Biometric Technology for Fighting Fraud in National Health Insurance: Ghana's Experience

Completed Research

Emmanuel Owusu-Oware
University of Ghana
ekowusu-oware001@st.ug.edu.gh

John Effah
University of Ghana
jeffah@ug.edu.gh

Richard Boateng
University of Ghana
richboateng@ug.edu.gh

Abstract

The purpose of this study is to understand how developing countries can deploy biometric technology to fight fraud in national health insurance. Information systems research has discussed the use and impact of ICTs in fighting corruption. However, little is known about biometric technology and national health insurance fraud. To fill this knowledge gap, this paper draws on interpretive case study methodology and sociomateriality theory to investigate Ghana's experience in using biometric technology to fight national health insurance fraud. The findings show that health insurance fraud can be reduced by employing an integrated solution of social and technical systems comprising: 1) online biometric enrollment of members and verification at the point of health service delivery; 2) use of complementary technologies such as e-claims and 3) operational policies such as the use of clinicians in vetting service providers' claims.

Keywords

Health insurance, biometric, interpretive case study, e-government, Ghana, developing country, sociomateriality

Introduction

This study seeks to understand how developing countries can deploy biometric technology to fight national health insurance fraud. Biometric technology uses information and communication technologies (ICTs) to capture body images such as fingerprints and behavioral characteristics such as signature to identify and verify a person's identity (Jain, Ross, & Prabhakar, 2004). National health insurance (NHI) schemes help governments to provide equitable and affordable access to health care as well as financial protection for unexpected health expenses (Currie & Guah, 2007; Lu & Hsiao, 2003). However, NHIs face sustainability problems involving huge debts and fraud (Frankfurter & Cuervo, 2016). Health insurance fraud concerns the deliberate act of deceiving an insurance provider to pay for illegitimate health services, including services not rendered, misrepresented, already paid for or not necessary (Li, Huang, Jin, & Shi, 2008; Rawte & Anuradha, 2015).

The potential use of ICTs in fighting corruption is well acknowledged in information systems (IS) research (Ojha & Palvia, 2012). Within the health care sector, the discourse has focused more on data mining applications for detecting fraud and generally on health information systems such as electronic health records which provide information and efficiencies to reduce fraud (Dave & Dadhich, 2013; Sherer, 2014). However, little is known about biometric technology and fighting NHI fraud. Research in biometric technology has focused more on national identification (McGrath, 2016), voting (Vidyasree, Raju, & Madhavi, 2016), immigration (Whitley & Hosein, 2010), security, privacy and access control (e.g. Zorkadis & Donos, 2004) and concepts (Jain et al., 2004).

The research question for this study, therefore concerns how developing countries can deploy biometric technology to fight NHI fraud. To address this question, the study employs qualitative, interpretive case study methodology (Klein & Myers, 1999; Walsham, 1995, 2006) and sociomateriality (Orlikowski & Scott, 2008; Orlikowski, 2007) as the theoretical lens to investigate Ghana's experience in the deployment of biometric technology to fight NHI fraud.

The remaining part of the paper is as follows: The next section discusses the background literature. Thereafter, the theoretical foundation of the study is presented. The next section, then describes the research methodology followed by the case description, analysis and discussion. The conclusion section follows with the study's contribution and recommendations for future research

Health Insurance Fraud and ICTs

Health insurance fraud involves misrepresentations for unauthorized benefit (Rawte & Anuradha, 2015) either by patients, insurers or service providers (Li et al., 2008). Corruption and fraud have been recognized as a major barrier to health care (Frankfurter & Cuervo, 2016). For instance, in the USA, healthcare insurance fraud is over 30 billion dollars annually and the situation in developing countries like India is not that different (Rawte & Anuradha, 2015).

