MedCrave
Step into the World of Research

Journal of Psychology and Clinical Psychiatry

Perspective

Open Access
CrossMark

Privacy of communications: faxes are not usually HIPAA compliant. An editorial perspective

Abstract

Privacy of medical and psychological information is of extraordinary importance. In the USA, it is regulated by HIPAA laws. The most common method of communication between health care and mental health practitioners is via faxes. Faxes have changed from the 'paper fax' to electronic faxes ('modern faxes'). There are advantages but numerous potential problems in ensuring compliance with HIPAA. This is even more so when recognizing that faxes are often delivered electronically to emails (electronic mails) which have traditionally been regarded as not complying with HIPAA. Solutions are suggested. The most obvious is delivery of private medical and psychological information by HIPAA compliant secure email. The various options are briefly outlined. Based on direct comparisons, the most logical is to use one that is usable and secure. The ZSentry technology which preceded the well-known blockchain technology fits that requirement because of the secure encryption, date and time stamps and user authentications.

Keywords: authentication, compliance, email, fax, HIPAA, 'modern fax', 'paper fax', privacy, secure electronic mail, security, usability

Volume 10 Issue 6 - 2019

Vernon M Neppe MD, PhD, FRSSAf, DFAPA[1,2,3,i,ii,iii], Ed Gerck PhD[iv,v]

[1]Director, Pacific Neuropsychiatric Institute and Exceptional Creative Achievement Organization, USA
[2]Executive Director and Distinguished Professor, Exceptional Creative Achievement Organization, USA
[3]Adj.Professor, Department of Neurology and Psychiatry, St. Louis University, USA

Correspondence: Vernon M Neppe, Director, Pacific Neuropsychiatric Institute and Exceptional Creative Achievement Organization, Seattle, Washington, USA, Tel 206 527 6289, Email psych@pni.org

Received: December 21, 2019 | **Published:** December 26, 2019

Introduction

The prevailing custom in medical and psychological communications has been to send a fax.

Faxes are currently fundamental to the entire health system, certainly in the USA, where the great majority of practitioners use faxes. Similarly, in 2018, two-thirds of Canadian doctors reported that they primarily used fax machines to communicate with other doctors.[1]

A fax is an image of a document made by electronic scanning and transmitted as data by telecommunication links.[2] The term 'fax' derives from the 1940s and is an abbreviation of facsimile, previously called 'telecopying'. Essentially, faxes apply telephonic transmission of scanned-in printed material (text or images), usually to a telephone number associated with a printer or other output device.[3]

Faxes treat the contents (text or images) as a single fixed graphic image, converting it into a bitmap digital form, for transmission.

Companies that fax often inherently encourage all its customers and suppliers to keep faxing, too. Therefore any changes are necessarily slow.[4]

Many physicians and psychologists don't have the time, expertise or resources to redesign their information workflow, and to eliminate their use of the fax: Major changes would be needed to eliminate faxes.

Practitioners think, wrongly, that faxes—older or modern—protect them. To many, these faxes are still seen as safe and secure. For many mental health practices, faxing continues because it is, convenient and comfortable. Faxes sometimes also have become relatively convenient for short written communications between mental health practitioners.

Faxes can be used in the 'old-fashioned' way: Linked with paper; or (what this author is calling) through the 'modern fax': This involves purely electronic transmissions. Modern faxes are still frequently sent to faxes that use paper so the old-fashioned problems with paper faxes receipt remains important for everyone using faxes.

Data Breach and Mandatory Notification: HIPAA compliance:[5–8]

In the United States, many communications like faxes are influenced by US federal initiatives trying to make medical records systems more compatible.[1] This is largely because of the Health Insurance Portability and Accountability Act (HIPAA). A focus of this article. Then, is to emphasize the United States, but the problem of security of faxes remains universal all the same.

Fax machines can be HIPAA-compliant as long as appropriate security safeguards are followed but the underlying bases are complex and might take time and effort. HIPAA regulations do not prevent covered entities (health providers, plans and clearinghouses that

[i] Vernon M. Neppe MD, PhD, Fellow Royal Society (SAf), DFAPA, DSPE, Pacific N europsychiatric I nstitute, S eattle; a nd E xceptional Creative Achievement Organization (Distinguished Professor) Adjunct Professor, Department of Psychiatry and Behavioral Neuroscience, St Louis University, St Louis. For perspective, Prof. Neppe is a Behavioral Neurologist, Neuropsychiatrist, Neuroscientist, Psychopharmacologist, Forensic specialist, Psychiatrist, Phenomenologist, Neuroscientist, Epileptologist, Consciousness Researcher, Philosopher, Creativity expert, and Dimensional Biopsychophysicist. His CV includes 10+ books, 2 plays, 800+ publications, 1000+ invited lectures and media interactions worldwide (http://www.vernonneppe.org/about.php).

