Implementing Biometrics in Healthcare:

A Change Paper

Annaliese LaGiusa & Bo Sananixai

Lakeview College of Nursing

April 1st, 2020

Implementing Biometrics in Healthcare

Security dangers that surround retrieving client records have expanded the need for dependable validation measures. An example of this includes the times that new convoluted passwords must be created and meet minimum password requirements or key cards that are easily shared, lost, or left at home. Once we finally do create a password that's accepted, it's expired and already time to choose a new password, which is usually at the most inconvenient times. All of this work to sign in to a client's EHR (Electronic Health Record), which is required at minimum 50-100 times per shift (Kashyap, 2019). These strategies are monotonous and not secure, as passwords and key cards can be hacked, shared, or stolen.

Additionally, if staff forget their ID badges or access cards, they are unable to efficiently do their job due to having limited access to medication or storage rooms. This paper proposes the use of biometric fingerprint authentication in place of ID key cards to preserve privacy and security in the healthcare system. Our change will employ biometric fingerprinting for user authentication, while continually monitoring the security and access to delicate client information.

Literature Review

Biometrics is a technology that uses the unique fingerprint pattern of an individual for authentication or identification (Hu et al., 2019). Some familiar places that we have seen biometrics used in current society include smartphones, access to secured buildings and offices, as well as entry into the pyxis machines utilized within hospitals. The use of biometrics to provide high levels of security are becoming increasingly popular in today's society. Some collective organizations that we are seeing utilize biometrics into their security systems include law enforcement, border control, consumer biometrics, such as cell phone companies, and financial service corporations (Hu et al., 2019). Biometrics can include the use of facial scanners, iris scanners, and voice-activated commands, however, the fingerprint has been the most widely deployed use of biometrics (Hu et al., 2019). A fingerprint is composed of a pattern of valleys and ridges that birth determines (Hu et al., 2019). No two prints are identical, even for identical twins (Hu et al., 2019). The article discussed in depth in this section discusses the benefits and disadvantages of using biometrics to increase the level of security.

One of the main benefits of using biometric security systems includes never losing or forgetting a password again (Hu et al., 2019). A biometric fingerprint is something that you take everywhere with you all the time. This type of security system decreases the number of times individuals spend changing their passwords, going back and forth between their email and the website, and finally gaining access to the user interface (Hu et al., 2019). Time saved using this type of security system can mean the difference between life and death in a hospital setting. While passwords and PINs are easily forgotten and required to be changed frequently, a fingerprint is unique to each individual and can never be biologically duplicated (Hu et al., 2019).

Disadvantages associated with biometrics can include counterfeit attacks into the user interface by presenting a fake biometric trait (Hu et al., 2019). Artificial traits include acquiring a copy of an individual's fingerprint or using a face mask to gain access to a specific user's profile. According to this article, 11 different fingerprint-based authentication systems were under attack using fake fingerprint films, and 67% were able to gain access to the account (Hu et al., 2019).

To obtain a biometric trait, specifically a fingerprint, a person would have to lift the print from an object touched by the person of interest, create a mold, and design a rubber fingerprint in which they could gain access to anything that individual uses their prints. While this process is lengthy and complicated, it is possible.

To combat these counterfeit attacks, they began incorporating liveness detection systems into the biometric security systems that can detect things such as perspiration and pulse, two things that a fake fingerprint would not have (Hu et al., 2019). Another disadvantage to this system includes compromised prints resulting in loss of access to all their information without the ability to reset the password and gain access again (Hu et al., 2019). Changing a biometric password would be a more in-depth process requiring security department officials to authorize the use of the individual's interface.

The use of biometrics in security is the up and coming form of high-level security. While there are flaws in this system, engineers and researchers are working diligently to determine them and figure out ways to deter them. Biometrics is working towards being the choice method of high-level security moving into the future.

Lewin’s Change Theory

Change is inevitable in healthcare; however, using best practices derived from change theories can help improve the odds of success and subsequent practice improvement. Kurt Lewin was a change theorist who believed that the status quo was the product of several forces in the social environment that govern individuals' behavior at a given point in time and could be analyzed (Batras et al., 2016). Lewin's change theory includes two opposing forces and three distinct stages. The opposing forces include driving and restraining forces, while the different stages include unfreezing, movement, and refreezing.