As ICTs are seen as potential means of fighting corruption (Ojha & Palvia, 2012; Srivastava & Thompson, 2006) biometric technologies, which are ICT-based human identification systems are expected to strengthen efforts in fighting fraud in various services. However, little is known about biometric technology and fighting fraud in NHI services.

The two main functions of biometric technology are: enrollment (or identification) and verification (or authentication) (Whitley & Hosein, 2010). The identification function captures biometric data, typically fingerprint images into a biometric database and ensures that individuals are not enrolled more than once in the database (Wayman, 2001; Whitley & Hosein, 2010). The verification function confirms a person's identity by comparing the live image to the stored image either in a database or on a smart card (Jain et al., 2004). A wide variation between the presented and the stored images implies the person is an impostor and access is denied while a low variation means the person is authorized and access granted to a service (Kim, 1995).

The varied applications and services offered by biometrics include: forensic applications such as criminal investigations; civilian applications such as national identification, driver's license, voter registration and immigration; commercial applications such as physical access control and credit card (Jain, Hong, & Pankanti, 2000; Jain et al., 2004). In the health care sector, the focus has been more on protecting patient health records using biometric technology (Jain et al., 2004). This study is therefore aimed at filling the knowledge gap by using Ghana's experience in deploying biometric technology to fight NHI fraud.

Theoretical Foundation: Sociomateriality

The theoretical foundation for this study is sociomateriality (Orlikowski & Scott, 2008; Orlikowski, 2007). Considered as an umbrella term for research streams that conceptualize technology, work and organizations as inseparable (Orlikowski & Scott, 2008), sociomateriality has been applied variedly and inconsistently in IS research (Jones, 2014). The fundamental concepts of sociomateriality are *social, material, practice* and *sociomateriality* (Orlikowski & Scott, 2008). Social relates to actions and interactions of human participants involved in organizational practice (Orlikowski, 2006), while material refers to physical and digital properties of artifacts through which humans act (Leonardi, 2013; Orlikowski, 2006). Practice refers to materially constituted human activity that gets work done (Orlikowski, 2002). Sociomateriality explains the relationship between the social and the material in various ways as entangled, intertwined, intermingled, interpenetrated or fused (Jones, 2014).

The principles of sociomateriality are *sociomaterial assemblage, relationality* and *performativity* (Barad, 2003; Orlikowski & Scott, 2008). Sociomaterial assemblage (assemblage for short) indicates that: 1) the social and the material are constitutively entangled in practice (Orlikowski, 2007; Orlikowski & Scott, 2008); 2) agency resides in the assemblage and not independently in either the material or the social (Wagner, Newell, & Piccoli, 2010). Relationality is the view that (Orlikowski & Scott, 2008): 1) the social and the material exist only in relation to each other through practice; 2) neither the social and the material

has inherent properties, instead their form, attributes, and capabilities emerge in practice. Performativity 1) considers reality as not just descriptive, but the enactment of the assemblages in practice (Scott & Orlikowski, 2014); 2) the performativity of the assemblage shapes the practice which in turn shapes the assemblage (Mueller & Raeth, 2012) making organizational practices emergent, dynamic and contingent (Orlikowski & Scott, 2008; Scott & Orlikowski, 2014).

We chose sociomateriality as the theory for this study because we found its concepts and principles appropriate in understanding the entanglement between social activities and the biometric technology in fighting identity and related fraud in the NHI. Sociomateriality has been found to be useful in studying IS phenomenon that involves entanglement between social entities and technological artefacts (e.g. Doolin & McLeod, 2012; Jones, 2014; Sesay, Ramirez, & Oh, 2017).

Research Setting and Methodology

Research setting

Ghana is a sub-Saharan African and a low middle-income country with a population of about 28 million. The country's NHI is administered by the National Health Insurance Authority (NHIA) with active members representing 38% of the population according to the NHIA 2013 annual report. Over the years, there has been challenges in sustaining free health services in the face of increasing membership, mounting debt as well as fraud. NHIA's 2013 annual report (NHIA - 2013 Annual Report, 2013) shows that claims payment was GH¢785.64 million (about U$364 million). Fraudulent claims by service providers have been estimated to be between 5 and 10% of claim costs (Gingong, 2015). The service providers are community-based health centers, district, regional and teaching hospitals as well as private hospitals and pharmaceutical firms.

