of data movement in an information system.

Fundamental to this relationship is the notion of transparency. People must be able to understand the policy that constructs the systems they depend upon. I would add transparency as

a fifth pillar of policy evaluation. In executing searches and policy research, the opacity of government publications quickly became apparent. For example, consent clauses contained complicated language and complex notions that may not support equitable understanding. India pushes hard on the two ideas of "data ownership" and "interoperability", but without a technical understanding of information systems or a legal understanding of those words it is difficult to fully decipher what the policy implications are. Given the stated significance of health data, nations should be pro-active in ensuring clear information publication and accessibility.

This relationship of policy and private needs and rights is further impacted by social context ethics. Any analysis of data systems has to recognize the importance of geo-political boundaries. While the core notions of data governance are abstracted out and inherent to data, policy responses must recognize the unique social complexities of a country. The size of India conveys a need to shift to digital services rapidly to provide equitable care. Rwanda is a resource-poor nation and is pushing an economic focus on improving abilities around information and communication technologies. Poland is serviced by the resources of countries surrounding it in building socio-technical systems because of its membership in the EU. Malaysia is discerning how to push out of a "middle-income trap" by building a data-structured economy.

Rwanda has focused on building data governance structures; this has created a larger quantity of policy informing system development than individual rights and is why conversations of data is centered around economic use of data. India's challenges are human-centered, as such the country has pushed to construct strong policies dictating individual's rights and the National Health Blueprint is focused on a wide array of health initiatives. Poland's lack of country-specific policy is impacted by the amount of policy generated by the EU, power has been

abstracted upwards. Notions of effective policy and health data initiatives are strongly dependent on the demographics and identity of relative countries.

Having a qualitative structure of analysis is a limiting factor. Attempting to define high-level metrics bundling policy effectiveness or comprehensiveness of legal frameworks would be nebulous. I do not have the resources or time at my disposal to collect data on patients served, data encryptions standards or the dozens of other more granular quantitative metrics that would inform this analysis. Second, this research is limited by the resources able to be deployed to identify all relevant policy measures in the specified countries. The websites of Rwanda's Ministries of Health often did not include all relevant policy and further, policy with regards to data security can be scattered across many functions of the government. For example, in Rwanda, policy pertaining to digital security have been classified under statistical practice. Third, this research is limited by the countries that could be selected. LMIC do not necessarily have the resources to translate their documentation into the English language and many LMIC have not reached a critical momentum in healthcare digitization to have significant policy. This required a close parsing out of documents generated that outlined aspirational goals for the healthcare sector and those providing concrete policy steps. Finally, there is an inherent juxtaposition between expensive data systems and classification as LMIC that challenged completing this research. Both the generation of policy and the construction of information technology systems are processes with high costs. Therefore, there is a basic restriction on the ability of LMIC to advance with pace on either and therefore constraining the need for further system development.

Iterating on the methodology used for this work, in the future I would take more time to examine financial flows. The movement of money is often representative of execution of policy

priorities, this would provide a necessary complement in thinking through both what the information system goals are of LMIC governments as well as performance in reaching those stated goals. Another subject for future work, discussed further later in this work, is the relationship between public and private sector provision of healthcare and how data is shared and moved between practitioners.

Health data generates policy because it holds value, it can be deployed to great effect in forecasting health outcomes and providing improved care but requires structured governance to ensure proper usage and empowerment of the patient. In examining the strategic plans of national health sectors, it is rapidly apparent how many stakeholders have input into its construction and the movement of the broader health landscape. This research enables me to gain a better understanding of the interdependent relationship of policy and technological development, the crux of constructing socio-technical systems. LMIC countries face the same inherent challenges of data governance as the high-income world, but are stepping into it with fewer resources and a systematically disadvantaged by a global economy built by the high-income world. My engineering practice is advanced by grappling with these questions of health equity, the privilege held by policy-makers and stakeholders with the influence to inform system construction can easily mute the voice of the populations meant to be served. This research underlines the breadth of challenges faced by global systems and the responsibility of engineers to think beyond just the local systems routinely engage with.

