

# BIOMETRIC TECHNOLOGY TOWARDS PREVENTION OF MEDICAL IDENTITY THEFT: PHYSICIANS' PERCEPTIONS

Chevella N. Oliver MHIIM, Sajeesh Kumar, PhD

Department of Health Informatics & Information Management, University of Tennessee

Health Science Center, Memphis, TN, USA

## ABSTRACT

*While Financial Identity Theft (FIT) has been an ongoing threat to the safety of American society with its horror and inconvenience, Medical Identity Theft (MIT) is now an additional risk on the horizon and there are many perils associated with this burgeoning phenomenon. This paper will examine the physician perceptions and look at the menacing burden that MIT places on its victims. It will also discuss ways in which the provider can better address issues by using biometric technology to combat this escalating problem. Also, MIT can be more damaging than FIT because it can create mayhem for the victim and his or her medical information when erroneous details have been created in the medical record due to a thief's scheming and deceitful usage of healthcare information. The literature suggests that biometric technology can revolutionize the healthcare industry with scientific tools that can scan your eye, hand or thumbprint and a person can be easily identified. This technology would add another layer of security to give greater protection to healthcare users as well as providers. Biometric technology is an exciting untapped resource that can make an incredible difference in the field of healthcare and PHI. This project will shed some light on this technology and may help the healthcare community understand the viability of biometrics and how it can possibly deter MIT.*

*Biometric Technology towards Prevention of Medical Identity Theft: Physicians' Perceptions*

## 1. INTRODUCTION

Medical Identity Theft (MIT) is a tremendous problem that is causing enormous concern in the healthcare community. If the health care industry does not explore and consider the use of biometric technology within its operating purview then it will perhaps be susceptible to a breakdown in the infrastructure which can likely be more devastating than financial identity theft. "Medical Identity theft (MIT) is a practice in which someone uses another individual's identifying information such as health insurance or social security number without the individuals 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."(Mancino, 2014) As a result, MIT has become a huge problem in the health care arena. It can be so much more devastating than the crime of financial identity theft and is extremely disturbing because MIT can affect anyone who is the holder of a medical or health insurance card.

"Biometric technologies are automated methods for identifying a person or verifying a person's identity based on the person's physiological or behavioral characteristics."(Radack, n.d.) Biometric technology is not new; however, based on the reading, it is not being used overwhelmingly by the healthcare community. With the proliferation of MIT in the American

infrastructure, the door has been opened to more data breaches, added security issues and wrongdoers scamming victims' medical identity. It is now a huge reality and far too common. Financial Identity Theft (FIT) was relatively unknown twenty years ago. Fast forward to 2015 and it appears that few professionals and consumers are aware of its evil twin medical identity theft and the snowball effect that it has on the victim as well as the American economy. Pam Dixon, Executive Director, of the World Privacy Forum brought attention to MIT by researching and writing the first known report on the crime in May 2006. (Dixon, P. & Gellman, B., 2006) It is now on the horizon as a moderately talked about topic. While FIT has been more of the hot subject matter and news reports have stated that FIT has cost the US billions of dollars annually, the toll can be even greater if MIT is the crime against an individual. (Dixon, et al)

Indeed, it is almost impossible to believe that in the not so distant past, FIT was a perplexing and a rather ambiguous crime. This infraction has reached exponential levels and Congress passed the Identity theft and Assumption Deterrence Act to respond to the growing problem of identity theft. (Identity theft overview, n.d.) Now MIT has taken center stage and is invasive in all areas and difficult at best to resolve. It has become evident that with the dawn of the new millennium that identity thieves are finding more clever ways to steal other peoples' personal information that includes not just social security numbers and credit cards but health care insurance cards. MIT is an increasing perplexity in this society and can cause more headaches than the theft of the beloved plastic money. Since The U.S. Department of Health and Human Services started keeping records on MIT in 2009, it has found that the medical records of between 27.8 million and 67.7 million people have been breached. (Ollove, 2014)