Research methodology

The study employed qualitative interpretive case study research methodology (Myers, 2009; Walsham, 1995, 2006) to gain deeper insight about the use of biometric technology as an information system phenomena within the social context of a developing country's NHI.

Data Collection and Analysis

Data was collected within a period of 12 months from August 2016 to August 2017. In line with the chosen research methodology, data were collected from multiple sources, including interviews and documents (Walsham, 1995). Sixteen (16) interview participants were selected from the NHIA (9), health service providers (2) and members of the insurance scheme (5), based on snowball sampling (Miles & Huberman, 1984). The participants from the NHIA were: a former ICT director, deputy director for ICT infrastructure, deputy director for applications and two systems-database administrators. The remaining were deputy director of business systems (claims), a district manager, public relations and management information system officers. The interviews were semi-structured and lasted between 15 minutes and one hour. The interviews were tape-recorded with the permission of the participants along with notes-taking. The interview recordings were transcribed and verified by participants. Data were also gathered through field observation as well as documents, including annual reports, legal and operations documents from both traditional and online media sources.

Data analysis took place concurrently with the data collection in accordance with interpretive tradition and was informed using the concepts and principles of sociomateriality theory. Periodically, the researchers met to discuss and consolidate findings. Data collection and analysis continued until no further insights were found (Eisenhardt & Graebner, 2007). Guided by sociomateriality notions, the case description was written.

Case Description

Introduction

In 2003, the Ghana government established the NHI scheme by an Act of parliament (Act 650) to replace out-of-pocket payment at the point of receiving health care. The NHIA, which oversees the NHI is governed by a board with the chairperson, chief executive and one member appointed by the president of Ghana. The NHIA's functions are decentralized within the ten administrative regions of Ghana, with each region having district offices. The main funding sources for the NHI are value added tax (VAT) and workers social security contributions. Over the years, increased coverage of the NHI has not been matched by increase in revenue. The negative income, increasing debt owed health providers and fraud continued to persist as threat to the viability of the NHI. The case description describes how the introduction of biometric technology into the NHI processes to help reduce fraud evolved.

Pre-biometric technology era: 2004 – 2012

The NHI started in 2004 as district mutual health schemes (DMHS), managed independently by private companies in the districts, subsidized by the state (about 80-90% of their revenue) and supervised by the National Health Insurance Council.

Within the period of 2004-2005, 145 DMHSs emerged. Each DHMS signed agreements with service providers, created its membership database, enrolled and issued photo identification (ID) cards to members for accessing health services in the districts. However, the DMHS systems constrained access to health services and were highly prone to fraud. First, the membership databases of the DHMSs were not integrated, so members could only access health services within the district where enrolled. To access health services in another district, members needed to transfer their membership to the said district. Members circumvented this restriction by registering at other districts without the mandatory transfer so that they could access services wherever they moved to. The multiple registrations distorted regional and national reporting of NHI operations. Second, the use of plain photo IDs exposed the NHI to identity related fraud, including multiple IDs, fake IDs impersonation, provider shopping and fraudulent provider billing. With impersonation, ID cards were shared among friends and relations and this encouraged provider shopping as users moved from one provider to another with the same ailment to collect more medication than was necessary. Fraudulent billing included billing for services not provided, double billing and misrepresentations. Third, claims vetting was not effective as it was largely paper-based and lacked claims professionals. According to the deputy director of business systems (claims), the DHMSs could only make a maximum saving of 2% of claims cost.

