ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 3, pp: (41-52), Month: July - September 2018, Available at: www.researchpublish.com

USING INFORMATION TECHNOLOGY AS A TOOL FOR PROTECTING PATIENTS MEDICAL RECORDS IN HEALTH MANAGEMENT SYSTEM: A CASE STUDY OF PROSTATE CANCER

[1]DR. NATHANIEL OJEKUDO, [2]EGBA IFEANYICHUKWU

[1]Head of Department, Department Of Computer Sciences, Faculty of Natural and Applied Sciences, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Rivers State
[2]Head of Computer Unit, School of Foundation Studies, Rivers State College Of Health Science and Technology, Port Harcourt. Rivers State

Abstract: **Prostate cancer is now known as one of the most standout amongst the well-known tumors in men and the worldwide weight of this malady is rising. Lifestyle alterations like smoking discontinuance, weight control and exercise provides chances to diminish the danger of creating prostate growth. The influxes of computerizing medicinal records in the healthcare industry have seen drastic changes. While the healthcare industry tackles approaches to avert prostate disease, security and protection of data issues are the focal point now as developing vulnerabilities and dangers keep on growing. This paper tries to identify the best in class data security, integrity and protection issues as applies to the prevention of prostate cancer amongst men in healthcare, industry. It also recognized different manners by which healthcare data can be ensured as well as computerized privacy measures which are connected to prevent unapproved access to databases, PCs and sites.**

Keywords: **Prostate cancer, healthcare industry, prostate disease.**

1. INTRODUCTION

Owing to the ever- expanding cost for medicinal services and premiums for expanded health care coverage, there is always requirement for a proactive desired healthcare and wellbeing. The new trend of digitizing medicinal records have caused a change in the world of healthcare ranging from responsive to a healthcare that is proactive which can result in an overall healthcare costs decrease and eventually lead to economic growth. As healthcare specialists search for each conceivable method to bring down expenses while enhancing care process, conveyance and administration, data security and integrity develops as a conceivable arrangement with the guarantee to change the medicinal services industry. The Security as well as the protection issues are the focal points now as rising dangers and vulnerabilities keep on growing in medicinal services conveyance delivery (IEEE Big Data Congress, 2014).

There have been issues relating to data breaches in health care which which incorporate cases in which criminal programmers take ensured wellbeing data to carry out restorative wholesale fraud, or occurrences when a worker sees the records of one patient without approval. Data security can be exorbitant for suppliers notwithstanding potential HIPAA fines and other compliance costs, heathcare facilities may endure reputational harm and lost patient trust (IEEE Big Data Congress, 2014).

However all healthcare facilities and other health service organizations should be watchful about ensuring touchy patient, money related and other information. Doing as such requires a blend of worker training, keen utilization of technological innovations and physical security for structures or buildings.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 3, pp: (41-52), Month: July - September 2018, Available at: www.researchpublish.com

Security of data is additionally vital as long as health care records is concern, so that wellbeing promoters and medical specialists in the U.S. even many nations are seriously progressing toward executing of security and privacy for electronic medicinal record (EMR), by creating awareness about patient rights identified with the arrival of data to laboratories and research centers, physicians, healing centers and other therapeutic offices (Techopedia, 2018).

The core segment of a data is *data integrity*. Data integrity viewing from itss broadest utilize refers to consistency and accuracy of information put away in a database, data warehouse, data mart or other build. It can be utilized to depict a capacity, a state, or a procedure and its regularly used as an intermediary for data quality. Data with "integrity" is said to have an entire or a whole structure. All the data qualities must be correct which includes its definitions, dates, business rules genealogy and relations for the information to be complete. Data integrity is forced inside a database when it is outlined or designed and is verified through the continuous utilization of oversight checking and validation routines or endorsed schedules (Michael, 2018).

Aims of the Paper:

This paper is aimed at revealing and identifying the art of data security, integrity and privacy issues as applies to the prevention of prostate cancer amongst men in healthcare industry.

It also identifies the Information's about the prostate gland and its cancer and how they can be secured and at the same time made available to men who are susceptible to developing the disease. The information so secured will then be stored in the cloud for access by health care providers, caregivers and the general populace. The reason is to have a uniform preventive measures and treatment as it concerns prostate cancer.

