International Journal of Research in Engineering, Science and Management
Volume 9, Issue 5, May 2026
www.ijresm.com | E-ISSN: 2581-5792 | RESAIM Publishing | www.resaim.com

An Assessment of Organisational Support and Challenges in Digital Health Procurement and Cybersecurity Implementation in Health Institutions in Bayelsa State

Lucky Ebiteinye Dogiye[1*], Biobelemoye Jack-Gbarabe[1], Chinyere G. N. Idiapho[2]
[1]*Department of Health Information Management, Bayelsa Medical University, Yenagoa, Nigeria*
[2]*Institute of Health Sciences and Management Technology, Delta State University Teaching Hospital, Oghara, Nigeria*

***Abstract*: The growing use of digital technologies in healthcare has increased the need for effective procurement systems and strong cybersecurity measures to protect patient information and support quality service delivery. This study examined the challenges affecting digital health procurement and cybersecurity practices in health institutions in Bayelsa State, with emphasis on organisational support and possible strategies for improvement. A descriptive cross-sectional survey design was used, and data were collected from 196 health personnel through a structured questionnaire. The study covered key areas such as procurement processes, cybersecurity policies, staff training, funding, availability of skilled personnel, management enforcement, incident response planning, and system audits. Data were analyzed using descriptive statistics, including mean scores and standard deviation. The findings revealed that organisational support for both procurement and cybersecurity is generally low. Procurement systems are affected by inadequate funding, bureaucratic delays, lack of transparency, weak monitoring, and corruption. Similarly, cybersecurity practices are weakened by poor training, low awareness of cyber risks, weak policy enforcement, shortage of skilled personnel, and lack of regular system audits and response plans. Despite these challenges, respondents strongly supported practical strategies such as increased funding, regular staff training, adoption of digital procurement systems, enforcement of cybersecurity policies, and continuous monitoring. The study concludes that although awareness is high, implementation remains weak due to insufficient institutional support. It recommends stronger management commitment, improved funding, clear policies, and continuous capacity building to enhance data security and strengthen digital health systems.**

***Keywords*: Organisational Support, Challenges, Digital Health Procurement, Cybersecurity, Implementation.**

1. Introduction

The healthcare industry has changed a lot in the few years because of new digital technology. We now have health records and telemedicine platforms that make healthcare better for everyone. These digital health systems also make it easier for people to get the healthcare they need. At hospitals and clinics these new technologies help doctors make decisions based on facts reduce medical errors and take better care of patients. Digital health systems, like health records and telemedicine platforms are really helping the healthcare industry. The healthcare industry is getting better because of health systems (Al Meslamani, 2023).

At the same time, all this progress means we're leaning more on digital systems, and that opens up a whole new set of challenges especially around cybersecurity. These days, health organizations deal with massive amounts of sensitive patient information, which basically puts a target on their backs for hackers. Rising cyberthreats have people genuinely worried not just about privacy, but about patient safety and keeping systems running smoothly (Ewoh & Vartiainen, 2024). So healthcare institutions are really starting to ramp up their efforts, tightening up digital health procurement and making their cybersecurity stronger.

Digital health procurement is very important because it helps us get the technologies and use them properly. This means we have to make decisions about which technologies to choose how much they cost how well they work and if they can work with other systems. We also need to make sure these digital systems are safe from people who should not be using them and from being disrupted. To do all of this we need our organizations to support us with things like leaders who care, money, training and rules to follow.

In some places like Nigeria digital health systems are being used more and more.. It is hard to get these systems working properly because we do not have the right infrastructure we do not have enough money and our rules are not being enforced well. These problems are even worse in some states like Bayelsa State, where hospitals are trying to update their systems. They do not have enough resources. So it is very important that we look at how our organizations are supporting digital health procurement and cybersecurity and that we find out what problems we are having so we can give better healthcare to people and keep their information safe. Digital health procurement and cybersecurity are crucial, for this.

*Corresponding author: luckiestman2@gmail.com

The use of health has changed healthcare systems all over the world. It helps to deliver services make patients healthier and make operations more efficient. Digital health technologies are very helpful in making healthcare more accessible simplifying tasks and aiding public health responses during emergencies like pandemics (Al Meslamani, 2023). Healthcare systems are becoming more digital. This makes it very important to get health technologies in a secure and efficient way.

Digital health procurement is about getting health technologies that fit the needs of a healthcare organization. It ensures that these technologies are of quality work well with other systems and are secure. Good procurement helps healthcare organizations invest in technologies that're sustainable work well with others and protect sensitive information. However, many healthcare organizations face challenges in procuring health technologies. These challenges include bureaucratic processes, not enough technical knowledge and limited funds. The digital health procurement process is crucial for healthcare organizations to get the technologies. It helps them to provide care to patients. Digital health is very important, for healthcare systems as it helps to make healthcare more efficient and effective.