In response to these challenges, the NHIA started a centralization project. The project was implemented within the period, 2008 to 2009. It was planned to implement biometric identification as part of the project. However, government agencies other than the national identification authority were barred by law from creating sector biometric ID cards because the goal was to have one national biometric ID card for both citizens and non-citizens. The former ICT Director narrated the challenge:

> *The NIA (i.e. National Identification Authority) law and the government's fiat prevented us from doing biometric at the time. The order from the Chief of Staff [at the office of the President] was – "nobody should go and do biometric not even Passport Office."*

The NHIA settled for magnetic strip photo ID cards for the centralization project. A technical partner who was engaged on a build-operate-maintain basis through an international competitive bidding, created the wide area network to connect the branch offices of the NHIA as well as a data center to host the central application and database servers. The NHIA was assisted by the DHMS software providers to merge the disparate databases into one centralized platform. The laminated photo ID cards of the DMHSs were replaced with magnetic strip versions through a nationwide registration exercise. Members used the magnetic strip ID cards which stored member IDs and names to access health services from accredited health facilities anywhere in the country. However, the centralized system did not reduce the identity-related fraud. In addition, the centralized printing of the cards introduced delays in the issuance of ID cards. Some of the participants described the challenges with the centralized system:

> *People wait for 3 months or more for their cards so we encountered multiple registrations resulting in huge data integrity and problems in reporting*. (Deputy Director – ICT Infrastructure)

> *People continued to dupe the system…Members could get drugs for others using their cards. …the hospitals were doing ghost bills, inflating them…* (An IT officer at a district health facility)

In 2009, following a national election and change in government, the NHIA got the opportunity to do biometric identification. Taking advantage of the stalled national biometric ID project, the NHIA made a case to the new government and were granted the permission to create biometric ID cards. Subsequently, in 2011, the NHIA introduced claims processing centers at designated regional capitals, staffed with clinicians and other claims professionals. According to the deputy director of business systems (claims), the claims processing centers could realize a cost savings of about 12% compared to the 2% cost savings by the DHMSs.

Biometric Technology Era: 2012 and Beyond

In 2012, the NHIA started implementing a biometric membership system for a more reliable identification verification system. The NHIA engaged the same technical partner used for the centralization project to upgrade the associated ICT infrastructure for higher performance, security and reliability. The upgrade included supply and installation of application and database servers for the biometric technology, VSAT and radio links for the wide area network and a new data center. The project team linked the district offices over the wide area network to the new data center to facilitate online biometric registration of applicants.

The system was rolled out in the middle of 2013 with both citizens and legal residents registering and being issued with biometric cards instantly at designated centers in the districts. Applicants completed registration forms with their personal biographical details, including name, telephone number and date of birth. NHIA registration officers then transferred such personal details into the biometric database using desktop or laptop computers that run the client biometric membership software. Applicants' biometric details which were based on each person's ten fingerprints as well as facial images were captured respectively using scanners and digital cameras attached to the client computers. Through the wide area network linking the centers and using the client software, the NHIA officers validated in real-time the scanned fingerprint biometrics against the already enrolled biometrics in the database hosted at the data center. The real-time validation of applicant's biometrics enabled the NHIA to prevent multiple registrations in the database. Following a successful data capture and validation, the registration officer printed and issued instantly a smart biometric card to each applicant using a card printer attached to the client computer. One entire registration process which was observed by one of the authors took about 10 minutes. The biometric card holds basic biographical information and biometric data and is valid for 5 years subject to yearly membership renewals.

The biometric enrollment was not without implementation challenges. Inadequate registration equipment and poor network connectivity in some districts slowed the process as hundreds of people thronged the registration centers eager to acquire the highly publicized and new NHI biometric cards. There were change management challenges in the acceptance and assimilation of the new system:

> *All these were new to our people. We had to go through a lot of training…technical training on-site and off-site…including the hospitals* (Former Director IT)

> *The providers did not embrace the system initially…they thought it will be cumbersome and delay their services. So we organized stakeholder meetings involving the ministry of health, Ghana health service, health providers as well as our heads of departments. We demonstrated the system.. (*An IT officer at a district office).