2. REVIEW OF RELATED LITERATURE

The Prostate:

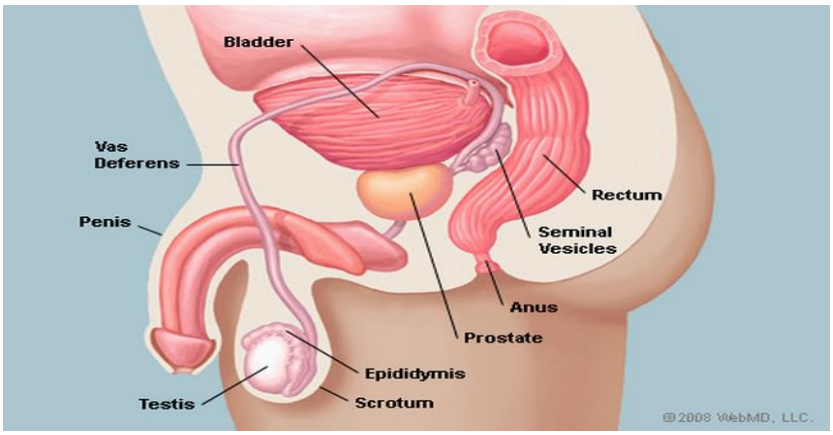


Figure 1: The Prostate Showing its Gland and Associated Structures (Source; WebMD, 2018)

The prostate is a compound tubuloalveolar exocrine organ of the male reproductive system in many well evolved creatures (Wikipedia, 2018). It contrasts extensively among species anatomically, physiologically and. chemically or artificially. It has capacity to discharge a marginally milky alkaline fluid, white in appearance, that generally make up about 30% of the volume of the semen in humans alongside seminal vesicle liquid and spermatozoa.

The Semen created is generally made up of alkaline with the emissions from other contributing organs, which includes in any event, the fundamental vesicle liquid (Wikipedia, 2018). The acidity of the tract of the vaginal is killed or neutralize by the helps of the alkaline nature of the semen, delaying the life expectancy of sperm. In the first ejaculate fractions,the prostatic liquid is removed alongside with a large portion the spermatozoa. In examination of the few spermatozoa removed together with primarily original vesicular liquid, those expelled in the prostatic fluid have better assurance , better motility and longer survival of the hereditary material.

In the midst of male seminal emission, It regulates male sexual function whereby sperm is transmitted from the vas deferens into the male urethra through the ejaculatory channels, that exist in the prostate organ. It is exclusively through incitement of the prostate organ that makes it workable for a few men to accomplish orgasm, for example, prostate massage or anal intercourse (goaskalice.columbia.edu, 2002; Rosentha, 2012; Komisaruk et al., 2009).

Prostatic discharges are for the most part made out of simple sugars and are frequently marginally alkaline (Alan et al., 2015). The Prostatic discharges protein content in human, is under 1% and incorporates proteolytic chemicals, beta-microseminoprotein prostatic, corrosive phosphatase, and prostate-particular antigen. The emissions likewise contain zinc with a 500–1,000 concentration times the concentration in the blood.

The prostate controls and regulates the male hormones (androgens), this is with the goal for it to work appropriately. The male hormones are in charge of male sex attributes. The testosterone is the male primary hormone which is made generally by the gonads. It is a metabolite of testosterone called dihydrotestosterone (DHT), that prevalently controls the prostate.

In every human cells, out of the 20,000 protein coding qualities (genes) communicated, almost 75% of these genes are communicated in the ordinary prostate (Proteinatlas, 2017; Uhlén et al., 2015). About 150 of these qualities are all the more particularly communicated in the prostate with around 20 qualities being very prostate particular (O'Hurley et al., 2015).

The Prostate Cancer:

Prostate growth (cancer) is known to be a standout amongst the most widely recognized tumors in men and the worldwide weight of this infection is rising. Lifestyle alterations like smoking discontinuance, weight control and exercise offer chances to diminish the danger of creating prostate growth. It is amongst the most common tumor in men and its incidence is on a continues rise in many countries (Ferlay et al., 2008). Screening for early prostate tumor and its management is a standout amongst the controversial and most difficult issues as found in all of medicine.

Testing for Prostate:

The following are the various ways in which prostate can be tested: (WebMD, 2018).

- **Digital Rectal Examination (DRE):** In this method the specialist embeds a gloved finger greased up into the rectum and then feels the prostate. A DRE can sometimes recognize an amplified lumps or handles of a prostate tumor, or the delicacy from prostatitis.
- **Prostate-Specific Antigen (PSA):** Here the prostate produces a protein called PSA, which can be estimated by a blood test. If off chance PSA is high, tumor is usually more probable, however a high PSA can likewise be caused by an amplified prostate.
- **Prostate Ultrasound (Transrectal Ultrasound):** This is done through an ultrasound test which is embedded into the rectum, and then it is brought near the prostate. Ultrasound is frequently done with a biopsy to probe for prostate tumor.
- **Prostate Biopsy:** This is another method for testing for prostate. A needle is implanted into the prostate to collect tissue out to check if there is prostate tumor. This is typically done from the rectum.