Cybersecurity is an important part of digital health systems now. Healthcare organizations are targets for cyber threats because they have a lot of valuable patient data and their systems are complex. If there is a cyberattack it can cause a lot of problems like data breaches and disruption of services, which can put patients in danger. Studies have found that healthcare systems over the world are being targeted by cybercriminals more and more which means we really need to have strong cybersecurity measures in place as noted by Ewoh and Vartiainen in 2024.

Even though people are becoming more aware of cybersecurity it is still hard to implement it in healthcare settings. There are obstacles, such as old infrastructure not having people with the right skills poor data management and weak rules. Other issues like internet connections, old computers and systems that do not work well together make it even harder to set up digital health systems especially in places, with limited resources as seen in the work of Wittich and others in 2026.

Organisational support is really important when it comes to dealing with these challenges. You need people in charge to be committed you need to plan things out you need to train your staff. You need to have enough money to make digital health systems and cybersecurity measures work. Some reports from (Guidehouse 2023) say that a lot of health systems are spending money on digital technologies and cybersecurity to be more efficient and able to deal with problems. This just shows how important it is to have support from the people in charge to get results.

In Nigeria people are starting to use health technologies more and more and this is helped by national health policies and global digital health initiatives.. The thing is, not all states are using these technologies at the same level and a lot of institutions are still facing big problems. In Bayelsa State health institutions are trying to use solutions but they are still having trouble with things like buying equipment keeping people safe from cybersecurity threats and getting organisational support. This is why we need to take a look, at what is going on and figure out what is missing so we can come up with solutions that will actually work for digital health systems and organisational support.

2. Statement of the Problem

Digital health technologies are really important for healthcare institutions to deliver services keep patients safe and manage health information properly. However, many healthcare institutions in places that are not very developed are still having a lot of trouble getting these digital health systems and keeping them safe from cyber threats.

One big problem is that these institutions do not have support from the people in charge. A lot of the time they do not have money the leaders are not fully committed and the staff are not well trained. Without support from the institution, it is hard to get digital health technologies and cybersecurity measures to work well. This can lead to people not using the systems properly not taking advantage of the technologies and being more vulnerable to cyber threats.

Also, when healthcare institutions buy health technologies, they often face a lot of challenges. These include not being transparent not having technical know-how and not planning well. These issues can lead to them buying systems that're not very good or do not work well with what they already have. Furthermore, if there are no rules for buying these technologies it can lead to inconsistencies and inefficiencies.

Keeping these health systems safe from cyber threats is also a big challenge. Healthcare institutions are more at risk from cyber threats but a lot of them do not have the right infrastructure, policies and skilled people to manage these risks. There are concerns about keeping patient data private, confidential and secure especially in places where the rules are not enforced well and the technology is not very advanced (Wittich et al., 2026).

The fact that digital health systems are changing fast has not always meant that people are more aware of cybersecurity and doing more to protect themselves. As a result, healthcare systems are still at risk from data breaches, ransomware attacks and other cyber incidents that can put patients in danger and disrupt healthcare services.

In Bayelsa State these problems are especially obvious as healthcare institutions try to adopt health solutions without having enough infrastructure and resources. Even though they are trying to modernize their healthcare systems there is no evidence about how well the institutions are supported what challenges they face when buying digital health technologies and how well they keep these systems safe from cyber threats.

So, it is really important to look at how the institutions are supported and what challenges they face when buying digital health technologies and keeping them safe from cyber threats in Bayelsa State. By doing this we can get an understanding of what is going on and develop strategies that are based on evidence to make the procurement process better increase awareness of cybersecurity and improve the overall

performance of digital health systems in the region. Digital health technologies are crucial, for healthcare institutions. We need to make sure they are used properly and safely.

The study aimed to assess organisational support and challenges in digital health procurement and cybersecurity implementation in health institutions in Bayelsa State and to specifically evaluate the extent of organisational support for cybersecurity implementation in health institutions in Bayelsa state; to identify key challenges affecting digital health procurement and cybersecurity practices in health institutions in Bayelsa state and to identify evidence-based strategies for strengthening procurement processes and cybersecurity consciousness in health institutions in Bayelsa state

A. Digital Health Procurement

Digital health procurement is the way healthcare institutions get and manage technologies like electronic health records and telemedicine platforms. This is not just about buying something it is about making sure the systems work together are cost effective and safe to use in the long run.

Recently people have found out that digital procurement is connected to the healthcare supply chain. This is where technologies like blockchain and cloud systems help make things more transparent, secure and efficient. These systems are complicated and need people with the right skills to manage them. Also, different departments have to work to make good decisions. If the people in charge of health procurement do not make good choices it can lead to problems like systems that do not work well together and security issues (Monferdini et al., 2024). Digital health procurement is very important because it affects how well digital health systems work, like health records and health information systems.

B. Cybersecurity in Healthcare

Cybersecurity in healthcare is about keeping systems, networks and patient data safe from people who should not have access to them. This is a deal because more and more healthcare places are using electronic health records and connected medical devices. This makes them a big target for people who want to hack into these systems.