Lewin's theory suggests that there are always two opposing forces in play when trying to incorporate change in any task or goal, which are the driving forces and restraining forces (Endrejat et al., 2017). Driving forces help facilitate change by motivating employees and team members to work together towards the desired goal (Endrejat et al., 2017). However, restraining forces operate in the opposite direction and interrupts progress and change (Endrejat et al., 2017). The change strategy involved in Lewin's work creates appropriate conditions for sustained change to occur through a group process of trial and error until the desired outcome is achieved (Endrejat et al., 2017).

The first stage in Lewin's change theory is to destabilize and unfreeze the status quo after a need for change is recognized, wanted, and welcomed. Once established, the next steps include collecting data, identifying problematic areas, and increasing the awareness and desire for change (Batras et al., 2016). Before implementing any action, an assessment of the advantages must outweigh the disadvantages of the suggested action. Achieving a successful unfreezing stage is reached when the driving forces exceed restraining forces (Batras et al., 2016). Engaging staff members with a survey can help reveal resistance and increase educational opportunities.

The second stage is movement, and it implements the alternative and moves to the process of initiating change. The goal is to move towards achieving a new process and address resistance that may arise along the way (Batras et al., 2016). It includes evaluating the driving and restraining forces, as well as formulating plans for change. By working together as a team, encouraging the team to view the situation from a different perspective, and using supporting leaders to influence change can help with the movement (Batras et al., 2016). During this stage, it is imperative to establish clear and open communication, along with support and encouragement, to allow room for modifications and evaluations.

Lastly, the third and final step is called refreezing, and it re-stabilizes the environment and the new status quo. During this stage, the goal is to take the steps needed to help maintain the implemented change (Batras et al., 2016). An evaluation of the implemented change is an essential part of the maintenance phase due to the need to reassess implemented strategies to measure their efficacy over time continually (Batras et al., 2016). Implementing formal and informal policies and procedures can help reinforce change and prevent the group from reverting to past behaviors and habits (Batras et al., 2016). If successful, implemented changes are accepted and become the new status quo.

Applying Lewin's change theory to implementing biometrics in healthcare will include unfreezing the organization's current process and perceptions when preparing for upcoming changes once the team becomes aware of previous behaviors and ways of thinking that lead to bias and realize the necessity for the change. During this transition, it is critical to talk to staff to understand their needs, concerns, and fears. Keeping channels of communication open will help build trust, transparency, and rapport that will lead to the feeling of urgency to become motivated. With motivation will come the momentum that is needed to transform the workplace to accept biometrics. As momentum builds to implement biometrics, the open communication channels previously established will allow employees to provide feedback information to allow the refreezing step to take shape and become the new status quo. By serving frequent personal feedback to staff members to help build up their confidence, it will, in turn, welcome the expectations for lasting change.

Data Collection & Analysis

HIPAA (Health Insurance Portability and Accountability Act) is a law that was passed by congress in 1996, and one of the main focuses regarding this act includes mandating protection and confidential handling of protected health information (DHCS, 2019). A breach of this law may consist of consulting or disclosing clinical or personal data to any medical personnel not included in the said client's clinical care (Beltran-Aroca et al., 2016). Another situation in which HIPAA may become breached is by improper disclosure of a client's clinical data due to inadequate infrastructure, equipment, or poor organization by a hospital (Beltran-Aroca et al., 2016). Lastly, a breach can occur due to obtaining custody of secret histories and records containing client data via computer access to such records (Beltran-Aroca et al., 2016).

In a study conducted over 7,138 days, including 33,157 hours of observation in a hospital setting, it was concluded that 54.6% of the recorded confidentiality breaches were due to disclosure of clinical and personal data (Beltran-Aroca et al., 2016). Furthermore, 11% was due to infrastructure breaches, and 34.4% was due to obtaining custody of clinical histories and records via online applications (Beltran-Aroca et al., 2016). Violations involving the disclosure of personal information and gaining control of clinical accounts were determined by overhearing individuals speaking of their activity and returning surveys in which they admitted to breaching client confidentiality (Beltran-Aroca et al., 2016). Questionnaires sent back from 630 employees included 520 employees who were exposed to have experienced a breach of confidentiality either of their own or a coworker (Beltran-Aroca et al., 2016). Overall the study concludes that 82.5% of these healthcare workers violated HIPAA.

Today most EHR systems allow all nurses within a hospital to have full access to all client charts. It is up to them to have the honesty and integrity to not look into client charts that are not theirs. According to these statistics, this is not occurring in the world today. It is crucial to decrease these high numbers of personal breaches by creating programs and security systems that only allow healthcare providers who directly oversee the clients to have access to their information. The use of biometric technology to access client charts can decrease the number of individuals granted access to these charts and therefore reduce the number of overall breaches observed.