At selected health facilities, the NHIA deployed portable biometric kits for the verification of members' identities before receiving service. A biometric kit comprises a computer tablet running the client biometric software, a card reader and a fingerprint scanner. A member attending a health facility will be verified by inserting his or her biometric card into the card reader and then placing the ten fingerprints successively on the scanner. The stored fingerprint images of the member on the card was compared with his or her live fingerprints automatically using the biometric kit. A successful match caused to be displayed on the kit's

screen, the personal details of the member, which include the member ID number, name, date of birth as well as the portrait. Also displayed was a unique 13-digit *claim check code* was generated as evidence of a member's attendance at the health facility. Where there is no match, or the fingerprints of a patient could not be used due for instance to an accident, the patient is referred to the NHIA office. Later (normally within 14 days), the claim check codes on the biometric kits were uploaded by the NHIA officer to the database through a GSM/3G mobile network. Subsequently, claims submitted by the service provider were validated by the NHIA claim officers against the claim check codes in the database before payments were authorized.

According to the deputy director of business systems for claims, about 1,300 out of a target total of 4,000 biometric kits were deployed at the health facilities. He indicated that supply of the kits and their maintenance were at a great cost to the NHIA and therefore had to be deployed on a selective basis:

> *It was not practical to have nationwide deployment of these kits. The providers saw it as rather limiting them, so no incentive for them to share in the cost. So, we had to fund and deploy the kits on selective basis, informed by claim volumes, patterns, and audit findings.*

In 2013, the NHIA introduced an electronic claims system (e-claims) to speed up claims processing and to compliment the biometric system which could not deal with false claims such as inflated bills. Like the biometric system, they were implemented at selected health facilities. An e-claim shows a list of members, bill amounts, ailments treated, the treatment as well as the claim check codes. A health facility submitted e-claims through the network to the head office. The NHIA officers will validate the e-claims on the backend e-claim system at the head office. According to the deputy director of business systems (claims), data analytics were generated by the e-claims system showing claims patterns such as claim volumes of health facilities. Above-average claims volumes were vetted by the NHIA clinicians who assessed the nature and cost of the treatment for the reported health problem. Where the submitted claims are not electronic but paper-based, a claims summary sheet was prepared electronically. A capitation policy which stipulates that a member cannot make more than one claim within 2 weeks was also introduced. A former director of ICT and the deputy director of business systems (claims) commented on the outcome of the biometric-based system in managing the NHI.

> *We are not 100% there yet, but so far it has helped in reducing fraud, remove the duplicates… ID cards are now instantly issued, and it is giving us a credible database* (former director of ICT).

> *Psychologically, it [the biometric system] is a deterrent …now it is a lot more difficult to pick a member details and generate claims… our claims volumes have reduced by approx. 15-16%. We would have maximum yield if we had the authentication across board.* (deputy director of business systems for claims)

Analysis

In this section, the theoretical concepts and principles of sociomateriality are used to analyze the case findings. The concepts are *practice, social, material* and *sociomateriality,* while the principles, are *sociomaterial assemblage, relationality* and *performativity*. Table 1 and Table 2 summarize the analysis.

As shown in both tables three sociomaterial assemblages were identified based on the NHI practices of *member identification*, *member verification* and *claims processing*. During the pre-biometric period the assemblages were constituted materially, mainly by photo-ID based systems. In the biometric era they were reconfigured with biometric technology. In both tables, *relationality* is depicted as the emergent boundaries of the social and the material entities and the intra-actions within and across the assemblages. The arc arrows show the intra-actions within an assemblage while the straight-line arrows depict the intra-actions across the assemblages. The *performativity* (i.e. the enactment) of the assemblages during the pre-biometric era resulted in multiple registrations, fake IDs, impersonation, ghost patients and consequently fraudulent billing. These outcomes were largely due to the weakness in using facial verification of patients and the lack of identifying members uniquely. In responding to the deficiencies with the pre-biometric systems, the assemblages were reconfigured with biometric technology.