[ii] We acknowledge permission to publish from Brainovoyage.com who holds the copyright over this work. ©. Reproduction of this publication requires written permission the primary author.

[iii] First draft June 2019. Final submission December 2019. This article has gone through numerous peer-reviewers in various forms.

[iv] Ed Gerck PhD is a physicist and cryptographer. He singlehandedly solved the problem of Internet Security with the ZSentry Engine which preceded blockchain technology. He has published in the key books in the area. We are honored that he has accepted co-authorship of this paper.

[v] We greatly acknowledge the feedback of (alphabetically): Dave McGrath and Suzan Wilson.

transmit health information electronically) from faxing Protected Health Information (PHI). However, and this is a big challenge, as the covered entity's is responsible to ensure their fax practices comply with HIPAA privacy rules. These include the 'minimum necessary' rule, which limits information in the fax to the minimum amount necessary in certain instances, as well as the implementation of administrative, technical, and physical security policies to protect PHI.[1]

HIPAA in the United States provides detailed instructions for handling and protecting a patient's personal health information. HIPAA was developed in 1996 and became part of the 'Social Security Act'. The primary purpose of the HIPAA rules is to protect the privacy of health care coverage for individuals who lose or change their jobs.

In effect, there are four main purposes of HIPAA[9]

1. Privacy of health information (PHI).
2. Security of electronic records.
3. Administrative simplification.
4. Insurance portability.

The cost for doing business online has increased greatly in the USA. Audits and fines for HIPAA and HITECH regulatory compliance faults can result in enormous fines in the thousands of dollars and beyond. It affects health-care providers plus all business because they all handle protected health information (PHI). Data breach notification is legally mandated by U.S. State Security Breach Notification Laws. The penalties for willful neglect are increased under the HIPAA HITECH Act. These HIPAA violation penalties can extend up to $250,000, with repeat/uncorrected violations extending up to $1.5 million. Under certain conditions, HIPAA's civil and criminal penalties now extend to 'business associates'.

US federal initiatives are trying to make medical records systems more compatible, and controlled at the 'Centers for Medicare and Medicaid Services' (CMS).[1] These HIPAA regulations do not prevent covered entities (health providers, plans and clearinghouses that transmit health information electronically) from faxing Protected Health Information (PHI). HIPAA is therefore of critical importance to Psychologists and Psychiatrists. This is because privacy is important and so is confidentiality of medical, psychological, and other day to day records like banking (Table 1).

Table 1 2019 Interpretation of the HITECT ACT's Penalties for HIPAA Violations.[10]

Penalty Tier	Level of Culpability	Minimum Penalty per Violation	Maximum Penalty per Violation	Old Maximum Annual Penalty	New Maximum Annual Penalty
1	No Knowledge	$100	$50,000	$1,500,000	$25,000
2	Reasonable Cause	$1,000	$50,000	$1,500,000	$100,000
3	Willful Neglect – Corrective Action Taken	$10,000	$50,000	$1,500,000	$250,000
4	Willful Neglect – No Corrective Action Taken	$50,000	$50,000	$1,500,000	$1,500,000

Direct HIPAA Problems of paper linked faxes

1. Pages are at a higher risk of compromising privacy e.g., often misplaced.
2. Manual signatures can be copied.
3. Paper fax is less accessible to staff who travel or work remotely. This may lead to using fax systems that are not private.
4. Fax machines in offices may sit open and accessible to a wide range of individuals in many healthcare settings: That is HIPAA non-compliant. This applies to incoming faxes sitting on publicly available fax machines and also information to be faxed.
5. The cover sheet must not include PHI.
6. Faxes can go anywhere, and can be received in printed form in a front office desk and be read by anyone.
7. Sometimes the cover page might state: "If you are not the named person in the cover page receiving this fax, please destroy and do not look at this". This may partly condone but how legitimate would this be if it fell to the wrong person?
8. To be HIPAA compliant, faxes require all machines to not retain the memory so that these cannot be contained for easy retrieval. This is a great problem though seldom applied. It can be done but is specialized.