Scholars say that cybersecurity is not about the technology it is also about how organizations are run. If the security is not good it can lead to bad things happening, like losing data not being able to use the systems and even putting patients in danger. There are kinds of threats to healthcare cybersecurity, like ransomware, phishing and attacks from people inside the organization. There are also problems with Internet of Medical Things devices, which are connected to the internet (Adnan, Kutafina, & Beyan, 2024). Cybersecurity, in healthcare is a concern because of all these threats, including ransomware, phishing, insider attacks and Internet of Medical Things devices. (Kazi, 2024).

C. Organisational Support

The people in charge of healthcare places need to support the use of digital health systems and cybersecurity measures. This means they have to be committed to the idea give money make good policies provide training and have the right infrastructure in place.

Organisational support is very important for making digital changes work. It affects how the staff behave if they use the systems and if they follow the rules to keep things secure. When the leaders of healthcare places think cybersecurity is important and give the staff what they need the staff are more likely to do things the way and keep the systems secure as shown by people, like Alharbi and Alkhalifah in 2025.

D. Challenges in Digital Health Implementation

Digital health is a thing but it is hard to make it work, especially in places that are not very developed. The main problems are infrastructure not having people who know what they are doing weak rules and not enough money. Scholars who have done some research have found that things like the internet not working right old computers and systems that do not work together are problems for digital health. Digital health is something that's hard to do because of these things, like when the internet is not working and the computers are old (Wittich et al., 2026). Also the rules are not clear. This makes it even harder to make digital health work as some people have found out (Al Meslamani, 2023).

E. Empirical Review

Digital health is something that lots of people are looking at and many studies have looked at how healthcare systems are using digital health and how they are protecting themselves from cyber-attacks. A study by Kazi in 2024 found that hospitals and other healthcare places are getting more and more vulnerable to cyber-attacks because patient data is very valuable. This study said that ransomware and data breaches are two of the threats and that hospitals need to keep training their staff and spending money on security systems.

Similarly, Adnan and others in 2024 looked at how healthcare placesre protecting themselves from cyber-attacks and found that many of them are struggling to put good security systems in place because their technologies are all connected in complicated ways. They said that having a plan for cybersecurity is very important to deal with the risks that come with sharing data and getting different systems to work together.

In another study Al Meslamani in 2023 found that in some countries digital health is not being used much as it could be because there are not enough rules and not enough money and also because the people in charge do not have the right technical skills. These things make it hard for digital health systems to be used properly. They also make it hard to buy the right equipment.

A recent study in 2025 found that people are still worried about cybersecurity and that hospitals do not have the right equipment and also that the data they have is not very good. This study said that if digital health systems are not standardized and if they are not connected properly then they will not work well (Alharbi, & Alkhalifah, 2025). When it comes to hospitals and other healthcare places research shows that the ones with leaders and enough money are better, at protecting themselves from cyber-attacks. If the hospital is not

organized very well then it will be harder for them to protect themselves and they will be more likely to be attacked (Wittich et al., 2026).

Overall digital health and digital health systems and cybersecurity are all things that people are talking about more and more. Actually, making them work is still a problem because of all the challenges that healthcare systems face with digital health and cybersecurity and digital health systems.

F. Theoretical Framework

This research is based on two ideas:

The Technology Acceptance Model (TAM):

The Technology Acceptance Model tells us how people accept and use technologies. It talks two important things: how useful people think a system is and how easy it is to use. For example, if someone thinks a system will help them do their job better they are more likely to use it. The Technology Acceptance Model also looks at how easy it's to use a system. If a system is hard to use people will not use it.

The Technology Acceptance Model helps us understand how healthcare workers feel about health systems and cybersecurity practices. If healthcare workers think digital systems are helpful and easy to use, they will use them more. This is what Venkatesh and Davis said in the year 2000. However, if healthcare workers do not get the training they need. If the systems are not well designed or if their organization does not support them, they will not use the systems. This is what Holden and Karsh said in the year 2010.

The Technology Acceptance Model is very important for understanding how healthcare workers behave when it comes to using health systems and following cybersecurity rules. The Technology Acceptance Model helps us understand why healthcare workers do or do not use health systems. The Technology Acceptance Model is really good, at explaining this.

Socio-Technical Systems Theory:

The Socio-Technical Systems Theory is about how people and technology and organizational structures work. It says that to make a system work you need to balance the social parts. The Socio-Technical Systems Theory was first talked about by Trist and Bamforth in 1951.

The theory says that organizations do well when technology and human factors like staff skills and leadership are in line. This means that if you introduce technology without thinking about the people and the organization it can cause problems. People might resist the technology or it might not work well. Sometimes it can even fail completely. This is what Bostrom and Heinen said in 1977.

The Socio-Technical Systems Theory is important for this study. Buying health tools and putting in place cybersecurity measures are not just about the technology. They also depend on how people use them and the rules of the organization. For example, even the best cybersecurity systems can fail if the staff are not trained properly. If the organizations rules are not good it can also cause problems. Similarly, if you make procurement decisions without thinking about what people need you might end up with systems that are not used or do not work well. Sittig and Singh said this in 2010.