Treatments of Prostate:

The prostate treatment fall under the following categories:

- **The use of Alpha-Blockers:** The Alpha-blockers do relax the muscles about the urethra in men with side effects of a developed prostate. Urine at that point flows more freely.

The Use of 5-Alpha Reductase Inhibitors: These decrease the level of a specific type of (DHT). The prostate shrinks when small DHT is available, enhancing the flow of urine.

- **Through Surgery:** Usually, medications settle indications of a developed prostate, yet a few men expect surgery to enhance side effects and avert complications (WebMD, 2018).

Data Security:

Data security is an essential aspect of IT for organizations of any size and sort. Its innovative unrest measure is encryption, the place where digital data, hardware/software, and unreliable drives are usually encrypted and also consequently rendered unreadable to unapproved users and hackers. With proper authentication, users must provide a password, biometric information, code, or other types of data to check personality character/identity before access to information or framework/system is allowed.

Data security refers to as a defensive as well as a computerized protection measures that connect to forestall unapproved access to PCs, databases and sites. **Additionally it also shields information from** debasement. Data security is otherwise known as Information security (IS) or as PC security.

It is concerns the insurance of information from coincidental or deliberate however unapproved alteration, demolition or revelation using administrative/ authoritative controls, physical security, logical controls, and also different protections to hinder accessibility.

Methods for securing your data may include:

- **Data Encryption:** changing the data into a unique code so that anyone without the key that unlocks it can't effectively read it.
- **Data Masking:** Some territories of the data is masked thus staff that hasn't the authorization can't take a gander at it.
- **Data Erasure**: guaranteeing that no more utilized information is totally uprooted and can't be recovered by unapproved individuals.
- **Data Backup**: making duplicates of data for easy recovery in case the original copy is lost.

General Best Practices to Secure Healthcare Data:

Clinics and other human services organizations should be watchful about securing delicate patient , financial and information. Doing as such requires a blend of worker instruction, smart utilization of innovation and physical security for buildings. The accompanying is a rundown of ten essential best prescribed procedure/ practices for healthcare data security: (HealthcareBusinessTech., 2016).

1. **Protecting of the Network:**

Since hackers have now developed somany techniques to breaking into the systems of healthcare organizations', healthcare IT departments and offices need to make use assortment of apparatuses to keep them out always. In most cases, lots of firms excessively spend on perimeter security, ie firewalls , antivirus softwares etc while experts caution that they ought to also be embracing innovations/technologies that helps limit the damage if assaults happen, as this incorporates procedures. for instance, isolating systems or a networks with the goal that an intruder into one zone do not approach every other information stored all other zones of the organization.

2. **Educating Staff Members:**

Whether because of carelessness or malicious activities, workers are frequently associated with healthcare information breaks/ breaches. Accordingly, any IT security program ought to incorporate a major spotlight on worker training, which may include:

- Training the staff to know what does and doesn't cause infringement to HIPAA.
- Organizing Lectures on abstaining from social engineering, phishing and other attacks whose objective targets the workers, and
- Advice based on picking strong passwords.

3. **Encryption of portable devices**

As of previous couple of years past, a few information breaches happened in light of the fact that a portable computing or capacity gadget containing ensured wellbeing data was lost or stolen. One thing medicinal institutions ought to dependably do is to prevent those breaks by encrypting all gadgets that may handle patient data, which includs workstations, tablets, cell phones and versatile USB drives. Notwithstanding to ensure encrypted gadgets is providing to workers, it's imperative to put strict arrangements that will be against conveying information on a decoded individual gadget.

4. **Secure wireless networks**

Progressively,organizations now depends on remote routers for its office systems. But shockingly, these remote systems frequently present security loop holes through which data can be stolen by hacking those systems from the parking garage, for instance, particularly if the association depends on obsolete innovation.

5. Implementation of Physical Security Controls:

Indeed, even as EHR turn out to be more common, great deal of some sensitive/touchy information is still keep on paper by some organizations. Therefore, suppliers should ensure entryways and file organizers/cabinets are bolted and the utilization of cameras and other physical security controls. Also, there should be a physically secured IT equipment by organizations by locking of the server rooms and the utilization of cable locks or different gadgets in other to keep workstations connected to office furniture.

6. Writing of a Mobile Device Policy:

Individual gadgets are utilized by healthcare services representatives to enable them do their work; therefore it's vital that each association developes a cell phone policy to governs what information to be stored on those devices, and what applications might be also installed, etc. Numerous suppliers are making use of cell phone administration (MDM) software to authorize those arrangements/ policies.

7. Delete Unnecessary Data:

Numerous casualties of information breach have discovered that the more data that is held by an organization, the more hoodlums there to steal. Organizations is supposed to have an arrangement that orders the erasure of patient and any other data that is never required again. It also pays to consistently review the data to be stored, so that the organization understands what's there and can also distinguish what should be erased.