Problems of paper linked faxes: Not direct HIPAA problems

a. Inefficiency of the work force in delivery, receipt and checking: Time and labor is considerable. 11. Faxing is not cheaper. Multiple faxes take a long time.

b. The staff must be responsible too.

c. Time is wasted by employees ensuring privacy.

d. Sending of multiple faxes is stepwise. Again time is wasted and push up employee costs.

e. Poor document workflow

f. When faxing protected documents, never leave the machine until the transmission is complete and call the recipient to ensure that their fax machine is in a protected location and out of the public's line of sight. Incoming faxes cannot be in publicly available fax areas. Remedy: Never leave the machine until the transmission of protected documents is complete and call the recipient to ensure that their fax machine is in a protected location and out of the public's line of sight. 11. That is a hassle.

g. Faxes can be read by staff-members and often go to open areas in an office. The same applies for letters and voice mails.

h. With HIPAA laws, the assumption is that faxes are anything but secure. Indeed, there is, unfortunately, little that is truly HIPAA compliant.

Solutions for paper-linked faxes

a. Clearly any faxes or devices must be located in secure, non--public areas to prevent unauthorized personnel from viewing faxes.

b. A Business Associate Agreement in which case the recipient may technically be more to blame than the sender. All employees must have signed such an agreement.

c. Fax PHI must be received in printed form in a doctor's desk and be read by anyone.

d. Always use cover pages and send appropriately and check.

The 'modern' fax might help with security, but still how is the information encrypted?

The 'modern fax' era

Despite the fax *machine* gradually becoming obsolete technology superseded by computer networks, the irony is that 'modern' faxing appears to be actually growing in popularity.

The modern fax (now far more popular in the USA than before) has been used more commonly over the past few years. It still fundamentally involves a phone line and transmission as a 'pict'—an image. But conveniently and in seconds, like a phone call, faxes can be sent simultaneously to many individuals and also broadcast a fax to multiple addresses. 'Modern faxes' being electronic alone no longer require fax machines. We can now send and receive faxes online, no matter where we are. Electronic Faxes require no hardware or software and is mobile on one's computer.

A major breakthrough in the development of the modern facsimile system was the result of digital technology, where the analog signal from scanners was digitized and then compressed, resulting in the ability to transmit high rates of data across standard phone lines with resolutions varying from as little as 150 DPI to 9600 DPI or more.[3] Moreover, even dedicated fax modems have been technologically superseded.

One technique is 'Fax Over IP' (FoIP). This can transmit and receive pre-digitized documents at near real-time speeds. Scanned documents are limited to the amount of time the user takes to load the document in a scanner and for the device to process a digital file. If done manually, this can be time consuming and require extra labor and checking. Nevertheless, automation helps this making the process take a few seconds only.[3]

Everything today is automated: Just type in the number, drag and drop the files to be faxed, and hit Send. The web interface is easy to understand and works flawlessly. We can now send faxes from anywhere (with a WIFI connection). We easily edit our custom cover pages to include logo and contact information which then is automatically included.

The Internet now allows new and cheaper ways to send faxes in some cases.

In many corporate environments, free-standing fax machines have been replaced by fax servers and other computerized systems capable of receiving and storing incoming faxes electronically, and then routing them to users on paper or via an email (which may be secured). Such systems have the advantage of reducing costs by eliminating unnecessary printouts and reducing the number of inbound analog phone lines needed by an office. 12 Remotely hosted fax-server services are widely available from Voice-over IP and email providers allowing users to send and receive faxes using their existing email accounts without the need for any hardware or dedicated fax lines. Personal computers have also long been able to handle incoming and outgoing faxes using analog modems or internet connections eliminating the need for a stand-alone fax machine.[1]

A number of free and commercial companies provide arrangements for using the Internet rather than the public telephone system for most or part of the path to the fax point. The receiving fax machine or fax outputs and inputs electronically reconvert the coded image. Even if a document is text only, it is treated by the computer as a scanned image and is transmitted to the receiver as a bitmap. Faxing a message online works well if the recipient wants only to read the message. Sending documents that require modification through email is more efficient but has new privacy issues (as below).

Nevertheless, the problems with paper faxes and fax machines still apply to sending 'modern faxes' because we don't know what technology the recipients of our faxes have.

Ironically, faxes now have the same problems as with electronic mail (email) , possibly sometimes even worse. This is because 'modern' faxes are sometimes are received in individuals emails. *Therefore, almost every HIPAA critique in emails now applies to modern faxes*.