So, the Socio-Technical Systems Theory helps us understand how technology and people and organizational support work together in healthcare. It gives us a view of how all these things interact with each other in a healthcare environment. The Socio-Technical Systems Theory is helpful because it reminds us that the Socio-Technical Systems Theory is, about people and technology and organizational structures.

3. Method and Materials

This study looked at how health personnel in some hospitals in Bayelsa State, Nigeria collect and protect health data. The researchers used a survey to find out what people think and do at the moment without trying to change anything.

They chose six hospitals, including Kolo General Hospital, Yenagoa Hospital and Maternity Tobis Hospital, Crest Specialist Hospital, Family Care Hospital and GloryLand Hospital because these hospitals are using health systems in different ways and they are a mix of public and private hospitals.

The researchers included all 208 health personnel in the study so they could get a picture of what is happening. This meant they did not have to pick and choose who to include. They could make sure their results were accurate. The people in the study were doctors, nurses and other staff who use or support health systems.

To collect data the researchers used a questionnaire that they had developed from studies on health information and cybersecurity. They made sure the questions were clear and relevant by getting experts to review them. They also tested the questionnaire in another hospital to make sure it worked well. They made some changes before using it in the main study.

The researchers collected the data over a week with the help of some trained assistants. They told the health personnel what the study was about. They promised to keep their answers secret. The health personnel agreed to take part in the study before they started answering the questions.

When the researchers got all the answers, they used a computer program called Statistical Package for the Social Sciences to analyse the data. They looked at the results to see what they could learn about health data and cybersecurity. They also looked for any differences or relationships between groups of people.

The researchers got permission to do the study from the Bayelsa State Ministry of Health Ethics Committee and from the hospitals where they collected the data. They made sure to follow all the rules, about doing research with people including keeping everything secret and making sure people took part voluntarily.

4. Results

A total of 196 questionnaires were completed and returned from 208 distributed, yielding a response rate of 94.2%. Table 3 presents the distribution of responses across the six selected health institutions.

Table 1
Response rate by institutions

Institution	Distributed	Returned	Response Rate (%)
Kolo General Hospital	32	30	93.8
Yenagoa Hospital and Maternity	35	33	94.3
Tobis Hospital	30	28	93.3
Crest Specialist Hospital	36	34	94.4
Family Care Hospital	37	35	94.6
GloryLand Hospital	38	36	94.7
Total	**208**	**196**	**94.2**

Field Survey, (2026).

The table 1 shows how many questionnaires were shared with health personnel at the selected institutions and how many were successfully returned. Overall, 208 questionnaires were given out. 196 Were completed and returned, which is a very high response rate of 94.2%. This means the data collected is reliable and representative because most of the participants took part in the study.

Looking at the institutions all of them had very strong response rates with only small differences between them. Kolo General Hospital gave out 32 questionnaires. Got 30 back which means they had a response rate of 93.8% and that is still very good. Yenagoa Hospital and Maternity had a higher response rate of 94.3% with 33 out of 35 questionnaires returned. Tobis Hospital had a response rate of 93.3% which's the lowest among the six institutions but it is still within a strong range. Crest Specialist Hospital had a response rate of 94.4%. Family Care Hospital had 94.6%, which shows that the participants were consistent in their responses. The highest response rate was at GloryLand Hospital, where 36 out of 38 questionnaires were returned, giving them a response rate of 94.7%.

In general, the response rates at all the institutions are very close ranging from 93.3% to 94.7% which shows that the participants were very cooperative. This consistency makes the study findings more credible because it reduces the chances of bias that could come from uneven responses. The table shows that health personnel at all the selected hospitals were very engaged which suggests that the topic of the study is relevant and interesting to them.

The table 2 gives us a picture of who the health personnel are. We have 196 health personnel who took part in the study. This gives us an idea of what they are like.

Looking at how old the health personnel're we see that most of them are between 30 and 39 years old. This group makes up 42.9% of the total. The next group is the 20 to 29 years old which is 31.6%. This shows that a lot of the health personnel are young.

Fewer health personnel are between 40 and 49 years old which is 16.3%. The smallest group is the 50 years and above which's 9.2%. So we can say that the health personnel are mostly young and middle-aged. They are likely to be active and able to adapt to digital health ideas.

When we look at the gender of the health personnel, we see that there are more females. Females make up 54.6% while males make up 45.4%. This shows that we have a mix of males and females. However, females are a bit more represented in the health institutions we studied.

Looking at what qualifications the health personnel have. Most of them have a Bachelor's degree, which's 60.2%. About 26.5% have a Diploma or Certificate while 13.3% have postgraduate qualifications. This shows that most health personnel have a level of education. This is important for understanding and using health systems.

