THE NEED FOR SPECIFIC LEGAL FRAMEWORK FOR MEDICAL IDENTITY THEFT IN NIGERIA

Dike C. Obalum*, Uwakwe Abugu, Maureen Maxine Stanley-Idum*****

Abstract

Medical identity theft (MIT) is a sensitive subject that concerns patients, potential patients, health insurance companies, health care providers, the general populace and governments. The concern has been heightened by the growing emphasis on privacy and security of electronic health information and the need to develop measures to protect them. Identity is a set of behavioural or personal characteristics by which an individual is recognized. It is also a collection of defining attributes that differentiates one individual from another. Traditionally, identity is used in relation to a person's name. Now, however, the scope of this term has been broadened to include bank, credit card and social security numbers. With the advances in technology, identity may now also cover personal identification number (PIN), computer usernames, passwords, email addresses, fingerprints, iris and deoxyribonucleic acid (DNA). Theft is the act or crime of stealing. Identity theft is the fraudulent appropriation and use of someone's identifying or personal data or documents. It is the unlawful use of someone else's personal identifying information in order to get money or credit or benefit. Identity connotes an individual's name. The overall aim of this work is to elucidate on the subject matter, stimulate the needed integrated legal and institutional measures to address the life important issue of medical identity theft and to generate future research in this obscure but dangerous emerging trend, especially in developing countries. Doctrinal method was utilised for this research. The findings basically covered issues relating to identity theft in general and medical identity theft in particular. It provided an understanding of

* LL.B, LL.M, B.L. MCIArb, Doctoral Candidate, University of Abuja. Corresponding Author, obalum@yahoo.com

** LL.B, LL.M. B.L, PhD, Professor of Law, Faculty of Law, University of Abuja, Abuja, Nigeria.

*** LL.B, LL.M, B.L. Deputy Director General, Nigerian Law School, Enugu Campus.

what medical identity theft entails and how these acts are recognised as criminal, and the far reaching implications. It also articulated the consequences, challenges, as well as why medical identity theft can be described as the "unarmed mass killer". There are laws on all kinds of identity theft in Nigeria that cover medical identity theft. Specifically, the study showed the absence of a specific legal framework on the subject. Consequently, it recommended the need for such a specific law and more research on medical identity theft.

1.1.1 Introduction

Medical identity theft (MIT) is an emerging issue that raises concerns for consumers, health care providers, health plans and governments[1]. The concern has been heightened by the growing emphasis on privacy and security of electronic health information and the need to develop measures to protect them[2]. Identity theft is fast becoming a crime to reckon with globally. According to Hornsby, it connotes using somebody else's name or personal information in order to obtain credit cards and other goods or to take money out of the person's bank accounts[3]. In Nigeria, several cases of identity theft have been reported. Different forms of identity theft exist one of which is Medical Identity Theft.

The term 'medical' means connected with illness and injury and their treatment[4]. Identity denotes who or what somebody or something is or characteristics, feelings or beliefs that distinguish people from others[5] while 'theft' defines the crime of stealing something from a person or place[6]. Oxford English Dictionary defines identity as "the set of behavioural or personal

[1]Mancilla, D and Moczygemba J. 'Exploring Medical Identity Theft' (2009) vol. 6, issue 1, Perspectives in Health Information Management, <https://www.ncbi.nlm.nih.gov/pmc/articles/pmc2804460/> Retrieved 11 January 2019

[2]Booz AH. 'Medical Identity Theft Final Report',US Department of Health and Human Services, Office of the National Coordinator of Health Information Technology US<https://www.healthit.gov/sites/default/files/medidtheftreport011509_0.pdf&ved=0ahUKEwjxpsTr-M_YAhXGZVAKHZapDsgQFggjMAA&usg=AOvVawOoHVZulFFwvtLjJIW-jLm9>. Retrieved January 15 2019.