There is certainly a recognized lack of confidentiality in regular email, which is insecure and can be intercepted by hackers with some difficulty. Additionally, there are problems such as identity theft (e.g. phishing / spoofing), spamming, and easy transmission of viruses.

However, bizarrely *the myth that faxes are HIPAA-compliant remains. Regular emails are not regarded as HIPAA compliant and are not, but because faxes commonly end up in emails, the faxes are now logically even less compliant than emails*.

True fax HIPAA compliance is possible, but is rare because many factors play into this. It means there has to be layers of security going out and being received and in transmission and in maintenance.

Problems with the more modern faxes and styles

Practitioners should not innocently open patients up to potential identity theft and fraud: This is also a fineable offense by HIPAA.

Here are obvious examples in the 'modern' fax of potential HIPAA problems.

a. When a company advertises "Lifetime fax storage", how are they storing the faxes in a HIPAA compliant way? Unless they use technologies that scramble them that would be very difficult, indeed and how do you scramble electronic images such that they cannot be hacked? That technology is very sophisticated and available usually only in specific secure technologies.

b. Faxes in any event, at times, can be e-faxed, and are therefore sent by non-HIPAA-compliant email. And if it arrives at an email address, then, as indicated, the problems of HIPAA compliant emails are relevant.

c. Email might therefore be relatively better than faxes because at least it will go to specific individuals, although those emails might be directed to several by one common email address, and are less likely to be on someone's desk in full view of all. Of course, though regular email is not HIPAA compliant, with some faxes redirecting to the email the emails they are often relatively more compliant than faxes.

d. The recipient's fax number may be erroneous or misdialed or even discontinued so that the fax reaches the wrong individuals. Fax numbers that are wrong are possible HIPAA violations. The senders may receive confirmation from their machine or server: "The fax was successfully delivered." But they might remain unaware of their potentially serious HIPAA error of incorrect delivery.

e. It's a HIPAA violation, even if the sender sends a message saying something akin to 'please disregard if sent to the incorrect recipient.' Of course, sending emails to the wrong recipient is another reason for non-compliance with HIPAA.

f. Often the recipient prints a paper copy of the document. Even that is fraught with HIPAA danger. Where is it received? Who has access to it?

g. Adding to this is keeping an accurate HIPAA audit trail of every activity that occurred.[13] The problem here is that others can access that trail and it will appear on one's computer unless encrypted. Question: How often do practitioners even encrypt their computers?

h. HIPAA requirements require a cover sheet with the approved HIPAA statement when transmitting PHI.[14]

i. Healthcare data breaches or theft of unsecured and unencrypted patient information on portable media like laptops, notebooks, and removable drives and also old computers can occur when they are trashed. Not only does this open patients up to potential identity theft and fraud, but this is also a fineable offense by HIPAA.[13]

Solutions for the 'modern' faxes

Practitioners should ensure compliance.[13]

'Cloud faxing' has become a solution which some believe is adequate. It is done automatically, with encryption being used. *Practitioners should ensure their cloud fax services encrypt all documents and allow enhancements from inside their secure data center, rather than on their device*.[11] However, though cloud faxing may be claimed to be adequate, the authors point out that this is simply not possible that it is end-to-end secure. This makes Cloud Faxing easily open to MITM (so-called "man-in-the-middle") attacks. The ZSentry technology solves this: ZSentry users have sole control of their own passwords by storing a unique cryptographic hash on a blockchain and allowing companies to confirm it for login.[6]

Some practitioners sign a 'business associate's agreement' (BAA) but they are not required to do so. But if they do, it lowers the fax-senders' risk. The HIPAA Privacy Rule requires all Covered Entities to have a signed Business Associate Agreement (BAA) with any Business Associate (BA) they hire or who may come in contact with PHI. Covered entities include physicians, health insurance, health plans and associated professionals. But they do not require a BAA between each other.[14] BAAs, however, may protect the companies with the BAA and potentially make the other side more vulnerable to HIPAA penalties as a consequence.

a. The HIPAA Omnibus Rule changed how BAs and Business Associate Subcontractors (BAS) can be held liable for potential HIPAA violations. 14 One change is the fines are less for violations.

b. Has the office performed checks for malicious software?

c. Hacking is another related problem.

d. These have the capability to remote wipe and disable a device that holds PHI .

e. Be aware of all PHI stored on local devices.