Table 2
Demographic characteristics of respondents (N=196)

Category	Frequency	Percentage
Age group of the respondents		
20–29 years	62	31.6
30–39 years	84	42.9
40–49 years	32	16.3
≥50 years	18	9.2
Gender distribution of the respondents		
Male	89	45.4
Female	107	54.6
Education of the respondents		
Diploma/Certificate	52	26.5
Bachelor's degree	118	60.2
Postgraduate	26	13.3
Years of Experience of the respondents		
1–5 years	68	34.7
6–10 years	62	31.6
11–15 years	38	19.4
≥16 years	28	14.3
Type of Institution		
Public	63	32.1
Private	133	67.9

Field Survey, (2026).

Regarding how the health personnel have been working the largest group has 1 to 5 years of experience which is 34.7%. The next group has 6 to 10 years of experience which's 31.6%. This shows that many health personnel are still developing their skills. Those with 11 to 15 years of experience make up 19.4% while 14.3% have 16 years or more of experience.

Finally for the type of institution the health personnel work in. Most of them 67.9% work in health institutions. The rest, 32.1%, work in institutions. This shows that private healthcare facilities are more represented in the study. This might affect what we find especially when it comes to resources and system adoption. In a nutshell, the health personnel are mostly young to middle-aged fairly well-educated and work, in healthcare settings. They have a mix of experience levels. This is important because it helps us understand their views and practices regarding health procurement and cybersecurity. The health personnel and their characteristics are important to consider when looking at health.

A. Organisational Support for Cybersecurity

Table 3 presents institutional support structures.

The table 3 shows us how much health institutions care about cybersecurity and the message is pretty worrying. They do not

do a job of supporting it in all areas.

Table 3
Organisational support (N=196)

Item	Mean	SD	Level
Written policy	1.95	1.12	Low
Regular training	1.88	1.15	Low
Dedicated cybersecurity staff	1.72	1.05	Low
Incident response plan	1.85	1.10	Low
Security budget allocation	1.68	1.02	Low
Management enforcement	2.25	1.18	Low
Security audits	1.92	1.08	Low
Overall Support	**2.22**	**0.85**	**Low**

Field Survey, (2026).

If we look at written policies the result is that many institutions do not have cybersecurity policies or they do not tell people about them. Policies are the base of any security system. A low score here means they are starting from a weak point.

In the aspect of training, the low score means that staff are not learning about cybersecurity practices on a regular basis. This is a problem because even the best systems can fail if users do not know about security measures like protecting passwords or dealing with phishing risks.

The situation is more concerning for dedicated cybersecurity staff, which has a very low score. This means that most institutions do not have people who specialize in managing cybersecurity so issues may not be handled in a timely way.

Similarly, the plan for responding to incidents is also low which means that many institutions are not ready to deal with cyberattacks or data breaches. Without a plan any security issue could cause big problems and lead to losing data.

The way security budget is allocated has the score, which means that cybersecurity is not a financial priority. This lack of money probably contributes to weaknesses, such as poor training and not having enough personnel. Although management enforcement is a bit better it is still low. This means that when there are rules, they are not strongly enforced by leaders.

Lastly, security audits are also low which means that institutions rarely check or test their systems to find vulnerabilities. The overall score confirms that health institutions do not support cybersecurity well. In terms many of these health facilities are not ready to protect their digital systems and patient data. This lack of support increases the risk of cyber threats. Shows that we need stronger policies, better funding, regular training and more involvement from management, for cybersecurity.

The table 4 shows that people really think there are problems with buying digital health things for hospitals in Bayelsa State. All the scores are high which means everyone agrees on this.

The biggest problem is that people are not honest when they buy things for hospitals, which is called corruption in procurement processes and it has a score of 3.43. This means that people think it is a problem.

There are also problems like it takes too long to do things, which is called bureaucratic delays and it has a score of 3.39 and there is not enough money, which is called inadequate funding and it has a score of 3.37. These things make it hard to buy health things for hospitals.

Other things that are problems include people not being open about what they do, internet and computers not checking what is going on and hospital staff not being trained well. All these things have scores.

This means that buying health things for hospitals in Bayelsa State is hard because of many reasons, including money problems, administration problems and hospital problems.

Overall, the problem with buying digital health things for hospitals in Bayelsa State is big and needs to be fixed in a big way, not just a little bit. Digital health procurement, in Bayelsa State health institutions is facing challenges that need to be solved with big changes, not just small ones.

The results in table 5 show that people think cybersecurity is a problem in health institutions. Everything we looked at had numbers, which means people think they are not safe when it comes to cybersecurity practices.

The biggest problem we found is people making mistakes.

Table 4
Summary of result of the challenges affecting digital health procurement practices

S.No.	Statement	Mean	Std. Deviation	Interpretation
1	Inadequate funding affects procurement	3.37	0.78	High
2	Lack of transparency in procurement	3.31	0.77	High
3	Bureaucracy delays procurement processes	3.39	0.75	High
4	Lack of training affects procurement systems	3.27	0.81	High
5	Poor infrastructure affects procurement	3.32	0.80	High
6	Vendor selection not based on standards	3.24	0.79	High
7	Corruption affects procurement	3.43	0.76	High
8	Weak monitoring of procurement	3.28	0.81	High

Field Survey, (2026).