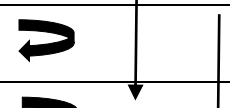
Sociomaterial Assemblage		**Relationality**	**Performativity**
NHI Practices/ Social	**Material / Technology**		
Member Identification	Photo-ID / magnetic strip technology		Multiple registration, Fake ID cards
Member Verification	Photo-ID / magnetic strip technology		Impersonation
Claims Processing	Member ID number		Ghost patients Fraudulent billing

Table 1 Pre-Biometric Era

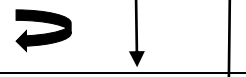
Sociomaterial Assemblage		**Relationality**	**Performativity**
NHI Practices (Social)	**Material / Technology**		
Member Identification	Biometric technology		Unique registration ID
Member Verification	Biometric technology		Claim check codes
Claims Processing	Biometric technology generated claim check codes		Billing based on claim check codes

Table 2 Biometric Era

In particular, the use of unique identifiers based on fingerprint biometrics of members and claim check codes as evidence of members visits to health facilities helped the NHIA to fight identity related fraud and therefore reduce fraudulent claims from service providers.

Discussion

This section discusses the findings in relation to the research question on how developing countries can deploy biometric technology to fight fraud in NHI. The findings are summarized in Table 3 below. Multiple identities create opportunities for fraudsters (Rejman-Greene, 2005). The findings show that the use of online biometric enrollment of members can eliminate multiple identities while the use of biometric verification at point of service delivery curtails opportunities for fraudulent insurance claims. The unique health facility attendance code that was generated through the biometric verification kit is akin to audit trails in information systems security where changes in a database made by users are logged and used as evidence for systems or forensic audit. The study shows how reconciliation of provider's claims with these evidential attendance codes help to filter out claims associated with ghost patients. This is an innovative use of biometrics that has not been discussed in the IS literature.

The study findings also show that a successful implementation of biometric technology requires high investment in ICT infrastructure comprising front-end systems such as biometric registration and verification computers, and backend systems such as database and server systems as well as the data center. The high cost and challenges with implementing such infrastructure for biometric identification systems have been discussed in literature (e.g. Beynon-Davies, 2007; Whitley & Hosein, 2010) and suggestions have been made in addressing them. For instance, Basu (2004) suggests the use of public private partnership arrangement to build ICT infrastructure while Pentland, Fletcher, & Hasson (2004) recommend using existing and low cost mobile wireless infrastructure.

NHI Forms of Fraud During Pre-Biometric Era	Effects of Biometric Technology in Fighting NHI Fraud
Multiple Identities	Biometric enrollment helped to eliminate multiple registration of NHI members
Fake IDs	Biometric verification helped to eliminate fake IDs at point of service
Impersonation	Biometric verification helped to eliminate impersonation at point of service
Ghost Patients	Biometric verification helped to eliminate the use of ghost patients in making claims
Fraudulent Billing	Biometric technology helped to reduce fraudulent billing

Table 3 Key Research Findings

In this study, through a public private partnership-built ICT infrastructure, the NHIA was able to enroll subscribers online and issue biometric cards instantly, while an existing mobile network of a telecoms provider was used to connect the biometric authentication devices at selected health facilities at a relatively lower cost compared to a dedicated WAN. Also, the study's findings show that there are technical and non-technical ways of addressing the high cost of ICT infrastructure that tend to hinder ICT developments in developing countries. When confronted with the high cost of deploying biometric kits to all designated health facilities the NHIA adopted the policy of selective implementation by targeting health facilities where the claims volumes were high and post audit patterns flagged potential fraudulent claims.