Conclusion

The broader significance of this work is visible in the relationship between each country's policies and the data system they shape, the connection between the politics of data and how

stakeholders wield it. Each strategic plan outlines aspirational goals for using data rightly centered around enabling better health care but the only country given marks across all four pillars is Poland, a country that benefits from membership in the EU. In a country with more sparse resources, such as Rwanda, the disconnect between policy and data systems is much more apparent. It is this friction between societal innovation for health data purposes and policy that represents a chance for improved policy. As Binagwaho and Scott (YEA) emphasize, constructing a digital health system requires collaborative efforts between public-private partners. For example, establishing a patient bill of rights should not be a reactionary step to using electronic health records. A patient bill of rights should precede deployment. Policy-makers must be at the table with the database technicians, the hospital executives, with persons of various backgrounds and experiences interacting with health care services. This enables stakeholders to approach policy and sector innovation with an accurate lens of which populations need to be served. While India did not include technical experts in developing the national health blueprint, it did include a wide array of sector stakeholders and the holistic efforts of the blueprint to push forward on human, technical, and regulatory aspects of data governance demonstrate that effort.

Further work should narrow scope to the policy side and consider how policy is generated. In this paper, it was mentioned that India is modeling its new policies after the EU and that the GDPR and HIPAA are considered standards for strong data governance. It is useful to question why and whether it is solely because the EU/US were first to develop digital health systems. Data systems are reliant on the social context of the country in which they are built, especially due to the sensitive nature of health data, and therefore so is policy. LMIC should not push towards a style of data governance that is not suitable for the needs of their stakeholders.

Resources cannot be wasted in the pursuit of foreign policies that cannot be domestically implemented, that would only increase the policy gap found in LMIC through this research. Useful policy models are impacted by geo-political ties, history and conflict with countries, regional economic conditions and ethnic ties. Health data cannot be bundled under a business data umbrella. As each of the countries analyzed in this paper step forward, intentional effort must be taken to break silos of data governance and construct human-centered policy efforts that engage the social partners driving the development of new uses of data in the health sector.

References

Gov Agency (YEAR). Act on the Protection of Personal Data, Item 1781.

Beck, E. J., Gill, W., & Lay, P. R. D. (2016). Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. *Global Health Action*, 9(1), 32089. doi: 10.3402/gha.v9.32089

Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). The Social construction of technological systems: new directions in the sociology and history of technology. Journal? Book chapter?

Binagwaho, A., & Scott, K. W. (2015). Improving the world's health through the post-2015 development agenda: perspectives from Rwanda. *International Journal of Health Policy and Management, 4*(4), 203–205. doi:10.15171/ijhpm.2015.46

Durieux, M. (2019). *Anesthesia Record. University Teaching Hospital of Kigali.*

European Commission. (2016). *General Data Protection Regulation*.

Government of India Ministry of Communications and Information Technology. (2011). *Information Technology Act Rules.*

Government of India Ministry of Health and Family Welfare. (2016). *Notification of Electronic Health Record (HER) Standards – 2016 for India.*

Government of India Ministry of Health and Family Welfare. (2017). *National Health Policy.*

Government of India Ministry of Health and Family Welfare. (2018a). *Draft of Digital Information Security in Healthcare, Act (DISHA).*

Government of India Ministry of Health and Family Welfare. (2018b). *Health Domain Metadata and Data Standards.*

Government of India Ministry of Health and Family Welfare. (2019). *Draft of Personal Data Protection Bill, 2019.*

Government of India Ministry of Health and Family Welfare. (2019). *National Digital Health Blueprint.*

Government of Malaysia Ministry of Health. (2010). *Country Health Plan.*

Government of Malaysia Ministry of Science, Technology, and Innovation. *The National Cybersecurity Policy.*

Government of Poland. (2010). *Computerization Trends for E-health Poland.*

Internet Society and the Commission of the African Union. (2018). *Personal Data Protection Guidelines for Africa.*