Solutions

There must be a robust process in place for password creation and password changes in place

a. There must be a have a complete inventory of all covered entities and business associates available.[13]

b. Providers must be able to prove that their organization has implemented policies and procedures to protect PHI from improper alteration or destruction.

c. Providers must show that their organization maintain an accurate inventory of information system assets, including mobile devices. They must:

d. Ensure that appropriate business associate agreements have been executed

e. provide evidence that the workforce has received HIPAA training

f. Conduct a 'self-audit' to check how well policies and procedures are being carried out throughout the organization.[11]

g. After faxing something, practitioners should check and document receipt.

h. They should consider using secure email technologies such as Zsentry.com which are automatically date and time stamped,

[vi] The reception and transmission of fax present several points for unfettered access (e.g., cache, hard drive, transmission to other sites, future sales, and so on) that the sender does not know or cannot control, or verify. The service providers can read anything that is sent in the fax. This involves technically a MITM attack where the attacker theoretically can secretly relay and possibly alter the communications between two parties who believe that they are directly communicating with each other. Such MITMs bypass encryption fully without the sender or recipient becoming aware of it. Thus, "cloud fax services" cannot be made secure even if the receiver only accepts encrypted faxes electronically. The process is Sender --> encryption:fax receiver -- decryption (storage, future sales, etc) -- encryption:transmission --> Receiver.

unmodifiable in message and have automated receipt. That also applies to other professions like law and banking. In this regard, faxes do not generally have automatically authenticated time and date recordings or authentications relating to the correct receipt, although the read-out might indicate the time and phone number. Also the faxes are modifiable as the pages can be replaced.

Advantages of faxes over emails

Strangely, an advantage of fax machines and multifunctional printers with a fax capability is they provide an inexpensive backup capability in case of technical problems with an Internet connection, or even a cyberattack, like the Russian attack on Estonia in 2007.[4]

In some countries, electronic signatures on contracts are not yet recognized by law, yet faxed contracts with copies of signatures are, fax machines enjoy continuing support in business.

Nevertheless, fax technology has faced increasing competition from Internet-based alternatives.

Changes are coming

This is not only the USA. In 2018, urged partly by the European Union's promotion of electronic identification, the British Law Commission concluded that electronic signatures were indeed legal but needed significant promotion to increase their acceptance and use.

In December, the National Health Service decided to stop buying fax machines in 2019 and end their use by the end of 2020. That's the same goal the Centers for Medicare and Medicaid Services' (CMS) has for American doctors to stop faxing.

Obvious disadvantages of regular email

As indicated, because faxes are often now directed to emails, the email difficulties amplify the fax non-compliance.

Because faxes are now often received as electronic emails, the following applies:

Regular email is similar to a postcard that anyone can read and even overwrite. Therefore, regular email communication is not a secure method of communication, for various reasons.[5,6,15]

For example:

a. Anyone can send a regular email using a false name and email address;

b. Any regular email that is sent to you or by you may be copied, changed, and held by various computers it passes through as it goes from the sender to you or vice versa;

c. Persons not participating in your regular email communications may intercept your communications by improperly accessing your computer or the sender's computers or even some computer unconnected to either of you which the email passes through.

But the lack of security in regular email is not limited to transmission exploits.

a. Regular email that is stored, even temporarily, in online servers or clients is vulnerable to a wide range of attacks, with external and internal sources that may also be exploited in combination. This is caused by hackers, automatic password crackers, virus, worms, buffer-overflow, software bugs, zero-day-exploits, delayed patching, patch conflicts, security gaps, collusion, conflicting business interests, lack of legal protection for data at rest, and other security breach reasons that plague not only Internet servers and even off-line machines but also users' desktops, laptops, and cell phones.

b. These exploits can cause additional problems, such as impersonation, —identity-theft, scams, and financial losses and in the medical field particularly, invasion of privacy in an otherwise trusted situation

c. Private data in regular email can be compromised in improper file access by a service provider employee or by their contractors, in an overly broad legal discovery processes, and in government-mandated broad surveillance, any of which can be rather easy to perform unilaterally in some jurisdictions.

d. An email sent to a server abroad, even if just for processing purposes (e.g., spam or virus detection) and as such is unknown to a sender and recipient who are both local and trust their local protection laws, is subject to compromise risks also in the foreign jurisdiction.

e. Online email services such as Gmail™ up the ante on the already large —and growing— Internet risk by using a multi-tenant architecture called Software-as-a-Service (SaaS).