Finally, drawing on the sociomateriality perspective, the study shows that the deployment and use of biometric technology for identity-controlled requires an integrated social and technical systems. In this study the social systems entailed NHI practices of identification, verification, claims processing and supporting policies such as capitation and selective deployment of biometric kits based on claims volumes. With the technical systems they involved not only the biometric technology but other technologies such as e-claims. For instance, with the detection of inflated claims, the biometric technology was limited and had to be complimented with e-claims as well as claims vetting professionals. This finding is consistent with the observation that ICTs alone cannot fight fraud, but it takes organizational arrangements as well (Srivastava & Thompson, 2006) to fight corruption related phenomena.

Conclusion

This study sought to understand how developing countries can deploy biometric technology to fight fraud in NHI. The findings show that the use of biometric technology can fight fraud in NHI by helping 1) to eliminate multiple identities and fake IDs through online biometric enrollment of members; 2) eliminate impersonation and ghost patients through biometric verification at the point of service delivery; 3) to reduce fraudulent provider bills. The findings also show that deploying biometric technology to fight NHI fraud requires an integrated social and technical systems; social systems such as the use of clinicians to detect inflated provider bills and technical systems such as e-claims system that complement the biometric technology.

The paper contributes to research, practice and policy. For research, this study contributes to the limited literature on biometric and NHI fraud by giving rich insight into how biometric technology can be deployed to fight NHI fraud. The study also demonstrates the use of sociomateriality lens in unpacking the social and technological dynamics involved in deploying biometric technology for NHI. For practice and policy, the study shows that with appropriate operational policies, biometric technology can be deployed effectively to reduce fraud.

The study findings are limited by the single nation experience. However, in line with interpretive studies, the findings can be applied to developing countries with similar context. Future studies can explore how biometric technology can be used to fight fraud in other areas such as public-sector payroll.

REFERENCES

Barad, K. (2003). Posthumanist Performativity: Toward an Understanding of How Matter Comes to Matter. *Signs: Journal of Women in Culture and Society*, *28*(3), 801–831.

Basu, S. (2004). E-Government and Developing Countries : An Overview. *International Review of Law, Computers & Technology*, *18*(1), 109–132.

Beynon-Davies, P. (2007). Personal identity management and electronic government: The case of the national identity card in the UK. *Journal of Enterprise Information Management*, *20*(3), 244–270.

Currie, W. L., & Guah, M. W. (2007). Conflicting institutional logics: A national programme for IT in the organisational field of healthcare. *Journal of Information Technology*, *22*(3), 235–247.

Dave, M., & Dadhich, P. (2013). Applications of Data Mining Techniques : Empowering Quality Healthcare Services. *International Journal of Information, Communication and Computing Technology*, *1*(1), 13–16.

Doolin, B., & McLeod, L. (2012). Sociomateriality and boundary objects in information systems development. *European Journal of Information Systems*, *21*(5), 570–586.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases : Opportunities and Challenges. *Academy of Management Journal*, *50*(1), 25–32.

Frankfurter, C., & Cuervo, L. G. (2016). E-Government as tool to advance health. *Global Journal of Medicine and Public Health*, *5*(6), 4–7.

Gingong, A. (2015). The Silo is Empty The Case of NHIS. Retrieved February 24, 2017, from http://www.nhis.gov.gh/publications.aspx

Jain, A. K., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, *43*(2), 90–98.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20.

Jones, M. (2014). A Matter of Life and Death: Exploring Conceptualizations of Sociomateriality in the Context of Critical Care. *MIS Quarterly*, *38*(3).

Kim, H. J. (1995). Biometrics, is it a viable proposition for identity authentication and access control? *Computers & Security*, *14*(3), 205–214.

Klein, H. K., & Myers, M. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67–94.

Leonardi, P. M. (2013). Theoretical foundations for the study of sociomateriality. *Information and Organization*, *23*(2), 59–76.