Recently, a small online Medical Identity Theft Knowledge Survey was administered by The Identity Theft Resource Center (ITRC) and 167 responses were received. A mere 13.8 percent claimed they understood the meaning of medical identity theft; however, 42.5 percent had to be excluded for the remainder of the survey questions because they had no concept as to what medical identity theft is. Sadly, MIT is not on most people's consciousness. (Mannino, 2014)

If an impostor accesses your healthcare care card to receive services at a hospital or doctor's office and the claim is submitted for reimbursement to the insurance company for his or her healthcare fees, this can be destructive to the holder of the medical insurance card financial well-being and medical life. What about diagnoses that have nothing to do with the victim's previous medical history? How can a person explain an STD diagnosis or a blood borne illness? What if the victim is given the incorrect blood type when receiving a blood transfusion? The diagnosis three months ago indicated that the person is in prime condition yet Stage IV colon cancer is now the ailment. (Linder, 2014) Of course, instances such as the aforementioned should raise red flags and give an insurance company reasons to question those situations. Will the victim be able to correct his or her record? How many records are out there for the victim? How many health care practitioners has the perpetrator seen? What type of services has the perpetrator been given? These are some of the questions that can bombard the mind and life of the innocent victim.

It is unusually challenging to correct inaccurate information when an MIT breach is exposed. Sensitive information may have already been released to other medical providers, medical clearinghouses or insurers. (Rebstock, 2009) Moreover, victims can be harassed by debt collectors, may experience loss of or difficulty finding work, may be rejected for insurance coverage and may even find that wrongful accusations of criminal activity have been imposed on them. Providers can also be victims. Having to return money to insurance companies, face possible litigation and civil penalties as well as deal with negative media and a decline in consumer confidence can weigh heavily on providers. (Rebstock, 2009)

MIT happens to be more profitable than financial identity theft. A pilfered Social Security number is anticipated to have a street value of \$1 per identity while ill-gotten medical identity information can fetch on average \$50 per identity. (Rebstock, 2009) Personal information can be obtained by thieves through lost or stolen wallets, purses, dishonest medical personnel, or perhaps family members and colleagues. (Medical id theft, n.d.) Also, there are people who rummage through outdoor trash receptacles who find medical documents that are not shredded which contain personal information that can be used for their fraudulent gain. It is unfortunate; however, reports estimate that 33% of medical ID theft happens when an acquaintance or even a family member uses an individual's medical information without their consent or knowledge. (Medical id theft, n.d.)

The primary objective of this study is to assess physicians' perceptions regarding the use of biometric technology as a deterrent against MIT. Data will be examined from a web based survey of physicians within the Memphis Medical Society to determine if they are aware of biometric technology and if they are familiar with the term medical identity theft.

## **2. TYPES OF BIOMETRICS**

Biometrics come in a number of different forms and this paper will discuss seven of them. The simplest and most common is the fingerprint. Nearly everyone has a fingerprint unless there has been some type of accident to disfigure the fingers. It is safe with no hassle. Police programs and crime prevention agencies such as the FBI have used fingerprint technology for decades. (Fingerprints, n.d.) The biometric modality known as speaker or voice recognition uses an individual's voice for detection purposes. It is a different technology than speech recognition which recognizes words as they are pronounced and does not fall into the category of a biometric. The method of speaker recognition depends on features which are impacted by the physical configuration of an individual's vocal tract and the individual's behavioral characteristics. (Voice recognition, n.d.)

Palm print is similar to the fingerprint because it deals with the ridge impression of the hand. History shows that the handprint was used when illiterate people did not have the education to know how to sign their names. While it has been available for more than a century, it is a technology that has lagged behind in automation because of constraints in computerization systems and operations. (Palm print, n.d.)

Facial recognition relies on the fine points of spatial geometry to differentiate the features of the face and analyze them for identification. (Woodward, Horn, Gatune, & Thomas, 2003) This biometric technology has been used to spot shoplifters in stores, and pinpoint criminals and terrorists in urban areas. In the casinos facial recognition has been used to identify card counters or other undesirables where gambling is the business. (Woodward, et al.) Although, the technology has not yet been perfected, it is developing and has tremendous potential. (Woodward, et al.)