Planning the Change Strategy

Using Lewin's change theory, the beginning stages of the planning process will include unfreezing the current policies of a specific hospital. After data collection and addressing the issue at hand that there is an ongoing problem with the lack of security of personal healthcare information, we can begin to make changes. The unfreezing stage may be the hardest part of the process because it requires that individuals admit that there is a need for change. During this process, it is imperative to present data and statistics regarding the high percentages of breached confidential client information. Invoking conversation, brainstorming, and team building is crucial to this step in the planning process. Allowing individuals to feel that they have a voice in the matter and can help to make a difference in the coming change will increase the success of the change. The goal of this unfreezing phase by including members of the healthcare team is to allow them to come to their conclusion that there is a current problem that needs to be addressed and changed (French et al., 2016).

Once through with the unfreezing stage comes the stage for change to occur. During this stage, planning will include new security programs to be incorporated into daily use. During this stage, it will be necessary for department heads as well as managers to educate their staff on the current changes (French et al., 2016). Training programs will be activated into each department so that all employees can have the chance to be educated on how to use new applications properly. Driving forces, such as rewards and ongoing support, should be utilized to increase the likelihood of success (Kaminski, 2011). Restraining forces should be discussed collectively, with all members being affected by the changes and solutions that accompany them. Obstacles will come into the path during this phase, and everyone must work together to solve the problems instead of giving up. Measuring and monitoring change is vital to determine if the planning process is on the right track or if alterations are necessary.

Upon establishing successful change into the healthcare system, refreezing will occur. During this stage of the planning process, it's essential to determine if the change was successful. If so, this stage can continue. Refreezing will incorporate a new normal to the healthcare facility in the form of all healthcare workers using biometric fingerprinting to access client charts and personal information. During this stage, it will be essential to continue teaching and educating the staff on how to use the system appropriately to maintain success. Supportive mechanisms will be put into place to assist all employees with proper use of the system. Distribution of rewards for employees who excel in using the new program and can help educate others can encourage participation. Plans that train new employees on how to use the new system can offer further assistance in the overall objective. The goal of this stage is to freeze new changes into place and not have any regression (Kaminski, 2011).

Implementation

Assessing the readiness of the employees for changes in policies, programs, and practices is essential to implement a change in an organization (Shea et al., 2014). Willingness to change can relate to the individual's ability to psychologically and behaviorally accept the difference and make an effort to implement the change (Shea et al., 2014). If the employees show that they are ready for change, implementation will be more successful, and there will less likely be resistance. Once established, policies and procedures can be put into place to enforce the new guidelines. Implementing biometrics onto hospital units should start with an informative education session on how the plan will roll out. Once the employees are made aware of the changes occurring, each employee will have to go through the fingerprinting process.

Fingerprinting will take the longest time to complete due to the high volume of employees hospitals maintain. After fingerprinting, installing biometric programs, including software and hardware devices, onto the individual units and into the EHR systems will begin. Once the software installation is complete, education teams will be required to work seven days a week all hours of the day to educate and help employees use the system correctly and navigate through issues.

Regular emails, as well as surveys, will be sent out to employees asking for feedback on what they like and what they don't, to help maintain employee satisfaction. These answers will be taken seriously and into consideration to make necessary changes and secure cooperation.

Furthermore, directors and managers of departments will inquire from their employees about their thoughts and feelings on the implementations to determine if further action is required. One of the most important things to keep in mind during the implementation phase will be the employee's commitment to making the change and their continued understanding of the value the change will bring (Shea et al., 2014).

Stabilizing the Change

A nurse manager will be assigned to reinforce the use of biometric fingerprinting to access client data to stabilize the change. They will be responsible for balancing both the driving and restraining forces that ensue. After all of the employees have registered their fingerprints within the organization, the nurse manager will announce when the new method will go into effect. Once the change has been initiated as a group activity to ensure group norms and routines, they will be able to track usage through weekly or monthly reports. By monitoring usage, the nurse manager will be able to see which individuals are using the implemented biometric method and which are not. If an individual is having trouble accessing their client’s EHR, then the nurse manager would be able to take the proper steps to help remediate the issue, such as re-registering the fingerprint or consulting the IT department for troubleshooting.