Li, J., Huang, K. Y., Jin, J., & Shi, J. (2008). A survey on statistical methods for health care fraud detection. *Health Care Management Science*, *11*(3), 275–287.

Lu, J. R., & Hsiao, W. C. (2003). Insurance Make Health Care. *Health Affairs*, *22*(3), 77–88.

McGrath, K. (2016). Identity Verification and Societal Challenges: Explaining the Gap between Service Provision and Development Outcomes. *MIS Quarterly*, *40*(2), 485–500.

Miles, M. B., & Huberman, A. M. (1984). *Qualitative Data Analysis: A Sourcebook of New Methods*. *Sage publications* (Vol. 19).

Mueller, B., & Raeth, P. (2012). What You See Is What You Get: a Comparison of Theoretical Lenses To Study Technology Organizations. In *ICIS* (pp. 1–20).

Myers, M. (2009). *Qualitative research in business and management*. Sage.

NHIA - 2013 Annual Report. (2013). *2013 NHIA Annual Report*.

Ojha, A., & Palvia, S. (2012). E-Government and The Fight Against Corruption : Conceptual Model and Five

Case Studies From India. *Journal of Information Technology Case and Application Research*, *14*(4), 11–30.

Orlikowski, W. (2002). Knowing in Practice: Enacting a Collective Capability in Distributed Organizing. *Organization Science*, *13*(3), 249–273.

Orlikowski, W. (2006). Material Knowing: The Scaffolding of Human Knowledgeability. *European Journal of Information Systems, 15*(5), 460–466.

Orlikowski, W. (2007). Sociomaterial Practices: Exploring Technology at Work. *Organization Studies*, *28*(9), 1435–1448.

Orlikowski, W., & Scott, S. (2008). Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, *2*(1), 433–474.

Pentland, A., Fletcher, R., & Hasson, A. (2004). Rethinking connectivity in developing nations. *Computer*, *37*(1), 78–83.

Rawte, V., & Anuradha, G. (2015). Fraud detection in health insurance using data mining techniques. In *International Conference on Communication, Information & Computing Technology (ICCICT)* (pp. 1–5).

Rejman-Greene, M. (2005). Privacy issues in the application of biometrics: a european perspective. In *Biometric systems* (pp. 335–359). Springer, London.

Scott, S., & Orlikowski, W. (2014). Entanglements in practice: performing anonymity through social media. *Mis Quarterly*, *38*(3), 873–893.

Sesay, A., Ramirez, R., & Oh, O.-O. (2017). Digital Transformation in Police Work: A Sociomaterial Perspective on Police Body Worn Cameras (BWC). In *Hawaii International Conference on System Sciences* (pp. 4266–4275).

Sherer, S. A. (2014). Advocating for Action Design Research on IT Value Creation in Healthcare. *Journal of the Association for Information Systems*, *15*(12), 860–878.

Srivastava, S. C., & Thompson, S. H. T. (2006). Facilitators for e-Government Development: An Application of the Technology-Organization- Environment Framework. *12th Americas Conference on Information Systems (AMCIS 2006)*. Acapulco, Mexico: AIS.

Vidyasree, P., Raju, S. V., & Madhavi, G. (2016). Desisting the Fraud in India's Voting Process through Multi Modalbiometrics. In *Advanced Computing (IACC), 2016 IEEE 6th International Conference on* (pp. 488–491). IEEE.

Wagner, E., Newell, S., & Piccoli, G. (2010). Understanding Project Survival in an ES Environment : A Sociomaterial Practice Perspective. *Journal of the Association for Information Systems*, *11*(5), 276–297.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, *4*(2), 74–81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330.

Wayman, J. (2001). Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics*.

Whitley, E., & Hosein, G. (2010). Global Identity Policies and Technology: Do we Understand the Question? *Global Policy*, *1*(2), 209–215.

Zorkadis, V., & Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective. *Information Management & Computer Security*, *12*(1), 125–137.