Alternative solutions

The alternative is to send HIPAA-compliant emails: There are, in fact, several different technological engines that provide compliant, secure responses.[8] Applying objective criteria, the ZSentry engine appears best.[8,15] ZSentry email is the most sophisticated and might be the first that provided both security and ease of use.[7] There are three other different fundamental engines that provide different levels of this -- PGP is one common example (Pretty Good Privacy) was the first released in 1991 and later followed by an S/MIME extension. PKI (Public Key Infrastructure, based on the X509).

ZSentry (ZS) provides per-message encryption, de-identification, two-factor authentication, control, auditing, data loss protection, secure archive and other services protecting information in transit and at rest. ZSentry supports the other main security technologies (PKI, PGP with later S/Mime) and one open (universal) choice. There is also IBE (Identity-Based Encryption, also marketed as Voltage and MessageGuard) because its design requires 'key escrow'.[6,8]

The most obvious example, then, of secure and usable email is Zmail. This far eclipses faxes, is a light-year ahead of regular email, and appears to be better than the other engines.[5–8]

Based on the available objective measures, prior to ZSentry being used , ease of use was problematic when there was great security, and vice versa, good usability and lesser absolute security.[158]

[vii] The principal author was able to consult over years on this technology and has invested in it. See Zsentry.com. However, he has particularly recognized the value of the ZSentry technological engine because it was developed after the others, and appears to be the only technology that is both usable and secure. It is certified in that regard by the Federal Government in research and has been used also to run many elections including nationally in Sweden.

[viii] ZSentry transactions are not just secure, they can be trusted. Since a 2001 USPTO patent application asserting prior art, and with ZSentry in 2004. The storing of a unique cryptographic hash on a blockchain and allowing companies to confirm it for login makes ZSentry unique and even more secure than the competing technological engines. This means that users are exclusively in control of their own login and their data. There are no copies of passwords or data elsewhere, not even in the blockchain. Users do not have to trust the online service ZSentry on login, just their choice of identity management tools and themselves. Yet ZSentry remains usable.[15]

Nevertheless, often, secure emails are major hassles because people have to register and put in particular passwords which may or may not be readable. The situation is still not perfect in that continual changes to browsers and operating systems, makes for certain character symbols to be distorted (e.g. apostrophes so 'I'm' should be written 'I am'). All these technological engines have costs associated and have attempted to make the limitations as few as possible. For example, Zsentry can be set up so one can use it from one's regular email client, or from a browser such as Internet Explorer, Google, Chrome or Safari or all the common ones. It will be received as quickly as regular email. However, sometimes, companies perceive these secure emails as Spam or junk mail or the ZSentry mail is blocked by Firewalls. So this is not perfect.

Eventually, the older generation of people more comfortable with faxing than emailing will retire. Until then, however, fax machines will continue. At that point, secure email technologies should take over. They're logical to implement in hospitals and clinics, particularly.

Funding

None.

Acknowledgements

None.

Conflicts of interests

The authors have no conflicts of interest to declare.

References

1. Coopersmith J. Faxed: The Rise and fall of the Fax Machine Baltimore, MD: Johns Hopkins University Press; 2015.
2. Stevenson A, Lindberg CA. New Oxford American Dictionary. 3rd ed. UK: Oxford University Press; 2015.
3. Rouse M. Fax. 2006.
4. Coopersmith J. Why do people still use fax machines? 2019.
5. Gerck ENV. Red flags in email security. 2010.
6. Gerck E. Cryptography Options: ZS, PKI, PGP and Universal. 2019.
7. Gerck E. Fax/Scanner/Voicemail. HIPAA & Safe Harbor compliant. 2019.
8. Gerck E, Neppe VM. The hazards of internet security and the methods of peace: A paradigm change and a solution. *Telicom*. 2010;23:38–47.
9. Bowers D. The Health Insurance Portability and Accountability Act: is it really all that bad? *Proc (Bayl Univ Med Cent)*. 2001;14(4):347–348.
10. HHS Changes HITECH Act Penalties for HIPAA Violations. *HIPAA Journal*. 2019.
11. Li Y. The slow disappearance of the fax machine in healthcare. 2014.
12. Fax. 2019.
13. Phase 2 HIPAA Audit Checklist. 2015.
14. Business Associate Agreement: everything explained. 2019.
15. Neppe VM. The email security-usability dichotomy: Necessary antinomy or potential synergism? Telicom. 2008;21:315–31.

Citation: Vernon MNMD, FRSSAf, DFAPA, et al. Privacy of communications: faxes are not usually HIPAA compliant. An editorial perspective. *J Psychol Clin Psychiatry.* 2019;10(6):249–254. DOI: 10.15406/jpcpy.2019.10.00661