Kanter, A. S., Borland, R., Barasa, M., Iiams-Hauser, C., Velez, O., Kaonga, N. N., & Berg, M. (2012). The Importance of Using Open Source Technologies and Common Standards for Interoperability within eHealth: Perspectives from the Millennium Villages Project. *Advances in Health Care Management Health Information Technology in the International Context*, 189–204. doi: 10.1108/s1474-8231(2012)0000012013

Malaysian Medical Council. (2011). *Confidentiality Guidelines.*

Patil, H. K., & Seshadri, R. (2014). Big Data Security and Privacy Issues in Healthcare. 2014 IEEE International Congress on Big Data. doi: 10.1109/bigdata.congress.2014.112

Personal Data Protection Act, Act 709. (2010).

Republic of Rwanda Ministry of Health. (2015). *Health Sector Policy*.

Republic of Rwanda Ministry of Health. (2016). *Health Sector Information and Communication Technology Security Policy*.

Republic of Rwanda Ministry of Health. (2018). *Fourth Health Sector Strategic Plan*.

Republic of Rwanda Ministry of Youth and ICT. (2017). *National Data Revolution Policy.*

Rosner, G. (2014). Who owns your data? Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication - UbiComp 14 Adjunct. doi: 10.1145/2638728.2641679

Rwanda Allied Health Professions Council. (2013). *Confidentiality Guidelines.*

Sileshi, B., Newton, M. W., Kiptanui, J., Shotwell, M. S., Wanderer, J. P., Mungai, M., … McEvoy, M. D. (2017). Monitoring Anesthesia Care Delivery and Perioperative Mortality in Kenya Utilizing a Provider-driven Novel Data Collection Tool. *Anesthesiology*, 127(2), 250–271. doi:10.1097/ALN.0000000000001713

Tiffin, N., George, A., & LeFevre, A. E. (2019). How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low-income and middle-income countries. *BMJ global health*, *4*(2), e001395. doi:10.1136/bmjgh-2019-001395

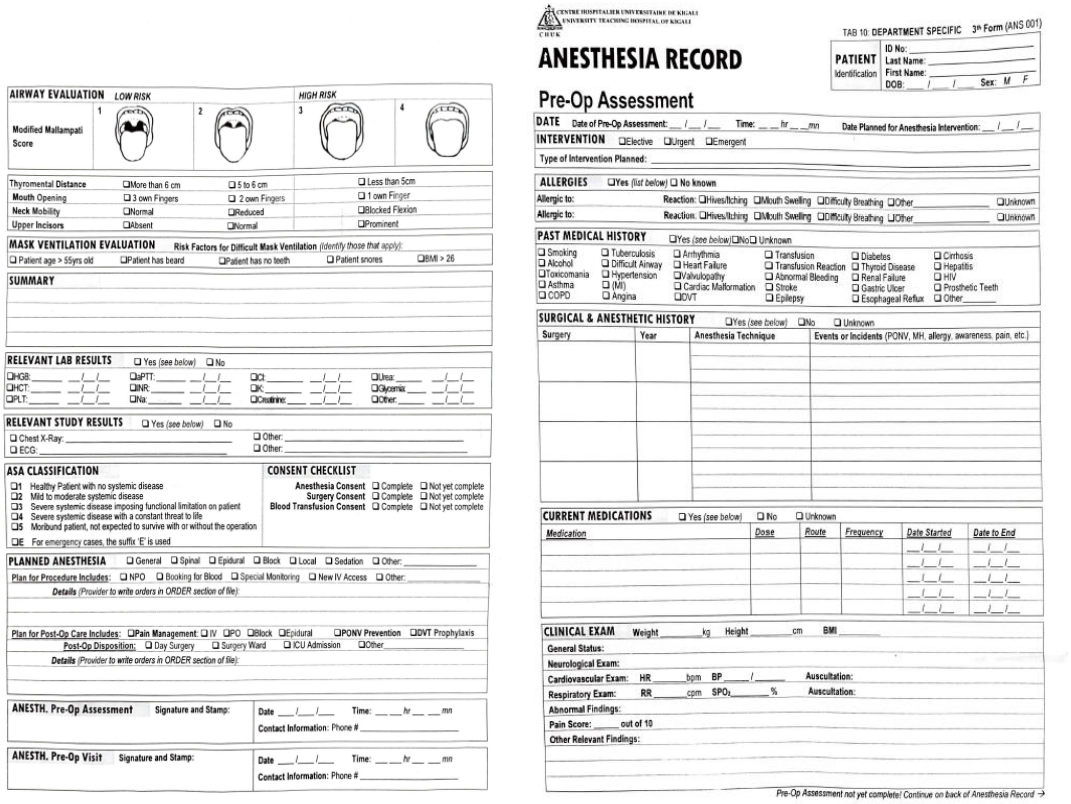
Tuti, T., Bitok, M., Paton, C., Makone, B., Malla, L., Muinga, N., … English, M. (2015). Innovating to enhance clinical data management using non-commercial and open source solutions across a multi-center network supporting inpatient pediatric care and research in Kenya. *Journal of the American Medical Informatics Association, 23*(1), 184–192. doi: 10.1093/jamia/ocv028