8. Vetting of Third Parties' Security:

Alongside mobile devices, the greatest of IT trend in previous couple of years has been the likely rise of cloud computing. Cloud-based computing has empowered smaller organizations so as to exploit a significant number of the same advancements or technologies as their bigger rivals by bringing down the up-front costs that is vital for deployment. Moreover, placing in the hands of third parties data, additionally makes various new dangers. Therefore, it's vital for organizations to vet the security of distributed computing merchants diligently and other outsiders they make contract with.

9. Patching Electronic Medical Devices:

As huge numbers of the IT security dangers medicinal services institutions confront also has influence on industries and companies. Therefore providers have another risk which is the threat of pacemakers, observing devices and also other electronic restorative gadgets being hacked.

Healthcare IT offices and departments must guarantee that the softwares on those gadgets are keep up to date and also patched to limit them being vulnerable.

While colossal quantities of the IT security perils therapeutic administrations associations stand up to likewise impact organizations and different businesses, suppliers have another hazard: the danger of pacemakers, watching gadgets and other electronic helpful devices being hacked.

Human services IT workplaces and offices must ensure that they keep the product on those contraptions fixed and cutting-edge to constrain their vulnerabilities.

While goliath amounts of the IT security risks remedial organizations affiliations face similarly affect associations and diverse organizations, providers have another peril: the threat of pacemakers, watching devices and other electronic accommodating gadgets being hacked.

Human administrations IT work environments and workplaces must guarantee that they keep the item on those contraptions settled and bleeding edge to oblige their vulnerabilities.

10. Having a Response Plan for Data-Breach:

It is impossible for an organization to ever have the capacity to keep each conceivable IT security occurrence. Which is the reason it's basic building up an arrangement of activity for when a breach does occur (HealthcareBusinessTech., 2016).

3. HEALTHCARE DATA SECURITY IN THE PREVENTION OF PROSTATE CANCER AMONGST MEN

Healthcare cyber security is aimed at keeping pace with the evolving threat and addressing threats to privacy and data protection on endpoints and in the cloud, and safeguarding data while it's in transit, at rest, and in use, which requires a multi-faceted, sophisticated approach to security. It can be done through the following ways: (HealthcareBusiness Tech.com, 2016).

1. Educating the Healthcare Staff:

This is carried out through security awareness training which equips healthcare employees with the requisite knowledge necessary for making smart decisions and using appropriate caution when handling patient data. This is because human element remains one of the biggest threats to security across all industries, but particularly in the healthcare field. Simple human error or negligence can result in disastrous and expensive consequences for healthcare organizations.

2. Restriction of Access to Data and Applications:

This has to do with restricting access to patient information and certain applications to only those users who require access to perform their jobs. However access restrictions require user authentication, ensuring that only authorized users have access to protected data. The Multi-factor authentication is a recommended approach, requiring users to validate that they are in fact the person authorized to access certain data and applications using two or more validation methods such as:

- The use of a password or PIN number; information possessed by the patient,
- A card or key (Something that only the authorized user would possess, and
- The use of biometrics (facial recognition, fingerprints, eye scanning) which is something unique to the authorized user.

3. Implementation of Data Usage Controls:

Healthcare organizations can use data controls to block specific actions involving sensitive data, such as web uploads, unauthorized email sends, copying to external drives, or printing. This is done to ensure that risky or malicious data activity can be flagged and/or blocked in real time. Data discovery and classification play an important supporting role in this process by ensuring that sensitive data can be identified and tagged to receive the proper level of protection.

4. Log and Monitor Use:

This is to enable providers and business associates to monitor which users are accessing what information, applications, and other resources, when, and from what devices and locations. These logs prove valuable for auditing purposes, helping organizations identify areas of concern and strengthen protective measures when necessary. When an incident occurs, an audit trail may enable organizations to pinpoint precise entry points, determine the cause, and evaluate damages.

5. By Encrypting Data at Rest and in Transit:

This is one of the most useful data protection methods for healthcare organizations. By encrypting data in transit and at rest, healthcare providers and business associates make it more difficult (ideally impossible) for attackers to decipher patient information even if they gain access to the data. HIPAA offers recommendations but doesn't specifically require healthcare organizations to implement data encryption measures; instead, the rule leaves it up to healthcare providers and business associates to determine what encryption methods and other measures are necessary or appropriate given the organization's workflow and other needs.

