

Biometrics in Pharma: Politics and Privacy

Daniel Shapiro* and Sidney Shapiro⁺

*School of Information Technology and Engineering, University of Ottawa
Email: dshap092@site.uottawa.ca

⁺Department of Political Science, Laurentian University
Email: sx_shapiro@laurentian.ca

Abstract:

The Drug Enforcement Agency (DEA) has announced the implementation of the use of both computerized and biometric security protocols in the electronic prescription of controlled substances. Electronic prescriptions which were up until this point not allowed to be prescribed by electronic means will now be easier for physicians and the DEA to monitor and prescribe.

This paper will examine the various practical, political, and privacy issues as well as the potential benefits of the use of biometric information for the prescription of narcotics and other controlled substances. The proposed changes will build in non-repudiation and improve accountability, while introducing problems such as delegation, privacy, cost, and information security. Another consequence of strong biometric authentication is false acceptance and false rejection rates. Not only are there annoyances due to false reject rates, there are serious medical consequences when a drug cannot be obtained due to failed biometric authentication.

Introduction:

"Sixty-four percent of American households are regular consumers of prescription drugs" [20]. The ever growing rates of prescribing of medications to patients creates a system that can be vulnerable to fraud and inefficiency. As far back as 1994 the integration of biometrics into prescriptions was discussed in the research community [17]. Many Electronic Medical Record (EMR) programs are designed to assist physicians with their prescriptions as well as their patient records, and many of these systems have built-in fraud-detection capabilities for the generated prescriptions [26]. These systems may be used by specialists such as dentists, oncologists, and anesthesiologists, who routinely prescribe controlled substances, such as narcotics. The widespread use of these systems opens up the possibility of abuse by staff, patients, or even criminals. The safeguards built into these systems are able to be overcome for nefarious purposes, representing a danger to the system of medication prescription, and the public which the system is designed to protect. Overall, prescription narcotics and other controlled substances represent approximately 1 in 10 prescriptions in the USA [1]. According to the DEA,

electronic prescription of controlled substances requires at least two methods of identification, including one biometric [1].

The US Health Insurance Portability and Accountability Act (HIPAA) contains privacy and security requirements regarding health records, including prescriptions [10]. Similar privacy safeguards of electronic patient medical data are regulated in a number of other states. Electronic Transmission of Prescriptions (ETP) is mandated by the National Health Service (NHS) in the United Kingdom, and Canada has issued the Personal Information Protection and Electronics Documents Act (PIPEDA) [14]. Generally, around the world, government policy has not kept up with rapidly changing technology. This has created a gap between legislation and technology due to the ever increasing potential for cost savings and streamlined regulation.

The effects of moving from personal patient care and human involvement to an electronic regime of prescribing and dispensing drugs creates numerous problems. The result of a system reliant on digital data which can potentially be compromised through numerous vulnerabilities is that care and attention are sacrificed for cost savings and expediency. Narcotics, which present powerful healing and pain management properties, require more, and not less supervision and human oversight due to their potential for abuse and diversion.

Improved Accountability:

Electronic prescriptions provide many potential benefits to society. For example, scientists can evaluate the adherence of patients to prescription regimens and patient compliance using electronic databases, reduce the cost of health care delivery, and reduce the number of medical errors [2, 3, 4]. Pilot projects have demonstrated electronic prescriptions to be a viable alternative to traditional prescriptions with increased accuracy and improved accountability [30].

As a further layer of security is introduced, additional benefits to society can be derived from the implementation of a secure biometrics-based electronic prescription system. The additional benefits of biometric security include verification, non-repudiation, and removal of delegation capabilities. Furthermore, biometric identification streamlines the process of identifying an individual, providing shorter wait times for patients, and lower costs in the long-term for pharmacies.

The verification of the identity of the person who brings in a prescription reduces the willingness of patients to misuse or divert a prescription. Since the prescription is tied to an individual, it is not worth selling. Third parties could not successfully access prescriptions not intended for their own use. This is particularly relevant to controlled substances prescribed to an individual which has the potential to be diverted. There are other cases where biometrics provide benefits as well. One example is the sale of a controlled substance, another is the distribution of fake pharmaceuticals. Such illicit transactions could be traced back to a specific prescription that can then be biometrically associated to a specific individual and pharmacy [16]. The prescription holder or

pharmacy would then have to explain to the authorities how the controlled substance ended up as a fake product or in the wrong hands.