Table 5
Summary of the result of cybersecurity practice challenges

S.No.	Statement	Mean	Std. Deviation	Interpretation
1	Inadequate cybersecurity training	3.38	0.78	High
2	Weak password practices	3.41	0.78	High
3	Lack of security software	3.30	0.80	High
4	Poor awareness of cyber risks	3.35	0.78	High
5	Weak internet security infrastructure	3.32	0.79	High
6	Limited enforcement of policies	3.39	0.79	High
7	Human error causes breaches	3.46	0.76	High
8	No incident response plan	3.30	0.80	High

Field Survey, (2026).

This has a mean of 3.46 which means that what staff do and the mistakes they make are a part of cybersecurity problems. Using passwords, which has a mean of 3.41 and not making sure cybersecurity rules are followed which has a mean of 3.39 are also big problems. This shows that both people and institutions have weaknesses that contribute a lot to cybersecurity risks.

Not training people enough not telling them about cybersecurity threats having systems and not having plans for when something goes wrong were also seen as big problems. This shows that cybersecurity is not about technology it is also about people being able to handle it and institutions being ready.

In summary what we found is that health institutions in Bayelsa State are, at risk of cybersecurity problems because people do not know enough rules are not. They do not have the right technology to protect themselves.

The table 6 shows what people think about ways to make digital health procurement better. They all much agree on this. Most of the scores are really high which means people are much in favor of these ideas.

The thing that people like the most is having money for digital health procurement. This got a score of 3.53. People think that having money is the key to making digital health procurement work. They also think that training the people who work with health procurement is very important with a score of 3.52. Using the steps every time when buying things for digital health procurement is also a good idea, with a score of 3.52. People think that we should check how well digital health procurement is working, which got a score of 3.50.

Respondents also like the ideas of using computers to help with buying things for health procurement being open and honest about what we are doing and making sure that everyone who is affected is involved in the process. This tells us that people think we can fix the problems with health procurement by making sure we have the skills we need by spending money in a smart way and by making our systems better.

So, it seems like people are feeling good about this and they really want to see some changes that will make digital health procurement more efficient, open and fair. They want to see digital health procurement work in a way that's good, for everyone.

The results in table 7 show the agreement among all sections with average scores between 3.50 and 3.56. This means people really agree with cybersecurity improvement plans.

Respondents think that regular cybersecurity training helps people know more and do better (Average = 3.54). They also agree with using passwords, checking systems, updating antivirus software and keeping an eye on systems, all of which got very high scores.

The similar answers suggest that respondents know what is needed to make cybersecurity better. The strong agreement on plans for responding to incidents and enforcing policies also shows that people know cybersecurity needs both prevention and response.

In short respondents think that making cybersecurity stronger, in health institutions mainly depends on training, strong policies, updated systems and active monitoring.

B. Discussion of Findings

The study of health procurement and cybersecurity practices in health institutions in Bayelsa State shows us what is going on. Digital health procurement and cybersecurity practices in health institutions in Bayelsa State are not doing well. The people who took part in the study know what the problems are. They also know how to fix them. Digital health procurement and cybersecurity practices in health institutions in Bayelsa State still have big problems.

The study found that health institutions in Bayelsa State do not support health procurement and cybersecurity practices very much. Things like making policies, training staff and having money are all lacking. Health institutions in Bayelsa State also do not have skilled people to deal with digital health procurement and cybersecurity practices. They do not plan well for when things go wrong. They do not check their systems often. This means that digital health procurement and cybersecurity practices are not a priority for the people in charge of health institutions, in Bayelsa State.

The lack of cybersecurity rules or their poor implementation

Table 6
Summary of the result of strategies for strengthening procurement

S.No.	Statement	Mean	Std. Deviation	Interpretation
1	Enforcing guidelines improves transparency	3.46	0.66	Very High
2	Training improves procurement efficiency	3.52	0.63	Very High
3	Digital procurement reduces corruption	3.48	0.65	Very High
4	Monitoring improves procurement outcomes	3.50	0.64	Very High
5	Adequate funding strengthens procurement	3.53	0.67	Very High
6	Stakeholder involvement improves decisions	3.43	0.69	High
7	Standardized procedures improve quality	3.52	0.64	Very High

Field Survey, (2026).

Table 7
Summary of the result of cybersecurity strengthening strategies

S.No.	Statement	Mean	Std. Deviation	Interpretation
1	Training improves cybersecurity awareness	3.54	0.64	Very High
2	Strong password policy improves security	3.56	0.62	Very High
3	Antivirus updates reduce risks	3.51	0.65	Very High
4	Clear policies improve compliance	3.54	0.63	Very High
5	System audits detect threats early	3.55	0.60	Very High
6	Incident response plans improve security	3.50	0.64	Very High
7	Continuous monitoring strengthens security	3.56	0.62	Very High

Field Survey, (2026).

is very worrying. These rules are essential to guide practices and ensure compliance. This agrees with Kruse et al. (2017) Who found that missing cybersecurity rules in healthcare make it more vulnerable to cyber threats. Also staff not receiving training plays a big role in security breaches caused by people. This is in line with Hadlington (2018) who said that poor awareness is a cause of cybersecurity risks, in healthcare settings.