6. Securing of Mobile Devices:

Mobile devices are utilized by healthcare providers in the course of doing business, whether it's a physician using a smart phone to access information to help them treat a patient or an administrative worker processing insurance claims. Mobile device security alone entails a multitude of security measures, including:

- Managing all devices, settings, and configurations
- Enforcing the use of strong passwords
- Enabling the ability to remotely wipe and lock lost or stolen devices

- Encrypting application data
- Monitoring email accounts and attachments to prevent malware infections or unauthorized data infiltration
- Educating users on mobile device security best practices
- Implementing guidelines or white listing policies to ensure that only applications meeting pre-defined criteria or having been pre-vetted can be installed
- Requiring users to keep their devices updated with the latest operating system and application updates
- Requiring the installation of mobile security software, such as mobile device management solutions

7. Mitigate Connected Device Risks

In the healthcare field, everything from medical devices like blood pressure monitors to the cameras used to monitor physical security on the premises may be connected to a network. The rise of the Internet of Things (IoT) means that connected devices are taking all kinds of forms. To maintain adequate connected device security the following should be put into consideration:

- Maintain IoT devices on their own separate network
- Continuously monitor IoT device networks to identify sudden changes in activity levels that may indicate a breach
- Disable non-essential services on devices before using them, or remove non-essential services entirely before use
- Use strong, multi-factor authentication whenever possible
- Keep all connected devices up-to-date to ensure that all available patches are implemented

8. Conducting Regular Risk Assessments:

Evaluating risk across a healthcare organization periodically to proactively identify and mitigate potential risks, healthcare providers and their business associates is beneficial and helps healthcare providers to better avoid costly data breaches and the many other detrimental impacts of a data breach, from reputation damage to penalties from regulatory agencies. This is carried out by conduction a proactive prevention, because regular risk assessments can identify vulnerabilities or weak points in a healthcare organization's security, shortcomings in employee education, inadequacies in the security posture of vendors and business associates, and other areas of concern.

9. Backing up Data to a Secure, Offsite Location:

Cyber attacks can expose sensitive patient information but they can also compromise data integrity or availability. If data isn't properly backed up, even a natural disaster impacting a healthcare organization's data center can have disastrous consequences. That's why frequent offsite data backups are recommended, with strict controls for data encryption, access, and other best practices to ensure that data backups are secured. Offsite data backups are an essential component of disaster recovery, too.

10. Evaluating Carefully the Security and Compliance Posture of Business:

Associates

Because healthcare information is increasingly transmitted between providers and among covered entities for the purposes of facilitating payments and delivering care, a careful evaluation of all potential business associates is one of the most crucial security measures healthcare organizations can take. The HIPAA Act of 1996 Omnibus Rule strengthened the previous guidelines and clarified definitions of the business associates, providing better guidance on the relationships in which contracts are required. The HIPAA Survival Guide summarizes these clarifications and changes including:

- The conduit exception applies to organizations that transmit Protected Health Information (PHI) but do not maintain and store it. Organizations that merely transmit data are not considered business associates, while those that maintain and store PHI are considered business associates.

- Third-party applications and services such as Google Apps are considered business associates when those services or apps are used to maintain PHI. In such cases, the third-party service would be considered a business associate, and therefore, a contract would be required. The HIPAA Survival Guide aptly points out that as more organizations make use of the cloud, they should be mindful of all instances that would make a vendor a business associate and the likelihood of those vendors to enter into the required contract.
- Any subcontractors who create or maintain PHI are subject to compliance regulations. This change alone has a substantial trickle-down effect and is a serious consideration for all healthcare organizations.
- All covered entities must obtain "satisfactory assurances" from all vendors, partners, subcontractors, and the like that PHI will be adequately protected. Liability follows PHI wherever it travels.

The Protected Health Information (PHI) empowered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The PHI is a law under the US that that needs to do with any information about wellbeing status, arrangement of medicinal services, or installment for human services that is made or gathered by a Covered Entity (or a Business Associate of a Covered Entity), connected to a particular person. This is interpreted rather extensively and incorporates any includes any part of a patient's medical record or installment history (Netsec News, 2018).

PHI is frequently searched out in datasets for de-identification before analysts share the dataset publicly. Researchers remove PHI from a dataset to safeguard security for research participants. (HIPPA Journals, 2018). Wellbeing and medicinal data about research subjects may likewise be controlled by HIPAA. This HIPAA Privacy Rule empowers the government to individual health data held by secured substances and also gives patients several rights with regards to that data. At the same time, there is an adjustment to this Privacy Rule with a goal that it allows the individual health data required a patient care and for other essential purposes to be exposed.

The Protected Health Information (PHI) is directed by the Health Insurance Portability and Accountability Act (HIPAA). The PHI is exclusively an identifiable wellbeing data that relates to the following: (https://www.safecomputing.umich.edu/dataguide/?q=node/61)

- A Past, present, or a future physical/ emotional wellness state of a person.
- Provision of health services to the person by a covered entity (for instance, healing facility or specialist).
- A Past, present, or a future installment for the arrangement of a health services to the individual.