Potential Problems:

Problems related to the adoption of biometrics in pharma include negative public perception, the inability to delegate responsibility for picking up a prescription, possibly leaking private information to hidden third parties, increased costs due to infrastructure investment, loss of biometric identification due to injury or illness, vulnerability to technology failure, vulnerability to hackers, and possible incompatibility of internet pharmacies with biometrics technology due to replay attacks. We avoid discussion of the plethora of problems associated with EMR and e-health more generally, including the security of health records upon storage, and human engineering.

Human Factors:

Public perception of biometrics in the United States is tied to the notion of a right to privacy for American citizens, and a fear that governments are tracking regular citizens in conjunction with their legitimate tracking of criminals and terrorists. For example, the use of biometrics in prescriptions for antidepressants may pose the additional problem that paranoid individuals may fear that their biometric compromises their security, and opt to avoid legal pharmaceuticals such as Selective Serotonin Reuptake Inhibitors (SSRI). The initial release of biometric data in an electronic form as the key to accessing electronic pharmaceutical dispensing creates a number of worrying potential problems for many patients and privacy advocates. Far from being a terrifying big brother, the United States and other governments have put in place legislative safeguards that prevent patient data from being used for illicit purposes. In response businesses have litigated to continue their privacy invading practices [24, 25].

In order to discourage fraud, misuse, or breach of privacy by healthcare workers, it has been suggested that practices such as limiting the number of queries to the electronic records system and allowing peers to review each other's conduct will ensure a lower level of misbehavior [29]. When the number of queries by an individual is exceeded, they could approach a peer to budget for additional queries to the system.

There are some practical issues with the use of biometric information that must be overcome in order to comply with HIPAA privacy and security rules. For example, in the United States a patient is legally allowed to have a friend or family member pick up a prescription for them at the pharmacy, at the discretion of the dispensing pharmacist. However, biometric identification completely prevents such delegation from taking place [9]. In Ontario, Canada, all prescriptions must be picked up by the person who has their name on the prescription. This is an example where differing regulations meet the limitations of technology. Biometric security for legitimate prescriptions, while strengthening the safeguards for the distribution and dispensing of certain types of pharmaceuticals such as narcotics, represents an apparent benefit to society. However,

these types of measures could have unintended consequences and have a limiting effect on access to other types of pharmacy dispensed prescriptions.

The Impact of Technology:

The medical consequences of false rejection of a valid prescription could have devastating patient care results. In the same vein, the false acceptance of fake, modified, or invalid prescription can be catastrophic to the trust and premise of security built into the entire system when dealing with the dispensing of controlled substances. The motivation for attempting to pass illegitimate prescriptions can be financial as well as drug seeking. Indeed, should a vulnerability in the electronic system be exploited, the potential for abuse could be much larger than in a system reliant on human judgment and detection. Indeed, a wide scale breach could result in far greater damage to society in terms of illicit pharmaceuticals available. When a false rejection is allowed by the electronic system, there exists similar, yet more specific, potential for harm. For example, consider a patient with a valid prescription that is turned away from a pharmacy due to a glitch in technology. That patient may experience severe pain, withdrawal, or even death as a result of the false rejection.

The loss of biometric authentication capability can result from injury, illness, or the environment. For example, a face recognition system might fail if the lights go out at night, or a patient with a cold may appear to have a different voice biometric. Similarly, a palm print may be modified by a burn or cut. The quality of biometric authentication can be improved when several biometric parameters are used together in order to avoid many such cases [21]. Face image biometrics can be improved by using thermal imaging, which does not vary greatly with the lighting condition in the room [23]. Using a number of biometric technologies simultaneously has the potential to increase overall accuracy, and be less prone to false rejection due to degraded authentication.