The problem of not having people who are good at cybersecurity makes it harder for places to stop and deal with cyber incidents. Coventry and Branley said something in 2018. They said that not having skilled cybersecurity people makes it really tough for healthcare systems to keep their digital environments safe. If a place does not have a plan in place to deal with incidents it is not ready for cyberattacks. Sittig and Singh talked about this in 2016. Said that being able to respond quickly is very important when there is a security breach.

Not having money for cybersecurity means that there is not enough money to train people or to upgrade systems. Martin and others said in 2020 that not having money is a big problem for cybersecurity in healthcare systems all over the world. The people in charge are doing a little better than areas but they are still not doing a great job, which is important for making sure everyone follows the rules (Alharbi & Alkhalifah, 2025). The fact that security audits are not done often means that places are not good at finding and fixing problems with their systems.

The study also found out that buying health things is hard because of big problems like not having enough money waiting a long time for things to happen, corruption and not being transparent. These problems are often seen in healthcare systems in countries that do not have a lot of money. Cybersecurity is a problem and it is hard to deal with cyber incidents when there are not enough people who are good, at cybersecurity.

The World Health Organization says that when the systems for buying things are not good it can lead to wasting time and money. The same thing is said by Asamani and others in 2020 they think that when people are not held responsible and things are not transparent it can lead to corruption and wasting time and money when buying things for health care. The delays caused by much bureaucracy that we found in this study are also seen by the World Bank in 2021 they say that complicated administrative procedures can slow down the process of buying things for the public sector.

The things we found out also show that the ways to keep the internet safe are not good because of mistakes made by people weak management of passwords not knowing enough and not making sure the rules are followed. These problems show that the dangers to the internet are not about technology but also about how people and organizations behave. The International Telecommunication Union said in 2022 that the things people do are a reason why healthcare systems are not safe on the internet. Fu also says that when staff do not know enough it makes the systems more vulnerable. The weak enforcement of internet safety rules that we saw in this study is, like what the National Institute of Standards and Technology said in 2020 they think that rules must be put into action and watched to be effective.

With all the problems the people we asked think that there are some practical ways to make things better. World Health Organization and these ways include getting money, training staff using digital systems making sure the rules are followed and regularly checking and evaluating the World Health Organization and these things.

The World Health Organization in the year 2020 says that having money is very important. They think that having a financial plan is necessary for making the health system better. The World Health Organization says this because they want to make sure the health system is strong. Asante in the year 2019 also says that building capacity is a thing to do to make procurement better and more accountable. Using systems for procurement is something that the World Bank in the year 2021 agrees with. They think that using systems makes things more transparent and reduces corruption.

When it comes to keeping things safe from cyber-attacks training staff all the time is very important. The World Health Organization in the year 2021 says that educating people is critical to reducing cyber risks. Checking the systems all the time and monitoring them is also an idea. The National Institute of Standards and Technology in the year 2020 recommends doing this to find and fix vulnerabilities. Using passwords and keeping security tools up to date is also a good thing to do. This is what the World Health Organization and other organizations say we should do to keep things safe.

The main thing we found out is that people know what they should do but they are not doing it. People in Bayelsa State know that they need to have procurement and cybersecurity systems. But they are not able to do it because they do not have money they are not trained well their leaders are not committed and they do not have good rules to follow. This means that to make the digital health systems in Bayelsa State better we need to do more than just tell people what to do. We need to make sure that the institutions are working well that the people in charge are doing their jobs and that we are investing in people and technology all the time. We need to make sure that the World Health Organization and other organizations are happy, with what we're doing in Bayelsa State.

5. Conclusion

The results of this study show that the support for cybersecurity in the health institutions we looked at is not good enough. Things like making policies, training staff getting money having people and checking the systems regularly are not done well. This means that a lot of institutions are not ready to protect their computer systems and the private information of patients which makes them more likely to be attacked by hackers.

At the time this study helps us understand better how health institutions in Bayelsa State buy digital health things and keep their systems safe. Even though health professionals know how important it is to have systems for buying things and keeping them safe they still face many problems.

In terms of buying things problems like not having money waiting too long for things to happen not being open about what

is going on not checking things well and people being corrupt are still big issues. These problems show that there are issues with how the system is set up and run. The same thing is true for keeping systems safe. Both people and the institutions themselves have problems like not training people not knowing enough not making sure policies are followed and people making mistakes, all of which make the systems for health information more vulnerable.

With all these problems the people we talked to were very supportive of practical ideas to make things better. These ideas include training staff all the time getting money using digital systems making sure policies are followed and checking and evaluating things regularly.