One of the most well-known biometric technologies is retinal scanning; however, it is extremely costly. This technology was discovered in the 1980s. Retinal scans map the distinctive configurations of an individual's retina. Within the retina are blood vessels which absorb light more easily than the tissue which encloses it and it is easily identified with the proper lighting. (King, 2013)

The most unique feature visible on the human body is the iris. Fortunately, no two irises are alike. Even identical twins have dissimilar iris configurations. There is much detail in the iris with

its variability and lack of genetic dependence. Also, it has the suitability for imaging without physical contact which could potentially make the iris an excellent personal identifier. (Eye controls, n.d.)

The physical activity of signing, such as the stroke order, the pressure applied and the speed are measurements and analysis of the biometric signature recognition system. (Signature biometrics, n.d.) “Dynamic signature devices should not be confused with electronic signature capture systems that are used to capture a graphic image of the signature and are common in locations where merchants are capturing signatures for transaction authorizations.” (Mayhew, 2012) Unfortunately, there may be issues with this technology since the signature can change over time.

### **3. METHOD**

Twenty-three questionnaires were administered via email to the 1403 Memphis Medical Society members. This community of physicians was chosen because it had a high volume of potential participants. The survey was initiated via email on June 23, 2015 and closed on July 7, 2015.

### **4. RESULTS**

The study indicates that physicians within their respective disciplines would be willing to accept change within their current state of affairs but cost appeared to be a major reason for not implementing this equipment. The sample size could have been expanded by including receptionists, business office managers and more of the individuals who actually deal with the clients and their presentation of insurance paperwork daily. Personal interviews would probably prompt better information regarding participants' knowledge and attitudes and offer the opportunity to clarify vague or confusing questions.

### **CONCLUSION**

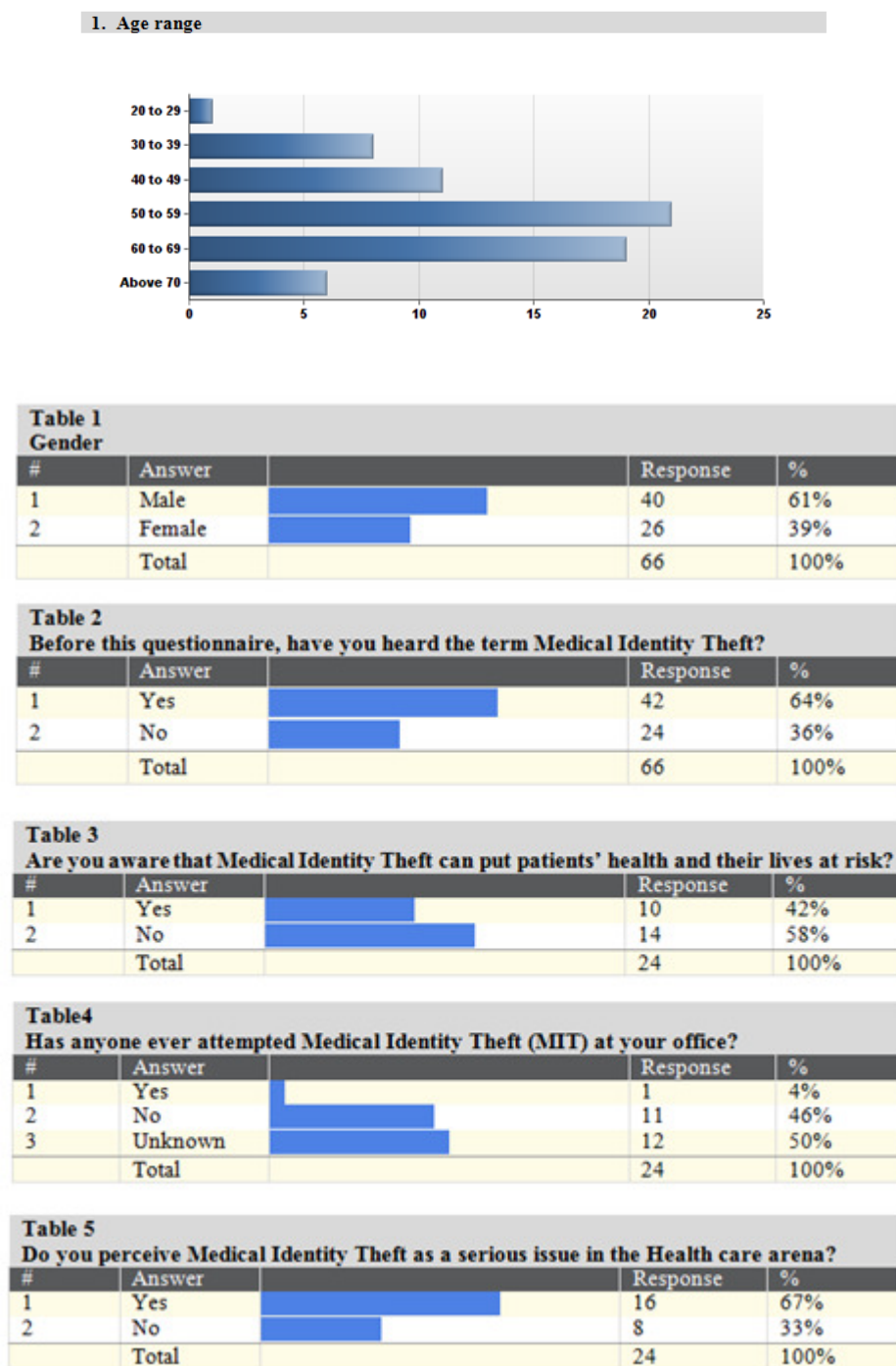
MIT is seen as a tremendous problem and biometric technology is recommended as being a possible protective measure to prevent that criminal activity. It must also be noted that MIT is an intricate and nefarious crime because it totally violates the victim in the most intimate areas of their lives. While HIPAA is stringent, it does not address MIT. (Mancini, 2014) Unfortunately, because there are no laws which really concentrate on this type of personal violation and crime, it is difficult to investigate and bring resolution to what is quickly becoming a burdensome and disturbing problem. (Mancini, 2014) More importantly, the research of this project shows that the actual physicians are not as aware or knowledgeable about this escalating fraud movement. If implemented, biometric technology can be an additional layer of protection to make strides in the improvement of patient security and safety. It can also be an effective means to promote enhanced office and hospital functioning. A well-structured system utilizing biometric technology can be designed to streamline the registration process and patients can be assured that they will receive high level quality of care specifically for their correct identity.