Data Integrity

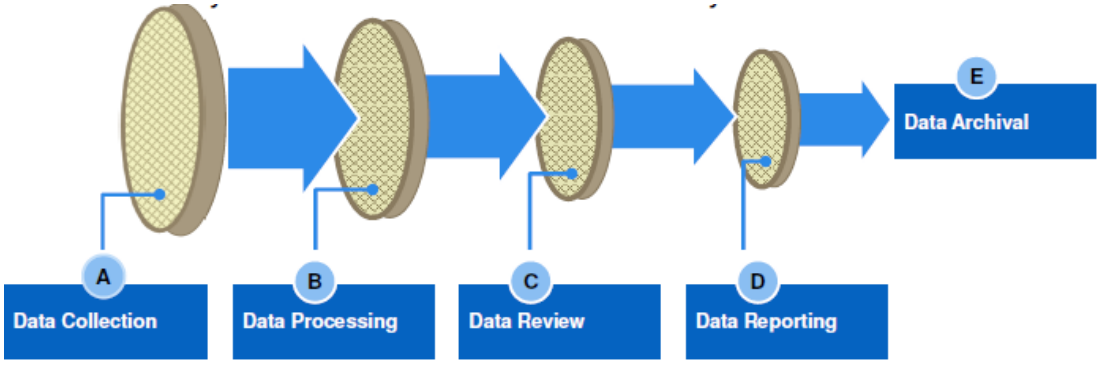
This is the upkeep of or maintenance of, as well as the assurance of data accuracy and consistency over its entire life-cycle, (*Boritz, 2011)* and it's the critical aspect to plan , design, and execution of data and as well as the utilization of any framework that stores, processes, or retrieves data. The term data integrity is expansive in scope and broadly may have widely different implications with reliance upon the particular context – even when it is under a similar general computing umbrella. On occasion it is utilized as an intermediary term for information quality, (Veracode, 2012) while data validation is a pre-essential for data integrity (Digitalguardian, 2018).

Data integrity is the opposite of data corruption (Googlebooks. 2018). The overall goal for any data integrity procedure is the same: guarantee data is recorded precisely as expected, and when later retrieved, it is sure the information is just the same way it was at the point at which it was initially recorded. To be precise, data integrity intends to avert accidental changes to data. It shouldn't be mistaken for data security, or the discipline of protecting data from an unapproved parties. Therefore, any unauthorized change to data as a result of a storage or recovery or processing task, which includes malicious aim, a sudden disappointment of equipment, and human errors, is a failure of data integrity. If changes are as a result of an unauthorized access, it may also be counted as a failure of data security.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 3, pp: (41-52), Month: July - September 2018, Available at: www.researchpublish.com

4. THE APPROACH OF A DATA INTEGRITY LIFECYCLE

It is the degree to which a collection of data is consistent, complete and accurate.



- **Data collection and recording:** This stage ought to guarantee that all information gathering and recording be performed emulating GDP and additionally applying risk-based controls to protect and confirm critical data to guarantee information integrity.
- **Data processing:** in this stage, information transforming (processing) ought to happen in an objective manner, and ought to be nothing from bias, utilizing validated/qualified or checked protocols, systems, methods, processes, equipment and according to endorsed procedures and also training programs to guarantee data integrity.
- **Data review and reporting:** In this phase to guarantee data integrity, the Data ought be reviewed and, where necessary, assessed statistically following fruition of the process to figure out if outcomes are consistent with established standards.
- **Data retention and retrieval:** Data maintenance of paper and electronic records designs guarantees the protection from asserting records from arranged or coincidental change or loss. At this stage, secure controls that guarantee information honesty is set up to guarantee the record all through the retention (maintenance) time frame. Archival processes is likewise characterized in written procedures and approved where proper.

Managing Data and Records across the Data Life Cycle:

Data procedures ought to be outlined such that it satisfactorily alleviate, control and persistently

audit the information integrity risks that is connected with those steps for acquiring, processing, reviewing and reporting weight information as well as the physical stream of the information and related metadata over this procedure through storage and recovery.

Good Data Process Design:

A Data Process design will be great assuming that it ensures that every venture of it will be Consistent; straightforward and Streamlined; Objective, Independent and Secure; Automated; Properly documented according to GDP; Scientifically and Statistically Sound; Well-defined and Understood , to enhance and guarantee control at whatever point possible, else integrity dangers might probable happen particularly when the data processes or any of its steps are inconsistent, unnecessarily complex or redundant, open to bias, subjective, not well understood, unsecured, , undefined, , built upon problematic presumptions ,etc.