[3] Hornby AS(2005); *Oxford Advanced Learner's Dictionary of Current English*, 7th ed, Oxford University Press. London

[4] *Ibid.*

[5] *Ibid.*

[6] *Ibid.*

characteristics by which an individual is recognised"[7]. It is a collection of defining attributes that differentiates one individual from another[8]. It also defined theft as, "the action or crime of stealing"[9]. Ordinarily, identity connotes an individual's name. In the 21st century, the meaning of identity has widened in scope to include bank card and social security numbers; Personal Identification Numbers (PIN), passwords, Deoxyribo Nucleic Acid (DNA) profile, fingerprints and iris scan pattern.

The UK Home Office Report on Identity Fraud highlights three categories of identity[10]. The first is attributed identity which includes those attributes assigned to an individual usually upon birth, such as names, date, and place of birth. Secondly, there is biometric identity, which are attributes peculiar to an individual, such as DNA profile, fingerprint and iris pattern. Third, is biographical identity, which refers to those attributes that an individual has accumulated in his life time, including academic and professional credentials, work history, among others[11]? Hence some identity characteristics are acquired at birth, while some are issued by government or other bodies[12]. Identity theft will normally involve attributed identity and biographical identity[13].

The objective of this work is to illuminate on medical identity theft, to stimulate more research on it, generate needed integrated legal and institutional measures to address it. From our search and research, this is the first academic work on medical identity theft in Nigeria.

1.1.2 Meaning of Medical Identity Theft

The United States Identity Theft and Assumption Deterrence Act of 1998 defined identity theft as an action by someone who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a

[7] Simpson J and Weiner E,(eds)(1989). *Oxford English Dictionary*, 2nd ed, Oxford UniversityPress, London. P 441

[8] Manap NA. (2015) 'Cyberspace Identity theft'. *Mediterranean Journal of Social Sciences*, 4 (6), p. 595-605

[9] Simpson J and Weiner E. *Op cit* at footnote 7.

[10] Koops B. (2009) 'A typology of identity related crime'. 12(1) Information, Communication & society, 12 (1), p.3

[11] Britz M.*Computer Forensics and Cybercrime.*(2nd edn, OECD Publication Paris 2007) 119.

[12] *Ibid.*

[13] Manap NA. *Op cit* at footnote 8.

violation of the Federal law, or that constitutes a felony under any applicable State or local law[14].

The term identity theft is thus the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name[15] and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences if he is held responsible for the perpetrator's actions.

Identity fraud is often but not necessarily the consequence of identity theft. Someone can steal or misappropriate personal information without committing identity theft, such as when a major data breach occurs. A US government accountability office study determined that "most breaches have not resulted in detected incidents of identity theft"[16]. The report also warned that "the full extent is unknown". A later unpublished study by Carnegie Mellon University noted that "most often, the causes of identity theft is not known," but reported that someone else concluded that "the probability of becoming a victim to identity theft as a result of a data breach is ... around only 2%"[17]. More recently, an association of consumer data companies noted that one of the largest data breaches ever, accounting for over four million records, resulted in only about 1,800 instances of identity theft, according to the company whose systems were breached[18].

Medical identity theft is defined as the appropriation or misuse of a patient's or a provider's unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or service[19]. This means the stealing of an identity and utilisation of same for any form of gain. By this definition, a provider may be an institution or an individual medical professional. Accordingly, medical identity theft occurs when someone uses another person's identifying information, such as health insurance information or social security

[14]'Identity Theft and Assumption Deterrence Act Sec. 003(d)'from <http://www.ftc.gov/os/statutes/itada/itadact.html> Retrieved September 5, 2018.

[15]Hoofnagle CJ.(2007)'Identity Theft: Making the Known Unknowns Known' *Harvard Journal of Law and Technology*, 21, p.46.

[16] 'Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown', Highlights of GAO-07-737, a report to congressional requesters, from gao.gov. Retrieved September 5, 2018.

[17]Romanosky S.'Do Data Breach Disclosure Laws Reduce Identity Theft?' Heinz First Research Paper, from <heinz.cmu.edu>. Retrieved September 5, 2018.