### **REFERENCES**

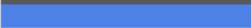
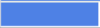
1. Andrews, M (2008) Medical identity theft turns patients into victims <http://health.usnews.com/health-news/family-health/articles/2008/02/29/medical-identity-theft-turns-patients-into-victims>
2. Carrazzo, V., retrieved July 24, 2015 from <http://www.mdmemphis.org/index.php/about-us/#history>









3. Dixon, P.,(2006). *Medical identity theft:the information crime that can kill you*, retrieved July 6, 2015 from [http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wp\\_f\\_exsum\\_medidtheft2006.pdf](http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wp_f_exsum_medidtheft2006.pdf) p.2
4. *Eye controls*, retrieved July 25, 2015 from <http://www.eye-controls.com/technology>
5. *Fingerprints& Other Biometrics* (n.d.) para.1-3, retrieved July 22, 2015 from [https://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics)
6. Hallam, K., (2013)*Biometric technology combats medical identity theft*, retrieved July 21, 2015 from <http://www.bloomberg.com/bw/articles/2013-05-09/biometric-technology-combats-medical-identity-theft>
7. *Identity theft overview*, retrieved July 23, 2015 from [https://www.fbi.gov/about-us/investigate/cyber/identity\\_theft/identity-theft-overview](https://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview)
8. King, R.,Explainer: Retinal scan technology, (2013), retrieved July 23, 2015 from <http://www.biometricupdate.com/201307/explainer-retinal-scan-technology>
9. Linder, A., Medical identity theft: the fraud that can kill you, (2014), retrieved July 10, 2015 from <http://www.dailyfinance.com/2014/03/31/medical-identity-theft-fraud-can-kill-you/>
10. Mancino, M., (2014). *Medical identity theft in the emergency department: awareness is crucial*, retrieved July 20, 2015 from <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4251251>
11. Mannino, N. (2014) *Medical Identity Theft: it's your life on the line* retrieved July 27, 2015 from <http://www.creditsesame.com/blog/medical-identity-theft-s-life-line/>
12. Mayhew, S., Explainer: Dynamic signature, (2012), retrieved July 25, 2015 from <http://www.biometricupdate.com/201206/explainer-dynamic-signature>
13. *Medical Identity Theft* retrieved July 20, 2015 from, <https://www.allclearid.com/blog/medical-identity-theft>
14. Ollove,,M., (2014), *The rise of medical identity theft in healthcare*, retrieved July 18, 2015 from <http://khn.org/news/rise-of-indentity-theft/>
15. *Palm Print* (n.d.) para. 1-2, retrieved July 22, 2015 from [https://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/biometric-center-of-excellence/modalities/palm-print](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/modalities/palm-print)
16. Pribish, M., *Medical ID theft cost victims big money* <http://www.azcentral.com/story/money/business/tech/2015/06/12/medical-theft-victims/71101190/>
17. Qualtrics at UTHSC (2015) retrieved July 10, 2015 from <http://www.uthsc.edu/edtech/productivity/qualtrics/>
18. Radack, S., (n.d.)*Biometric technologies: helping to protect information and automated transactions in information technology systems*,retrieved July 20, 2015 from <http://www.itl.nist.gov/lab/bulletns/bltnsep05.htm>
19. Rebstock, J., (2009), *Preventing medical identity theft*, retrieved July 25, 2015 from [http://sip.omnera.com/?post\\_type=risk\\_rx\\_article&p=834](http://sip.omnera.com/?post_type=risk_rx_article&p=834)
20. Reubens, P. (08/17/2012), *Biometric authentication: How it works?* Retrieved July 24, 2015 from <http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html>
21. RightPatient®(n.d.)retrieved July 27, 2015from <http://www.rightpatient.com/>
22. Shin, L., (08/31/2014) *Medical identity theft: How the healthcare industry is failing us?* Retrieved July 20, 2015 from <http://fortune.com/2014/08/31/medical-identity-theft-how-the-health-care-industry-is-failing-us>
23. *Signature biometrics*,(n.d.) retrieved July 25, 2015 from [http://www.biometricnewsportal.com/signature\\_biometrics.asp](http://www.biometricnewsportal.com/signature_biometrics.asp)
24. *Voice Recognition*(n.d.) para.1, retrieved July 22, 2015 from [https://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/biometric-center-of-excellence/modalities/voice-recognition](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/modalities/voice-recognition)
25. Woodward, J., Horn,C., Gatune, J.,& Thomas, A., *Biometrics: a look at facial recognition* (2003), retrieved July 24, 2015 from <https://www.ncjrs.gov/App/publications/abstract.aspx?ID=204484>

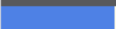
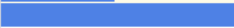
Figure 1



| Table 6<br>How do you agree with the following statements? |  |                |       |         |                 |          |                 |      |
|--|--|----------------|-------|---------|-----------------|----------|-----------------|------|
| #  | Question   | Strongly Agree | Agree | Neutral | Strong Disagree | Disagree | Total Responses | Mean |
| 1  | Patients should be more diligent in protecting their healthcare ID cards so Medical Identity Theft would not be so widespread. | 24             | 28    | 10      | 1               | 2        | 65              | 1.91 |
| 2  | Physicians should protect patients against medical identity theft.   | 34             | 25    | 5       | 0               | 1        | 65              | 1.60 |
| 3  | Physicians should protect themselves against problems arising from medical identity theft.                                     | 40             | 22    | 3       | 0               | 0        | 65              | 1.43 |