False accept rates are not expected to be a serious problem in the long-term since each new biometric technology has shown an increase in accuracy over time. For example, fingerprint scanners can identify fake fingerprint attempts using sensors to observe the finger temperature, pulse, oxygenation, blood pressure, movement, and electrical resistance [22]. In 2004 RiteAid pharmacies implemented a fingerprint biometrics system for picking up prescriptions, and serious consequences such as false acceptances were not reported [31].

Vulnerability to a technological failure goes beyond rates of false acceptance and rejection. Even if the system is working perfectly there may be long service interruptions due to power failures in remote pharmacies. Any system solely reliant on biometrics for authentication would be unable to function without access to communication and information unless the data was stored locally, negating the usefulness of a large scale distributed system. Another possible source of biometric system failure is a software failure due to a bug in the implementation, or a hardware failure in any component in the system including cameras, fingerprint scanners, barcode readers, and computers.

Secure authentication, secure data transmission, cost-effective security, and fast execution of security mechanisms are all highly desirable when implementing biometrics and electronic prescriptions on a large scale. Public key infrastructures are good for protecting secret information such as biometrics, but they are also relatively slow when it comes to encrypting and decrypting data such as a scan of a prescription. It is therefore much more desirable that prescription information be encoded in a digital certificate that is digitally signed by a physician. However, legislation does not currently allow for such a scheme in many jurisdictions. It has been suggested in [13] that in order to accelerate the execution of encryption software, a risk-based approach should be taken for data encryption. The concept is that a framework for data transmission should be adopted which understands the level of risk associated with a given document, such as a prescription, and the level of encryption employed in securing the document will match the risks associated with the document. Clearly a prescription for a controlled substance would fall under the category of a high-risk, and would be heavily encrypted.

Electronic prescriptions and automated data entry and processing reduce the cost to physicians, pharmacies, and patients while providing easier access to healthcare statistics [7, 30]. The initial cost of the infrastructure for electronic health records is, in the long term, well worth it. However, new technologies such as biometrics will continually arise and offer the possibility to improve the existing electronic infrastructure. In terms of face recognition, the cameras required are low-cost [23]. This contrasts sharply with smart card technology, which requires large investment in infrastructure for cards and readers [30]. Costs associated with new technology are a barrier to their adoption, and so portable USB storage devices are preferred over smartcards because they are half of the cost, and do not necessitate new readers because they work with existing interfaces [30, 27].

The state of privacy implemented into e-health systems is not impressive [28]. In a world where biometrics are the gateway to access control, hackers could begin harvesting biometric information from poorly secured e-health system, or by setting up a fake service with the express purpose of aggregating biometric information. Although we do not discuss here the plethora of vulnerabilities in existing infrastructure, it is worth mentioning that besides for the corporate interests in prescription data, there is a group of nasty individuals out there intent on crime and mayhem who will also attempt to violate patient privacy. Imagine a scenario where a patient prescribed with a syphilis medication is blackmailed by individuals residing in a rogue state. Paying a few hundred dollars may be worth avoiding the trouble of confessing said condition to a spouse, or attempting to deny a prescription that is tied to an undeniable biometric.

A certificate authority cannot reissue a biometric. For this reason a weak biometric system for an online pharmacy can be completely broken. A replay attack is a case where a biometric has been copied by a third party and is being used (fraudulently) to authenticate. For example, imagine taking a picture of a doctor's face in the parking lot, and then displaying the photo to a biometric face scanner in order to enter a locked room filled with narcotics, or access a locked laptop that prints prescriptions. When the password for an email account is compromised, the rightful owner of the account is asked

to change the password. With biometrics this is not possible, and if adding a password to the biometric is the solution, then what is the use of the biometric? The possible incompatibility of internet pharmacies with biometrics technology due to replay attacks is discussed in the literature [12].

One of the cheapest alternatives to the existing system of pharmacy dispensing of medications is to order drugs online, reducing the demands on the existing healthcare delivery infrastructure. Unfortunately, consumers put little trust into such online systems, and there have been problems with regards to illegitimate pharmacies [20]. Internet pharmacies represent a unique policy problem with regards to a biometric electronic prescription. In 2004 one fourth of all Americans had looked online for drug information, and four percent purchased drugs online [20]. The majority of online drug purchases were from American companies and the patient had a prescription from a doctor. The DEA has been pushing to shut down illegal online sales of controlled substances while promoting the electronic prescription of such medications by physicians [5]. It is important to remember when considering healthcare delivery alternatives that the cost of the technology is important, but there exist several other factors in cost control and service quality. One of these factors is privacy [24].