Verbeke, F., Karara, G., Van Bastelaere, S., & Nyssen, M. (2012). Patient Identification and Hospital Information Management Systems in Sub-Saharan Africa: A Prospective Study in Rwanda And Burundi. *Rwanda Medical Journal*, 69, 7–12. Retrieved from www.rwandamedicaljournal.org/previous-issues

Winner, L. (1980). Do Artifacts Have Politics? Daedelus, 109, 121–136.

Wyber, R., Vaillancourt, S., Perry, W., Mannava, P., Folaranmi, T., & Celi, L. A. (2015). Big data in global health: improving health in low- and middle-income countries. *Bulletin of the World Health Organization, 93*(3), 203–208. doi: 10.2471/blt.14.139022

Appendix A



CENTRE HOSPITALIER UNIVERSITAIRE DE KIGALI
UNIVERSITY TEACHING HOSPITAL OF KIGALI
CHUK

TAB 10: DEPARTMENT SPECIFIC 3th Form (ANS 001)

ANESTHESIA RECORD

PATIENT Identification: ID No: / Last Name: / First Name: / DOB: / / Sex: M F

Pre-Op Assessment

DATE Date of Pre-Op Assessment: / / Time: hr mn Date Planned for Anesthesia Intervention: / /

INTERVENTION ☐Elective ☐Urgent ☐Emergent

Type of Intervention Planned:

ALLERGIES ☐Yes (list below) ☐ No known

Allergic to: Reaction: ☐Hives/Itching ☐Mouth Swelling ☐Difficulty Breathing ☐Other ☐Unknown

Allergic to: Reaction: ☐Hives/Itching ☐Mouth Swelling ☐Difficulty Breathing ☐Other ☐Unknown

PAST MEDICAL HISTORY ☐Yes (see below) ☐No ☐ Unknown

☐ Smoking	☐ Tuberculosis	☐ Arrhythmia	☐ Transfusion	☐ Diabetes	☐ Cirrhosis
☐ Alcohol	☐ Difficult Airway	☐ Heart Failure	☐ Transfusion Reaction	☐ Thyroid Disease	☐ Hepatitis
☐ Toxicomania	☐ Hypertension	☐ Valvulopathy	☐ Abnormal Bleeding	☐ Renal Failure	☐ HIV
☐ Asthma	☐ (MI)	☐ Cardiac Malformation	☐ Stroke	☐ Gastric Ulcer	☐ Prosthetic Teeth
☐ COPD	☐ Angina	☐ DVT	☐ Epilepsy	☐ Esophageal Reflux	☐ Other

SURGICAL & ANESTHETIC HISTORY ☐Yes (see below) ☐No ☐ Unknown

Surgery	Year	Anesthesia Technique	Events or Incidents (PONV, MH, allergy, awareness, pain, etc.)