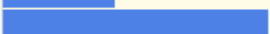
| Table 7<br>Are you familiar with the term biometric technology? |        |   |          |      |
|---|--------|---|----------|------|
| #   | Answer |   | Response | %    |
| 1   | Yes    |  | 47       | 72%  |
| 2   | No     |  | 18       | 28%  |
|   | Total  |   | 65       | 100% |

| Table 8<br>Please indicate which, if any, biometric technology you have heard of: |                    |   |          |      |
|---|--------------------|---|----------|------|
| #   | Answer             |   | Response | %    |
| 1   | Fingerprint        |  | 24       | 37%  |
| 2   | Voice recognition  |  | 0        | 0%   |
| 3   | Palm               |  | 1        | 2%   |
| 4   | Facial recognition |  | 5        | 8%   |
| 5   | Retinal scan       |  | 14       | 22%  |
| 6   | Iris scan          |  | 8        | 12%  |
| 7   | Signature          |  | 7        | 11%  |
| 8   | None               |  | 6        | 9%   |
|   | Total              |   | 65       | 100% |







| Table 9<br>Are you aware that biometric technology is currently being used in some medical offices to confirm patient identity at check-in? |        |   |          |      |
|---|--------|---|----------|------|
| #   | Answer |   | Response | %    |
| 1   | a. Yes |  | 21       | 32%  |
| 2   | b. No  |  | 44       | 68%  |
|   | Total  |   | 65       | 100% |

**Table10**

Please indicate which, if any, biometric technology you have seen used in a medical office setting:

| # | Answer             |   | Response | %    |
|---|--------------------|---|----------|------|
| 1 | Fingerprint        |  | 4        | 6%   |
| 2 | Voice recognition  |  | 1        | 2%   |
| 3 | Palm               |  | 1        | 2%   |
| 4 | Facial recognition |  | 2        | 3%   |
| 5 | Retinal scan       |   | 0        | 0%   |
| 6 | Iris scan          |   | 0        | 0%   |
| 7 | Signature          |  | 17       | 26%  |
| 8 | None               |  | 40       | 62%  |
|   | Total              |   | 65       | 100% |

**Table 11** What do you believe is the biggest benefit of using biometric technology in the medical office?

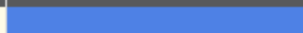
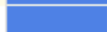

| # | Answer                              |   | Response | %    |
|---|-------------------------------------|---|----------|------|
| 1 | Reduce data breaches                |    | 6        | 17%  |
| 2 | Eliminate duplicate medical records |    | 4        | 11%  |
| 3 | Raise patient safety levels         |  | 8        | 23%  |
| 4 | Prevent fraud                       |  | 13       | 37%  |
| 5 | Medical costs will decrease         |  | 1        | 3%   |
| 6 | Other                               |  | 3        | 9%   |
|   | Total                               |   | 35       | 100% |

Other

Increase efficiency to decrease typed log-in to EHR  
wasting money  
None

**Table12**









What do you believe is the biggest drawback to using biometric technology in the medical office?

| # | Answer                                      |   | Response | %    |
|---|---|---|----------|------|
| 1 | Cost  |  | 24       | 69%  |
| 2 | Implementation                              |  | 8        | 23%  |
| 3 | Educating staff                             |   | 0        | 0%   |
| 4 | None of the technologies are 100% foolproof |  | 3        | 9%   |
| 5 | Other                                       |   | 0        | 0%   |
|   | Total                                       |   | 35       | 100% |





**Table 13**

**Which type would be most practical for your office?**

| # | Answer             |   | Response | %    |
|---|--------------------|---|----------|------|
| 1 | Iris scan          |  | 2        | 6%   |
| 2 | Finger print       |  | 17       | 49%  |
| 3 | Palm               |  | 0        | 0%   |
| 4 | Facial recognition |  | 3        | 9%   |
| 5 | Voice recognition  |  | 0        | 0%   |
| 6 | Signature          |  | 4        | 11%  |
| 7 | Retinal scan       |  | 2        | 6%   |
| 8 | None               |  | 7        | 20%  |
|   | Total              |   | 35       | 100% |



**Table14**

**If cost was not a factor, would you implement biometric measures at your office?**

| # | Answer |   | Response | %    |
|---|--------|---|----------|------|
| 1 | a. Yes |  | 28       | 82%  |
| 2 | b. No  |  | 6        | 18%  |
|   | Total  |   | 34       | 100% |

**Table15**

**Have you given thoughtful consideration to biometric technology?**

| # | Answer |   | Response | %    |
|---|--------|---|----------|------|
| 1 | a. Yes |  | 9        | 26%  |
| 2 | b. No  |  | 25       | 74%  |
|   | Total  |   | 34       | 100% |

**Table16**

**Why or why not?**

**Text Response**

too many unanswered questions and violation of privacy

Have had a patient use her sister's credit card to pay for surgery. Pretended to be her sister, had the surgery and we only found out when the sister called us to complain!