Protecting Prescription Privacy:

Imagine a prescriber being labeled in the media as drug distributor for distributing more narcotics than average, or a patient assaulted after it is revealed that she was prescribed and picked up the morning after pill. Clearly, the privacy of prescription information does not end with the medication pick-up. As long as the information on a prescription can be deciphered, it can cause damage to integrity of the system. Although there has been regulation passed to protect the public, pharmacies may legally sell prescription data to companies interested in aggregating statistics on drug usage or prescriber preferences [14, 32, 24]. In some jurisdictions the pharmacist need not inform the physician that the prescription information was sold, since the information is not covered by HIPAA [24]. There are other reasons for accessing stored prescription information such as access to a database of patient records for longitudinal studies [18]. The issue of prescription privacy can be separated into patient privacy and prescriber privacy [24, 25]. In the context of biometrics, a mountain of private patient and prescriber information could be tied to real people even more easily, completely shattering the privacy aspect of pharmaceutical delivery systems.

Currently, prescriptions from hospitals or retail pharmacies may be sold for data mining, possibly revealing prescriber identity, patient age and gender but the patient name should be redacted [24, 25]. With biometrics built into prescriptions there is a real concern that even though the patient name is not being revealed, a biometrics database can tie the individual back to the record that was sold, even years after the sale. Hospital prescriptions have the added risk of being associated with admission and discharge dates [25]. Under the current regime, there exist circumstances where the patient name can be reconstructed based on the limited information on the sold prescription data [24]. For example, a rural clinic and a newspaper report of an accident may be all you need to

identify the treatment of a celebrity car crash victim. Furthermore, pharmacogenomics, the designing of a drug specifically to match one individual, is one form of biometric identification that may someday be inherent in the basic prescription information itself [25].

Luckily, directly identifiable patient information such as a biometric is covered by privacy laws in most jurisdictions, but most laws allow the sale of identifiable information if a waiver is signed. Since the public is blissfully unaware of the practice of selling prescription data to third parties, the pharmacy can continue this practice by asking all patients to sign a vague waiver.

Legislators have focused heavily on prescriber privacy while mostly ignoring the possibility that patient privacy could be affected by changes in technology such as the broad adoption of biometrics [24]. This may be a rational approach today, since the profit motive today is identifying and selling patterns in the prescription practices and preferences of prescribers, but tomorrow this profit motive may also be directed at patients' identities. Profit driven entities acquiring prescription data have claimed that their First Amendment right to free speech provides them with the right to purchase and sell prescription information [24]. It does not require a lot of foresight to imagine how the same data brokers could sell biometrics to parties totally unrelated to pharmaceuticals. For example, a credit score could be affected by the prescription of antiretroviral AIDS medication, all because of the leaking of private prescription data into the public domain. Clearly, associating a person to a prescription can reveal the diagnosis as well as the prescription [25].

The privacy of patient prescription data can be provided in a variety of ways. Hardware mechanisms for privacy preservation include wearable tokens and encrypted smart cards which can selectively disclose information according to the patient's wishes [27, 19]. Software can be used to manage policies for access control to encrypted electronic prescriptions, removing the burden of storage from the individual but also removing their ability to explicitly control the prescription in favor of the third party hosting the data [29]. A compromise approach called "The Salford model" is to use paper prescriptions along with barcodes and error-resistant alphanumeric letter encoding in order to ensure that technological or equipment failures do not cause patients to be turned away [11]. Furthermore, patients using paper receipts can choose the pharmacy and time that they will pick up their prescription, patients maintain their confidentiality, and existing infrastructure can be used to read the barcode and/or alphanumeric code on the prescription [11]. In the privacy context the Salford model allows access to the prescription by the patient and the medical staff, while third parties to store the prescription are not required until the prescription is handed over to the pharmacy.