CURRENT MEDICATIONS ☐ Yes (see below) ☐ No ☐ Unknown

Medication	Dose	Route	Frequency	Date Started	Date to End
				/ /	/ /
				/ /	/ /
				/ /	/ /
				/ /	/ /
				/ /	/ /

CLINICAL EXAM Weight kg Height cm BMI

General Status:

Neurological Exam:

Cardiovascular Exam: HR bpm BP / Auscultation:

Respiratory Exam: RR cpm SpO_2 % Auscultation:

Abnormal Findings:

Pain Score: out of 10

Other Relevant Findings:

Pre-Op Assessment not yet complete/ Continue on back of Anesthesia Record →

AIRWAY EVALUATION *LOW RISK* *HIGH RISK*

Modified Mallampati Score: 1 2 3 4

Thyromental Distance	☐More than 6 cm	☐ 5 to 6 cm	☐ Less than 5cm
Mouth Opening	☐ 3 own Fingers	☐ 2 own Fingers	☐ 1 own Finger
Neck Mobility	☐Normal	☐Reduced	☐Blocked Flexion
Upper Incisors	☐Absent	☐Normal	☐Prominent

MASK VENTILATION EVALUATION Risk Factors for Difficult Mask Ventilation *(identify those that apply)*:

☐ Patient age > 55yrs old ☐Patient has beard ☐Patient has no teeth ☐ Patient snores ☐BMI > 26

SUMMARY

RELEVANT LAB RESULTS ☐ Yes (see below) ☐ No

☐HGB: / / ☐aPTT: / / ☐Cl: / / ☐Urea: / /

☐HCT: / / ☐INR: / / ☐K: / / ☐Glycemia: / /

☐PLT: / / ☐Na: / / ☐Creatinine: / / ☐Other: / /

RELEVANT STUDY RESULTS ☐ Yes (see below) ☐ No

☐ Chest X-Ray: ☐ Other:

☐ ECG: ☐ Other:

ASA CLASSIFICATION

☐1 Healthy Patient with no systemic disease
☐2 Mild to moderate systemic disease
☐3 Severe systemic disease imposing functional limitation on patient
☐4 Severe systemic disease with a constant threat to life
☐5 Moribund patient, not expected to survive with or without the operation
☐E For emergency cases, the suffix 'E' is used

CONSENT CHECKLIST

Anesthesia Consent ☐ Complete ☐ Not yet complete
Surgery Consent ☐ Complete ☐ Not yet complete
Blood Transfusion Consent ☐ Complete ☐ Not yet complete

PLANNED ANESTHESIA ☐ General ☐ Spinal ☐ Epidural ☐ Block ☐ Local ☐ Sedation ☐ Other:

Plan for Procedure Includes: ☐ NPO ☐ Booking for Blood ☐ Special Monitoring ☐ New IV Access ☐ Other:

Details (Provider to write orders in ORDER section of file):