Minimizing Data Integrity Risks:

For healthcare establishments to feel certain that there is no loss of its value when using digital frameworks, there are methodologies viable that healthcare organizations may implement to handle efficiently its data integrity dangers and ensure their information with respect to the guideline of ALCOA. The accompanying key prerequisites and controls that might be setup to ensure data integrity and furthermore minimize danger to your association (GlobalVision, 2017):

- **Ensuring All Systems Are 21 CFR Part 11 Compliant**

The 21 CFR Part 11 is an FDA directives that is applied to digital records. It is need to guarantee that digital records are dependable, solid and proportional to paper records. All computer frameworks that preserve data used in other to settle on quality choices must have to be consistent, making it an ideal place where information integrity can begin with.

- **Following a Software Development Lifecycle**

The technique of Software Development lifecycle manages that quality related assignments which are performed to address the appropriate development lifecycle stages beginning with development of the software, the programming integration, testing and installation to an ongoing system maintenance. Every piece of machine systems ought to be suitably created, tried, evaluated and qualified at all time.

- **Validating the Computer Systems**

Software Validation gives recorded confirmation to convey certification that a specific procedure dependably produces an item that meets its pre-decided details and quality properties. To guarantee your framework can be endorsed, it is important to work with vendors that give approval.

- **Implementation of an Audit Trails**

A computerized-generated, time-stamped, secure audit review trails exhibit important data proprietorship and guarantee that dependability of the electronic health record, since it records date of information entries, deletions, and changes and also those time identities.

- **The implementation of Error Detection Software**

Investigation of software automatically can encourage, confirm critical reports to guarantee their precision. It is proven that manual proofreading or investigations are inefficient and so regularly can't guarantee that documents are without mistake.

- **Securing Your Records with A Limited System Access**

All frameworks/systems ought to require a login with nothing less than two interesting pieces of information and also give access to only expected people so as to ensure information integrity.

- **Maintain Backup and also Recovery Procedures**

Backup and a recuperation system is principal in the case of an unexpected occasion of information m adversity and application errors. This technique guarantees that recreation of data is accomplished by media recovery; the recovery of both logical and physical data makes a safeguard to ensure the honesty of your database documents.

- **Design a Quality Management System with Sops and Logical Controls**

A good Quality Management System with good Standard Operating Procedures incorporates the procedure with quality by efficiently controlling the procedure. To write and as well as take after powerful good methods to guarantee clear accountability is fundamental.

- **The Protection of the Physical and Logical Security of Systems**

Good controls are expected to ensure the physical and logical security of your frameworks, change administration, service management and the continuity of your framework. By this your support frameworks and your association development is guarantee ceaselessly.

- **The Establishment of a Vendor Management Qualification Program**

This has to do with evaluating critically and continually on all supplies of vendors to affirm that those results are personal satisfaction items which meet the necessities (critical validation services). Constant examination may be required taking after the beginning assessment. Frequently asking about the data integrity methods your vendors have put in place will assist for the integrity practices of your organization's own data.

- **Properly Training of Users and Training Records Maintained**

Appropriate training should be given to users with a goal to have the correctly skill to discharge competently their job. The training record should be documented for confirmation.

- **Evaluate Controls and Procedures by Conducting Internal Audits**

Audits internally guarantee that continuous improvement is underscored and also that all procedures are taken after

5. METHODOLOGY

To identify the various strategies for prostate cancer prevention, a web search was carried out.

6. DISCUSSION

Data integrity and data security for prostate cancer prevention amongst men.

The data generated in cause of talking to your doctor during interviews and check-ups should be well stored/preserved and updated regularly as any development is observed which will determine the next line of action(s) that will either reduce the risk of developing the prostrate or eliminate/manage the cancer if already developed. Therefore it is worthy of note that these data if not kept with the highest of security and integrity, and it is maliciously tampered with knowingly or accidentally, the prostate cancer prevention would only be a mirage/impossible.

Therefore data security and integrity is very necessary if prostrate prevention is of be achieved.

7. CONCLUSION

To ensure data against assaults, healthcare suppliers should make sure that their network passwords are changed as often as possible, their routers as well as other components are updated with the latest, are secure and changed, and unapproved gadgets are obstructed from getting to the network.

Information breaks/breaches can incorporate cases in which criminal programmers / hackers steal secured wellbeing data to carry out restorative fraud or occurrences when a representative without approval views the records of another patient.(HealthcareBusinessTech.com, 2016)

8. RECOMMENDATIONS

- All the procedures to minimizing data integrity risks should be employed.
- All the procedures to ensure Healthcare Data Security should be employed.
- Proper Training should be given to healthcare providers at all level to maintain highest of standard with regard to Data Security and Integrity in cause of handling data.
- Finally, Data Security and data Integrity as an ICT tool should be added as one among the tools for the prevention of Cancer amongst men.