[18]*Ibid.*

[19]Agrawal S, Budetti P.(2012) 'Physician Medical Identity Theft' *The Journal of the American Medical Association*, 307 (5), p. 459-460.

number, without the owner's knowledge or permission, for the purpose of obtaining medical services or goods. Money may also be obtained by falsifying claims for medical services as well as medical records to support such claims.

Dixon is of the view that Medical identity theft is a practice in which someone uses another individual's identifying information, such as health insurance or social security number, without the individual's knowledge or permission, to obtain medical services or goods, or to obtain money by falsifying claims for medical services and falsifying medical records to support those claims[20]. Medical identity theft can also occur when an individual willfully shares his or her medical identifying credentials with another person with the aim of helping the person acquire medical care.

1.2 Methods of Medical Identity Theft

The common ways of committing medical identity theft include:[21] using someone else's insurance card to receive medical services; use of a person's stolen identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims; opening credit cards in a victim's name with the perpetrator running up large hospital bills that can go to collections; stealing a doctor's name and medical license number to forge their signature and falsify patient records and prescriptions.

In a study on Medical Identity theft conducted in US by Ponemon Institute[22], 24% of the respondents opined that medical identity theft was accomplished when a family member took personal identification or medical credentials without their consent; 23% of the respondents revealed that they shared their personal identification or medical credentials with someone they know; 15% of the respondents indicated that they did not know how the fraud materialized, while 12% of them admitted that they mistakenly gave their personal information to a fake email or spoofed websites even as 10% of the sampled population responded that their healthcare providers or insurers had data

[20] Dixon P. Medical identity theft: The information crime that can kill you. World Privacy Forum Web site. Available at: <http://www. worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you>. Retrieved October 24 2018.

[21] http://www.protectmyid.com (Accessed 3 October 2018).

[22] Fifth Annual Study on Medical Identity Theft, Ponemon Institute, February 2015. From <ponemoninstitute.gov>. Retrieved October 24, 2018)

breaches; 6% of them posited that healthcare providers' employees stole their health information, while 5% of them fell victims when they lost their wallet with personal identification and/or medical credentials. The identity thief took a medical statement/invoice mailed to the address of 3% of the respondents, while in the case of 2% of the respondents; the thieves intercepted an email with their medical information/credentials to enlist them as part of the statistics of medical identity fraud victims.

In the cases of victim-facilitated medical identity theft as reported by the study under reference, the circumstances wherein the rightful beneficiaries of health insurance let a family member or someone they know use their credentials to obtain medical services were because the person did not have insurance (91%), could not afford to pay for treatments (86%) or it was an emergency (65%). In Nigeria, there is no data on medical identity theft including how it is accomplished.

Medical identity theft is mostly perpetrated through the cyberspace arising from the creation and advancement of technology. Cyberspace is a term used in computer science, which signifies, the connections between computers in different places, considered as a real place where information exist. There people can communicate with one another. Like physical space, cyberspace contains objects such as files, mails, messages, graphics, etc. It may be referred to as the total inter connectedness of human beings.[23] In the same respect, Graham Todd more specifically refers to cyberspace as, "an evolving man-made domain".[24] William Gibson who coined the term 'cyberspace' described it as, "a graphic representation of data abstracted from banks of every computer in the human system".[25] A notable characteristic of cyberspace is that people do not have to move physically from one point to another within it in order to perform their activities. They simply click a mouse or punch a key on a computer keyboard. Cavoukian defines cyberspace as "the electronic airways and information residing in electronic or digital form, capable of being transmitted online via networked communications".[26]

Legally speaking, cyberspace, and real space are not the same.[27] Indeed, attributing the rules of real space to cyberspace may lead to legal conflicts.[28] This

[23]Schaap A, (2009)"Cyber Warfare Operations: Development and Use Under International Law" *The Air Force Law Review*, 64 p.121-173.