Not pursued at this time

increases efficiency.

I work in the ED so it could be difficult to have the government actually allow something beneficial for patients to be implemented.

How is it best implemented in pediatrics?

Overwhelmed with too many other problems - EHR implementation (and EHR updates that don't work and crash the system and clueless IT people who don't know how to fix it), Meaningful Use documentation, Medicare audits, ICD-10 etc.

I don't think this will be a reality before I retire.

I am a hospitalist

I have recently retired from active medical practice

have not thought about it yet, we do photo ID in the office

I am a pediatrician. It is unlikely a child would attempt to defraud anyone or misrepresent themselves.

we have the patient take a photo. we add that to there chart. no need for biometrics

Finger print is easy, How do we confirm that, we accept what we get.

Biometric measures have already been implemented in our office but for the protection of radioactive sources, not for patient identification. We are hospital based & I would unfortunately be the last person consulted about whether to implement biometric tools or not. Hospital administrators, the persons making this type of decision, do not interact with us.

I am a Regional One Employee. That type decision is far above my pay grade  
time, cost

Too many other things to worry about

I have been victim of ID theft

Basic lack of awareness.

Unnecessary

Part of a large multispeciality group - not tasked with these decisions.

It would be too early to consider this technology in my current office setting due to cost.

i work exclusively in a hospital so not my choice  
It doesn't seem to be widely used at this time.

**Table 17**

| # | Question   | Strongly agree | Agree | Neutral | Strongly Disagree | Disagree | Total Responses | Mean |
|---|--|----------------|-------|---------|-------------------|----------|-----------------|------|
| 1 | Biometric tools are still a developing technology and too expensive to implement at my office. | 8              | 15    | 8       | 1                 | 2        | 34              | 2.24 |
| 2 | I believe that my office will put biometric technology into operation in the next 2 years.     | 2              | 4     | 14      | 7                 | 7        | 34              | 3.38 |
| 3 | The culture in this office is implementing biometric technology.                               | 2              | 4     | 15      | 7                 | 6        | 34              | 3.32 |

**Table 18****Biometric technology increases security against medical identity theft**

| # | Answer               | Response | %    |
|---|----------------------|----------|------|
| 1 | a. Strongly agree    | 10       | 24%  |
| 2 | b. Agree             | 29       | 69%  |
| 3 | c. Neutral           | 3        | 7%   |
| 4 | d. Strongly Disagree | 0        | 0%   |
| 5 | e. Disagree          | 0        | 0%   |
|   | Total                | 42       | 100% |

**Table 19****Biometric technology is the best way to prevent medical identity theft.**

| # | Answer               | Response | %    |
|---|----------------------|----------|------|
| 1 | a. Strongly agree    | 4        | 10%  |
| 2 | b. Agree             | 16       | 38%  |
| 3 | c. Neutral           | 18       | 43%  |
| 4 | d. Strongly Disagree | 2        | 5%   |
| 5 | e. Disagree          | 2        | 5%   |
|   | Total                | 42       | 100% |

**Table 20**

**Would you like to learn more about available biometric office safeguards against Medical Identity Theft?**

| # | Answer |  | Response | %    |
|---|--------|--|----------|------|
| 1 | a. Yes |  | 40       | 67%  |
| 2 | b. No  |  | 20       | 33%  |
|   | Total  |  | 60       | 100% |

**Table 21**

**Would you be interested in attending a free webinar on MIT & biometric technology solutions?**

| # | Answer |  | Response | %    |
|---|--------|--|----------|------|
| 1 | a. Yes |  | 24       | 40%  |
| 2 | b. No  |  | 36       | 60%  |
|   | Total  |  | 60       | 100% |