REFERENCES

[1] Alan J., Wein; Louis R., Kavoussi; Alan W., Partin; Craig A., Peters (23 October 2015). Campbell-Walsh Urology (Eleventh ed.). Elsevier Health Sciences. pp. 1005–. ISBN 9780323263740.

[2] Boritz, J. "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. Archived from the original on 5 October 2011. Retrieved 12 August 2011.

[3] Digital guardian (2018). Gotten from https://www'digitalguardian.com/blog/what-data-integrity-data-protection. Retrieved on 18/04/2018.

[4] Ferlay J, Shin HR, Bray F, Forman D, Mathers C, Parkin DM. (2008). Estimates of worldwide burden of cancer in 2008: GLOBOCAN 2008. Int J Cancer. 127(12):2893–917. [PubMed] Google books (2018).

[5] Goaskalice (2002) "The male hot spot-Massaging the prostate". Go Ask Alice!. 2002-09-27 [Last Updated/Reviewed on 2008-03-28]. Retrieved on 09/04/2018. From http://www.goaskalice.columbia.edu

[6] HealthcareBusinessTech (2016). 10 Best Practices to Secure Healthcare Data. Gotten from http://www. healthcarebusinesstech.com. Retrieved on 09/04/2018.

[7] Https://www.netsecnews/definition-hipaa-covered-entity/ Definitions of a Covered Entity. Retrieved on 18/04/2018

[8] HIPAA Journal (2018)"De-identification of Protected Heath Information". Retrieved on 18/04/2018

[9] Https://www.safecomputing.umich.edu/dataguide/?q=node/61). Retrieved on 18/04/2018

[10] https://www.hhs.gov/answers/hipaa/what-is-phi/index.html. Retried on 18/04/2018.

[11] https://www.google.com.ng/search?q=what+is+prostate+Cancer&oq=what+is+prostate+Cancer&aqs=chrome..69i57.20746j0j8&sourceid=chrome&ie=UTF-8. Retrieved on 22/04/2018

[12] IEEE Big Data Congress (2014). Big Data Security and Privacy Issues in Healthcare Gotten from http://www.ieee.explore.ieee.org. Retrieved on 09/04/2018.

[13] Komisaruk, Barry R.; Whipple, Beverly; Nasserzadeh, Sara & Beyer-Flores, Carlos (2009). The Orgasm Answer Guide. JHU Press. pp. 108–109. ISBN 0-8018-9396-8. Retrieved on 09/04/2018.

[14] Mayo Foundation for Medical Education and Research (MFMER) (2014). Prevention of prostate cancer. Retrievd on 20/04/2018. https://www.mayoclinic.org

[15] O'Hurley, Gillian; Busch, Christer; Fagerberg, Linn; Hallström, Björn M.; Stadler, Charlotte; Tolf, Anna; Lundberg, Emma; Schwenk, Jochen M.; Jirström, Karin (2015-08-03). "Analysis of the Human Prostate-Specific Proteome Defined by Transcriptomics and Antibody-Based Profiling Identifies TMEM79 and ACOXL as Two Putative, Diagnostic Markers in Prostate Cancer". PLOS ONE. 10 (8): e0133449. doi:10.1371/journal.pone.0133449. ISSN 1932-6203.

[16] Rosenthal, Martha (2012). Human Sexuality: From Cells to Society. Cengage Learning. pp. 133–135. ISBN 0618755713. Retrieved on 09/04/2018.

[17] "The human proteome in prostate - The Human Protein Atlas". www.proteinatlas.org. Retrieved on 09/04/2018.

[18] Uhlén, Mathias; Fagerberg, Linn; Hallström, Björn M.; Lindskog, Cecilia; Oksvold, Per; Mardinoglu, Adil; Sivertsson, Åsa; Kampf, Caroline; Sjöstedt, Evelina (2015-01-23). "Tissue-based map of the human proteome". Science. 347 (6220): 1260419. doi:10.1126/science.1260419. ISSN 0036-8075. PMID 25613900.

[19] Veracode (2012). What is Data Integrity? Learn How to Ensure Database Data Integrity via Checks, Tests, & Best Practices. Gotten from https://www.veracode/blog/2012/05/what-is-data-integrity. Retrieved on 18/04/2018

[20] Vijay divecha(2018).View of the Manufacturer “Data integrity”. Retrieved on 19/04/2018.

[21] Vijayan Prabhakaran (2006). "Iron file systems" (pdf). Doctor of Philosophy in Computer Sciences. University of Wisconsin-Madison. Retrieved 9 June 2012.

[22] WebMD (2018). The prostate and its gland. Gotten from https://www.webmd.com/matthew-hoffman. Retrieved on 09/04/2018.

[23] Wikipedia (2018). Functions and secretions of the prostate. http://www.en.wikipedia.org/prostate/cancer. Retrieved on 09/04/2018.