Once it is evident that utilizing biometric fingerprinting to access client data is the new status quo and meets the overall group personality and environment of staff, weekly follow-up meetings should be planned. During the sessions, the team would be encouraged to voice their concerns and issues with the new change so that the new status quo is not challenged. If nurse managers can respond to staff concerns with the new proposed change, it is less likely that the staff will regress to behaviors that bypass the use of fingerprinting to access a client's EHR. Also, it will boost usage if staff members realize that the change is a definite benefit, saves time, and decreases the number of potential issues that may occur if the change had not been implemented.

Evaluation of the Change Experience

During the unfreezing stage, it was particularly challenging to get staff on board to realize the need for change and break down the existing status quo for accessing client EHRs. Initially, most of the team believed that there were too many factors that went into implementing the change, including time restraints, cost of new equipment, and training. There were many efforts to spark employee interest and education via employee email blasts and links to articles that showed the many advantages of implementing the new change. Once the staff realized the timeline for the proposed amendment and the minimal steps it would take to implement, they were a little less apprehensive. Then, once we were able to address how security threats would be minimized and how it provides an extra layer of protection for nurses, we were able to show not only that the change was necessary, but also a benefit to staff.

Our goal to reduce security threats were achieved and feel secure about the elimination of passwords and key cards being hacked, shared, or stolen. If staff forget their ID badges or access cards, they are still able to efficiently do their job and have full access to medication or storage rooms. The proposal, implementation, and stabilization of using biometric fingerprint authentication in place of ID key cards to preserve privacy and security in the healthcare system is a success. Monitoring the security and access to delicate client information will help confirm that the long-term benefits will outweigh the cost.

References

Batras, D., Duff, C. & Smith B. J. (2016). Organizational change theory: implications for health promotion practice. *Health Promotion International, 31*(1), 231-241.

Beltran-Aroca, C. M., Girela-Lopez, E., Collazo-Chao, E., Montero-Pérez-Barquero, M., & Muñoz-Villanueva, M. C. (2016). Confidentiality breaches in clinical practice: What happens in hospitals? *BMC Medical Ethics*, *17*(1), 52.

DHCS. (2019). *Health insurance portability & accountability act.* Retrieved from https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx.

Endrejat, P. C., Baumgarten F., & Kauffeld, S. (2017). When theory meets practice: Combining lewin's ideas about change with motivational interviewing to increase energy-saving behaviours within organizations. *Journal of Change Management, 17*(2), 101-120.

French, E., Murphy, P., Pearsall, T., & Wojciechowski, E. (2016). A case review: Integrating lewin's theory with lean's system approach for change. *OJIN: The Online Journal of Issues in Nursing, 21*(2), 4.

Hu, J., Valli. C., Wang, S., Yang, W., & Zheng, G. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry*, *11*(2), 141.

Kashyap, R. (2019). Security, reliability, and performance assessment for healthcare biometrics. *Design and Implementation of Healthcare Biometric Systems, 29*(1), 29-54.

Shea, C.M., Jacobs, S.R., Esserman, D.A., Bruce, K., & Weiner, B. (2014). Organizational readiness for implementing change: A psychometric assessment of a new measure. *Implementation Science, 9*(7), 122-143.

Appendix

Meeting minutes:

- 2/26/2020 - Group members present: Bo Sananixai & Annaliese LaGiusa
  - Members of the group decided via a face-to-face meeting at LCN.
- 3/4/2020 - Group members present: Bo Sananixai & Annaliese LaGiusa
  - All members brainstormed ideas for change topics via a face-to-face meeting at LCN and how the sections of the paper will be divided equally.
- 3/11/2020 - Group members present: Bo Sananixai & Annaliese LaGiusa
  - All members decided on one topic to focus on via a face-to-face meeting at LCN and researched information regarding the topic.
  - All members approved the idea for the change paper.
- 3/22/2020 - Group members present: Bo Sananixai & Annaliese LaGiusa
  - All members discussed via phone meeting a timeline of when specific portions of the paper should be completed.
- 3/25/2020 - Group members present: Bo Sananixai & Annaliese LaGiusa
  - All members discuss via phone meeting if further information is needed.
  - All members agree that equal work was distributed and confirm that all sections of the paper are complete.
  - All members assigned to re-read the paper in its entirety for clarity, perform edits via Grammarly and confirm no plagiarism present via turnitin.com.
  - All members agree that the final paper will be complete and turned in by the assigned due date.