[24]Todd G, (2009) "Armed attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition" The Air Force Law Review from <http://lexisnexis.com>. Retrieved September 17, 2018.

[25]Gibson W, (1984) *Neuromancer*, Ace Books Publication, New York.

[26]Cavoukian A, (1997) *Who Knows: Safeguarding your Privacy in a Networked World*, McGraw Hill Publication, New York. P. 51.

[27]Cohen J, (2007) 'Cyberspace as Land space' Columbia Law Review, from <http://www.lexisnexis.com>. Retrieved September 17, 2018)

is because offences committed in cyberspace vary from those carried out in the real world; the former are committed at an alarming rate, and their repercussions, unlike those of the real world, are comparable to weapons of mass destruction[29].

From the foregoing, it is evident that the crime of medical identity theft is perpetrated through various forms and also some subscribers to Health Insurance schemes can inadvertently incur the deleterious consequences of medical identity theft in a bid to showing benevolence to family members or the people they know. An appreciation of the techniques used in the commission of identity theft in cyberspace is vital to our understanding of the crime, and possible modes of prevention. This makes it pertinent to examine some of the more common of those techniques.

1.3 Damaging Effect of Medical Identity Theft

It is clear that medical identity theft is a form of identity theft that occurs when someone steals personal information and/or documents (like your name or health insurance number, credit card, etc.) to obtain medical care, buy drugs, submit fake bills and for impersonation purposes. Medical identity theft and fraud constitutes a major societal problem exerting pressure on our healthcare and financial ecosystems. Medical identity theft can disrupt people's lives, lead to wrongful suspicion and even arrest of victims, damage credit rating, and waste taxpayer monies. The damage can even be life-threatening to any individual if the wrong information ends up in personal medical records or where the impersonation of medical personnel proceed to give wrong diagnosis and treatments to victims.

The severity of the problem is aptly captured in this passage:

> Health insurance needs and general financial opportunity has created an emerging market in medical identity theft. Medical offices have the perfect storm of information collection, personal, credit, banking, health, and insurance. Thieves have realized that medical facilities have as much economic value as banks and the security is much easier to crack. Mostly committed by insiders, medical identity theft is a well-hidden information

[28]Folsom T. (2007) 'Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality)' *Tulane Journal of Technology and Intellectual Property*, vol.75 no.9 from <http://www.lexisnexis.com> (Retrieved September 5, 2018).
[29]*Ibid.*

crime. In spite of its covert nature, the catastrophic ramification to the victims is overt[30].

Medical identity theft is not just a financial crime; it can kill[31]. The crime can have long-lasting and dangerous effects, both on health and finances. The thief may obtain health services in the victim's name or billed fraudulently for services that, although never received could maximise out the victim's annual or lifetime insurance limits. Whether the thief is actually receiving medical treatment or just billing for fictitious treatments in the victim's name, incorrect information—about blood type, diagnoses, or drug allergies, for instance—may infiltrate the victim's medical records as a result. Unpaid bills listing the victim as the patient may be sent to debt collection agencies and reported under the social security number to credit bureaus, affecting the victim's credit history[32].

Healthcare providers and payers are usually the secondary victims of medical identity theft. Providers will likely write off all healthcare expenses incurred as a result of treating fraudulent individuals[33]. It follows that medical identity theft can cause avoidable loss of lives and resources due to management of non-existent medical conditions introduced into a patient's record by the identity theft, great financial losses to the victim and may also have legal implications. Also, the government and health providers suffer huge losses alongside the society. Bonafide persons may be unduly deprived of medical care following the activities of medical identity thieves.

Medical Identity Theft represents a huge form of fraud perpetrated in diverse forms with dire consequences both to the patient, government, Health Insurance service providers and the society. Despite extant laws prohibiting this heinous crime and efforts aimed at preventing its rise, it continues to pose a challenge. In the United States of America, according to the Federal Trade Commission (FTC), medical identity theft accounted for 3% of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities stolen in 2005[34].