Applying biometrics to prescriptions could maintain patient privacy in the context of encryption and decryption of a prescription held on a patient's device such as a smartcard, Smartphone or pendant. However, biometrics could also be used to remove anonymity from prescriptions because biometrics are unique and therefore traceable. For example, a

prescription including a photo ID on it will reveal the physical appearance of the patient to anyone who sees it.

Ultimately, if a biometric is used as a password it makes lost smart cards and tokens easier to return but difficult to deny ownership. It is not difficult to foresee a future where employers require access to electronic medical records before employing an individual; records that are impossible to deny.

Conclusion:

There are numerous theoretical potential benefits to the introduction of biometric authentication in pharma. Incorporating changes in the way in which prescription drugs, particularly narcotics, are dispensed could yield increased security and lessen the potential for abuse. Numerous issues need to be fully explored to measure the practical and social ramifications of implementing a dispensing and authentication system. The practical and political hurdles aside, there is great concern regarding the security and privacy of biometric data. Biometric data is ultimately a unique “fingerprint” which cannot be duplicated or exchanged and as such becomes the most personal and important method of authentication. As explained in this paper, biometric security represents a step forward in terms of secure authentication, but is by no means infallible. Improving authentication and systems security will ultimately improve accountability, user experience and the potential for error. New problems, such as delegation, privacy issues, cost factors, and information security will continue to play a major role in the adoption, implementation and integration of biometric security in pharma.

References:

1. DEA insists on biometrics for e-prescribing. (2010). *Biometric Technology Today*, 2010(4), 3-3. doi:DOI: 10.1016/S0969-4765(10)70071-0
2. Fischer, M., Stedman, M., Lii, J., Vogeli, C., Shrank, W., Brookhart, M., & Weissman, J. (2010). Primary medication non-adherence: Analysis of 195,930 electronic prescriptions. *Journal of General Internal Medicine*, 25(4), 284-290.
3. Kaushal, R., Kern, L., Barrón, Y., Quaresimo, J., & Abramson, E. (2010). Electronic prescribing improves medication safety in community-based office practices. *Journal of General Internal Medicine*, 25(6), 530-536.
4. Rivkin, V. (2005). *E-prescriptions offer hospitals a cheaper rx; HHC facilities, others install automated drug order systems.(special report: Health care)*
5. DEA proposes regulations to curtail illicit internet prescriptions. (drug enforcement administration). (2008). *Alcoholism & Drug Abuse Weekly*, 20(28), 5.
6. Figge, H. L., Fox, B. I., & Tribble, D. A. (2009). Electronic prescribing of controlled substances. *American Journal of Health-System Pharmacy*, 66(14), 1311-1316. doi:10.2146/ajhp080597
7. Gail-Joon Ahn, & Dongwan Shin. (2002). Towards scalable authentication in health services. *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*, 83-88.