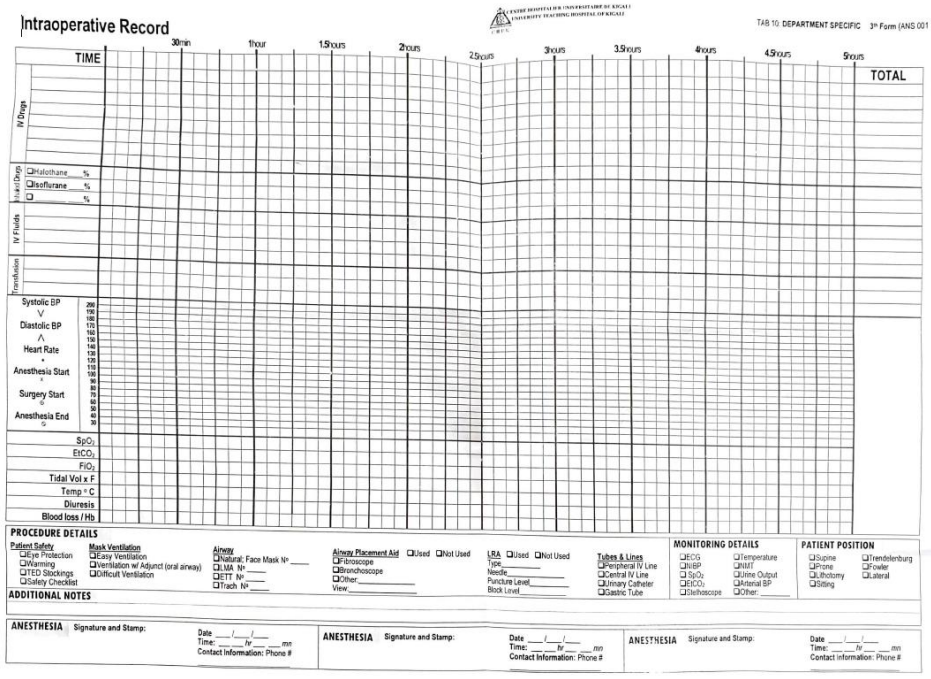
Plan for Post-Op Care Includes: ☐Pain Management: ☐ IV ☐PO ☐Block ☐Epidural ☐PONV Prevention ☐DVT Prophylaxis

Post-Op Disposition: ☐ Day Surgery ☐ Surgery Ward ☐ ICU Admission ☐Other

Details (Provider to write orders in ORDER section of file):

ANESTH. Pre-Op Assessment Signature and Stamp: Date / / Time: hr mn Contact Information: Phone #

ANESTH. Pre-Op Visit Signature and Stamp: Date / / Time: hr mn Contact Information: Phone #



CENTRE HOSPITALIER UNIVERSITAIRE DE KIGALI
UNIVERSITY TEACHING HOSPITAL OF KIGALI
CHUK

TAB 10: DEPARTMENT SPECIFIC 3th Form (ANS 001)

Intraoperative Record

30min 1hour 1.5hours 2hours 2.5hours 3hours 3.5hours 4hours 4.5hours 5hours TOTAL

TIME

IV Drugs

Inhaled Drugs: ☐Halothane %, ☐Isoflurane %, ☐ %

IV Fluids

Transfusion

Systolic BP v
Diastolic BP ^
Heart Rate •
Anesthesia Start
Surgery Start
Anesthesia End

SpO_2
$EtCO_2$
FiO_2
Tidal Vol x F
Temp ° C
Diuresis
Blood loss / Hb

PROCEDURE DETAILS

Patient Safety: ☐Eye Protection ☐Warming ☐TED Stockings ☐Safety Checklist

Mask Ventilation: ☐Easy Ventilation ☐Ventilation w/ Adjunct (oral airway) ☐Difficult Ventilation

Airway: ☐Natural: Face Mask N° ☐LMA N° ☐ETT N° ☐Trach N°

Airway Placement Aid ☐Used ☐Not Used: ☐Fibroscope ☐Bronchoscope ☐Other View

LRA ☐Used ☐Not Used: Type Needle Puncture Level Block Level

Tubes & Lines: ☐Peripheral IV Line ☐Central IV Line ☐Urinary Catheter ☐Gastric Tube

MONITORING DETAILS

☐ECG ☐Temperature ☐NIBP ☐NMT ☐SpO_2 ☐Urine Output ☐$EtCO_2$ ☐Arterial BP ☐Stethoscope ☐Other:

PATIENT POSITION

☐Supine ☐Trendelenburg ☐Prone ☐Fowler ☐Lithotomy ☐Lateral ☐Sitting

ADDITIONAL NOTES

ANESTHESIA Signature and Stamp: Date / / Time: hr mn Contact Information: Phone #

ANESTHESIA Signature and Stamp: Date / / Time: hr mn Contact Information: Phone #

ANESTHESIA Signature and Stamp: Date / / Time: hr mn Contact Information: Phone #