[30]Figg W, Kam HJ. (2011) 'Medical Information Security' *International Journal of Security*, 5 (1) p. 22-34.
[31]Joshua C, DeCorato C, Federico S; (2015) Medical Identity Theft –The Crime That Can Kill, Dateline, 14(2) p.1.
[32]Kimberlee R, (2012) "Stop Thief: How to protect yourself against medical identity theft. Neurology Now, 8 (5), p.32-33
[33]Apgar C, (2008) Mitigating Medical Identity Theft. J AHIMA. Vol. 79 no7, p. 63–69.

[34]Federal Trade Commission.FTC – 2006 Identity Theft Survey Report.Federal Trade Commission Web site. Available at: <http:// www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-

1.4 The Crime of Medical Identity Theft and the Relevant Legal Framework

According to the US Identity Theft and Assumption Deterrence Act of 1998[35] which became effective October 30, 1998, identity theft is a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000. It establishes that the person whose identity was stolen is a true victim. Previously, only the credit grantors who suffered monetary losses were considered victims. This legislation enables the Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies to combat this crime. It allows for the identity theft victim to seek restitution if there is a conviction. It also establishes the Federal Trade Commission as a central agency to act as a clearinghouse for complaints, (against credit reporting agencies and credit grantors) referrals, and resources for assistance for victims of identity theft[36].

In the United States, the Federal government in conjunction with State governments provides health care coverage for 100 million people through Medicare, Medicaid and the Children's Health Insurance Program, which is equivalent to about one out of every four individuals and amounts to expenditures of more than $732 billion in tax payer dollars per year[37]. The Federal Trade Commission (FTC) and the Centres for Medicare and Medicaid Services (CMS) track cases of provider and patient medical identity theft. The latest FTC data shows that more than 3,600 physician and patient cases of medical identity theft were reported in 2009, with more than 12,000 cases reported between 2007 and 2009[38]. It is likely that substantial medical identity theft is unreported[39]. FTC data also show that 32% of thefts are discovered more than one year after they occurred[40]. "Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained"[41], and identity theft is not always detectable

identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf>. Retrieved October 25, 2018.

[35]Identity Theft and Assumption Deterrence Act 1998 s 1028: Fraud and Related Activity in Connection with Identification Documents and Information.

[36] *Ibid*

[37]Centre on Budget and Policy Priorities.'Policy Basics: Where Do Our Federal Tax Dollars Go?' from <http://www.cbpp.org/cms/?fa=view&id>.(Retrieved September 5, 2018).

[38]Federal Trade Commission,'Consumer Sentinel Network Data Book for January-December 2009' (2010) from <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf> (Retrieved September 5, 2018).

[39]Federal Trade Commission.'Identity Theft Survey Report' (2006) from <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf> (Retrieved September 5, 2018).

[40]*Ibid.*

[41]*Ibid.*

by the individual victims, according to a report done for the FTC[42].

An estimated 1.4 million Americans were victims of medical identity theft in 2009[43]. While this number is only 5% of all reported identity theft incidents, medical identity theft is expected to increase dramatically as new federal regulations defined in the Health Information Technology for Economic and Clinical Health (HITECH) Act provide incentives for healthcare providers to quickly move medical records online.[44]

A study in US by Ponemon Institute published in 2015 estimated that 2.32 million adult-aged Americans or close family members became victims of medical identity theft during or before 2014. The increase from last year's estimate of 1.84 million individuals represents a net change of 21.7 percent. The incremental difference between 2013 and 2014 provides an estimated 481,657 new cases[45]. The trend is same for most other developed countries.