8. *Electronic Prescribing of Controlled Substances: Addressing Health Care and Law Enforcement Priorities: Hearings before the Senate Judiciary Committee, 110th Cong., 1* (2007) (testimony of Joseph T. Rannazzisi).
9. "HIPAA Privacy FAQs | CDPHP | Flexible, Comprehensive Health Plans | New York". CDPHP. 09/03/10 <<http://www.cdphp.com/providers/hipaa.aspx>>.
10. Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191. Print.
11. Ball, E., Chadwick, D. W., & Mundy, D. (2003). Patient privacy in electronic prescription transfer. *Security & Privacy, IEEE, 1*(2), 77-80.
12. Bodnar, P. (2008). A solution to remote biometric identification. *Information Technology, 2008. IT 2008. 1st International Conference on*, 1-4.
13. Boonyarattaphan, A., Yan Bai, & Sam Chung. (2009). A security framework for e-health service authentication and e-health data transmission. *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*, 1213-1218.
14. Dick E Zoutman, B Douglas Ford, & Assil R Bassili. (2004). The confidentiality of patient and physician information in pharmacy prescription records. Canadian Medical Association. Journal, 170(5), 815-6. Retrieved August 17, 2010, from ProQuest Nursing & Allied Health Source. (Document ID: 592656151).
15. Chadwick, D. W., & Mundy, D. (2003). Policy based electronic transmission of prescriptions. *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on*, 197-206.
16. King, B., & Xiaolan Zhang. (2007). Securing the pharmaceutical supply chain using RFID. *Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on*, 23-28.
17. Leedham, C. G., & Sagar, V. K. (1994). Using forensic handwriting analysis techniques to enhance automatic handwritten script recognition and processing. *Handwriting Analysis and Recognition: A European Perspective, IEE European Workshop on*, 2/1-2/3.
18. Watters, P. A., Kuh, D., Latham, S., Shah, I., & Garwood, K. (2009). Enabling access to british birth cohort studies: A secure web interface for the NSHD (SWIFT). *E-Health Networking, Applications and Services, 2009. Healthcom 2009. 11th International Conference on*, 94-100.
19. Yee, G., Korba, L., & Song, R. (2006). Ensuring privacy for e-health services. *Availability, Reliability and Security, 2006. ARES 2006. the First International Conference on*, 8 pp.
20. Fox, Susannah (2004). "Prescription drugs online". Pew Internet & American Life Project. NHS Service Delivery And Organization R&D Program.
21. Feng, G., Dong, K., Hu, D., & Zhang, D. (2004). When faces are combined with palmprints: A Novel biometric fusion strategy. In D. Zhang, & A. K. Jain (Eds.), *Biometric authentication* (pp. 1-10) Springer Berlin / Heidelberg. doi:10.1007/978-3-540-25948-0_95
22. Jia, J., & Cai, L. (2007). Fake finger detection based on time-series fingerprint image analysis. In D. Huang, L. Heutte & M. Loog (Eds.), *Advanced intelligent computing theories and applications. with aspects of theoretical and methodological issues* (pp. 1140-1150) Springer Berlin / Heidelberg.

23. Arandjelovic, O., Hammoud, R., & Cipolla, R. (2006). Multi-sensory face biometric fusion (for personal identification). *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06. Conference on*, 52-52.
24. Kosseim, P., & El Emam, K. (2009). Privacy interests in prescription data, part I: Prescriber privacy. *Security & Privacy, IEEE*, 7(1), 72-76.
25. El Emam, K., & Kosseim, P. (2009). Privacy interests in prescription data, part 2: Patient privacy. *Security & Privacy, IEEE*, 7(2), 75-78.
26. Tagaris, A., Mnimatidis, P., & Koutsouris, D. (2009). Implementation of a prescription fraud detection software using RDBMS tools and ATC coding. *Information Technology and Applications in Biomedicine, 2009. ITAB 2009. 9th International Conference on*, 1-4.
27. Srinivasan, U., Datta, G., Hons, M. S., & Hons, B. E. (2007). Personal health record (PHR) in a talisman: An approach to providing continuity of care in developing countries using existing social customs. *E-Health Networking, Application and Services, 2007 9th International Conference on*, 277-279.
28. Yi Hong, Patrick, T. B., & Gillis, R. (2008). Protection of patient's privacy and data security in E-health services. *BioMedical Engineering and Informatics, 2008. BMEI 2008. International Conference on*, 1 643-647.
29. Al-Nayadi, F., & Abawajy, J. H. (2007). An authorization policy management framework for dynamic medical data sharing. *Intelligent Pervasive Computing, 2007. IPC. the 2007 International Conference on*, 313-318.
30. Chu, S. (2004). ePrescription: Road map from wired to wireless point-of-care order entry. *Enterprise Networking and Computing in Healthcare Industry, 2004. HEALTHCOM 2004. Proceedings. 6th International Workshop on*, 26-33.
31. US pharmacy prescribes fingerprint recognition. (2004). *Biometric Technology Today*, 12(5), 2-3. doi:DOI: 10.1016/S0969-4765(04)00106-7
32. Barbara Wells, Dick E Zoutman, B Douglas Ford, & Assil R Bassili. (2004). Privacy of pharmacy prescription records/The authors respond. *Canadian Medical Association. Journal*, 171(7), 711-2; author reply 712. Retrieved August 17, 2010, from ProQuest Nursing & Allied Health Source. (Document ID: 716581481).