In the United Kingdom personal data is protected by the Data Protection Act 1998[46]. The Act covers all personal data which an organization may hold, including names, birthday and anniversary dates, addresses, telephone numbers, etc. Also, under English law (which extends to Wales but not necessarily to Northern Ireland or Scotland), the deception offences under the Theft Act 1968[47] increasingly contend with identity theft situations. In ***R v Seward***[48] the defendant was acting as the "front man" in the use of stolen credit cards and other documents to obtain goods. He obtained goods to the value of £10,000 for others who are unlikely ever to be identified. The Court of Appeal considered sentencing policy for deception offences involving "identity theft" and concluded that a prison sentence was required. Henriques J. said "Identity fraud is a particularly pernicious and prevalent form of dishonesty calling for, in our judgment, deterrent sentences.

In the light of the above, statutory efforts have been made in Nigeria with respect to medical identity theft. For instance, in an attempt to address the crime, the provisions of the Criminal Code Act[49] defined stealing. Similarly, some

[42] *Ibid.*
[43] Poneman L. (2010) 'National Survey on Medical Identity Theft' Experian, vol.1 no.1, p.1.
[44] Poneman L. (2010) 'The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches' Experian, vol.1 no.3 p.1.
[45] Fifth Annual Study on Medical Identity Theft, Ponemon Institute, February 2015. From <ponemoninstitute.gov>. Retrieved on October 24, 2018)
[46] Data Protection Act 1998
[47] Theft Act 1968
[48] *R v Seward* [2005] EWCA Crim 1941.
[49] Cap. C34, LFN 2004. Section 382

elements of the crime fall under other sections of the Criminal Code Act that define obtaining credit by false pretence, cheating, conspiracy to defraud and forgery. The Penal Code also provides for theft, cheating, cheating by personating, making a false document, forgery and forged document.[50] Similarly, the recently enacted Cybercrimes Act, 2015 provides against identity theft and impersonation, against use of electronic card of another, against dealing in card of another, and purchase or sale of card of another[51]. Under the Act, medical identity theft in itself would qualify as false pretence[52] and impersonation with the intention (*mens rea*) to commit fraud, while the act (*actus reus*) of successful use of the stolen medical identity to obtain medical care, buy drugs, submit fake bills for recompense or even to impersonate and practice as a medical personnel would amount to a felony under the Act[53] The Penal Code Act also contains a similar provision[54]. In a related vein, a suspect of medical identity theft could alternatively be charged under the provisions of the Criminal Code Act on stealing[55].Also, the Medical and Dental Practitioners Act[56] provides specifically against impersonation of a medical practitioner[57].

It is however sad that there is no legislation in Nigeria dealing specifically and comprehensively with medical identity theft, not even the National Health Insurance Scheme (NHIS) Act of 1999. This is one of the major motivations for this work. Although the Nigerian Criminal Code Act, the Penal Code Act and the Cybercrime Act 2015, accommodate certain aspects of identity theft in general, there is no specific legal framework capable of effectively addressing medical identity theft in Nigeria.

1.5 Conclusion

Medical identity theft is the appropriation or misuse of a patient's or a provider's unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or service. It involves purposeful misuse of identifiers and can lead to consequences such as monetary losses, criminal fines, imprisonment, and exclusion from medical insurance. It unduly compromises patient care through the entry of inaccurate health information into a victim's health record, loss of accuracy of medical records, expenses to

[50]Sections 286, 320, 321, 362, 363.
[51]Cybercrimes Act 2015. Sections 22, 33, 34, 35.
[52]Section 418.
[53] Section419.
[54]Section 320.
[55]Section 421.
[56] Cap. M8 Laws of the Federation of Nigeria 2004.
[57] Section 17

individuals whose identities are stolen, widespread expenses to the health care system and compromised patient care if inaccurate health records are relied on at the point of care. In many cases, it can kill. This crime takes many forms and invariably leaves victims that are alive with the task of repairing the damage to their lives. This study found that there are laws on all kinds of identity theft in Nigeria that cover medical identity theft. Specifically, the study showed the absence of a specific legal framework on the subject. Consequently, it recommends the need for such a specific law and more research on medical identity theft. These underscore the need to heighten awareness of the crime to stimulate the National Assembly to enact a specific legislation setting out a specific legal framework for the definition, types and punishment for the crime.