Overall, this study says that to make the digital health systems in Bayelsa State better we need to do more than just know what to do. We need to do it by having institutions that are committed leaders who are effective and, by investing in people and technology over a long time.

A. Recommendations

Based on what is found out from this study here are some recommendations to help Bayelsa State health institutions improve their health procurement and cybersecurity:

1. The government and health institution managers should provide funds for health systems. This will help make digital health systems in Bayelsa State work better faster and more secure.
2. When buying health tools for Bayelsa State health institutions we should follow the rules. Make sure everything is transparent. This can be done by checking and auditing procurement processes for health systems and using digital systems to track everything.
3. Easier means to buy health tools for Bayelsa State health institutions should be provided. This means making the process of getting approval and buying health tools faster.
4. Health workers at Bayelsa State health institutions need training on how to use procurement systems and cybersecurity best practices for digital health systems. This will help them do their jobs better and avoid mistakes with health systems.
5. Bayelsa State health institutions should have rules on cybersecurity for health systems. These rules should be enforced across all departments at Bayelsa State health institutions to protect health systems.
6. Staff should be taught at Bayelsa State health institutions about cyber risks and how to handle data safely for health systems. This will help protect information for health systems.
7. Cybersecurity tools like firewalls and antivirus software for health systems at Bayelsa State health institutions should be provided. We should also make sure our digital health systems are updated and maintained regularly.
8. Bayelsa State health institutions should have a plan in place in case of a cybersecurity breach for health systems. This plan should help us detect, respond and recover from breaches of health systems quickly.
9. Regularly evaluate procurement and cybersecurity practices for health systems at Bayelsa State health institutions should be introduced. This will help us make sure we are following the rules and improving health procurement and cybersecurity all the time.
10. Bayelsa State health institutions should hire experts who can manage and protect health systems.
11. Leaders and stakeholders including government agencies and IT experts should enforce procurement and cybersecurity strategies for health systems, at Bayelsa State health institutions.

References

[1] M. Adnan, E. Kutafina, and O. Beyan, "Cybersecurity frameworks in healthcare data: A short literature review," *Stud. Health Technol. Inform.*, 2024.

[2] A. Z. Al Meslamani, "Technical and regulatory challenges of digital health implementation in developing countries," *J. Med. Econ.*, 2023.

[3] A. Z. Al Meslamani, "Why are digital health policies crucial?," *J. Med. Econ.*, 2024.

[4] A. Alharbi and A. Alkhalifah, "Cybersecurity governance in healthcare during digital transformation," *Front. Public Health*, vol. 13, p. 1703689, 2025.

[5] J. A. Asamani *et al*., "Strengthening health systems through improved procurement practices," *BMC Health Serv. Res.*, 2020.

[6] E. K. A. Asante, "Capacity building in health systems procurement," *Int. J. Health Plann. Manage.*, 2019.

[7] R. P. Bostrom and J. S. Heinen, "MIS problems and failures: A socio-technical perspective," *MIS Q.*, vol. 1, no. 3, pp. 17–32, 1977.

[8] A. Cavoukian, "Privacy and cybersecurity in healthcare systems," *Health Inform. J.*, 2020.

[9] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[10] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, vol. 13, no. 3, pp. 319–340, 1989.

[11] P. Ewoh and T. Vartiainen, "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review," *J. Med. Internet Res.*, 2024.

[12] K. Fu, "Cybersecurity risks in healthcare infrastructure," *J. Cybersecurity*, 2021.

[13] Guidehouse, Health Systems Prioritizing Cybersecurity as 2024 IT Budgets Increase, 2023.

[14] L. Hadlington, "Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 4, no. 7, p. e00652, 2018.

[15] R. J. Holden and B. T. Karsh, "The Technology Acceptance Model: Its past and its future in health care," *J. Biomed. Inform.*, vol. 43, no. 1, pp. 159–172, 2010.

[16] International Telecommunication Union, *Global Cybersecurity Outlook*, 2022.

[17] N. F. Kazi, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *J. Cyber Security*, 2024.

[18] C. S. Kruse, B. Frederick, T. Jacobson, and D. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technol. Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[19] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: How safe are we?," *BMJ*, vol. 369, p. m1327, 2020.

[20] L. Monferdini, B. Pini, B. Bigliardi, and E. Bottani, "Challenges and opportunities of digitalization in the healthcare supply chain: A literature review," *Procedia Comput. Sci.*, 2024.

[21] National Institute of Standards and Technology, *Cybersecurity Framework*, 2020.

[22] S. Sitaru, G. Bramm, A. Zink, and M. Hiller, "Cybersecurity in digital healthcare—Challenges and potential solutions," *Dermatologie*, 2023.

[23] D. F. Sittig and H. Singh, "A new socio-technical model for studying health information technology in complex adaptive healthcare systems," *Qual. Saf. Health Care*, vol. 19, suppl. 3, pp. i68–i74, 2010.
[24] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks in healthcare," *J. Am. Med. Inform. Assoc.*, vol. 23, no. 4, pp. 784–790, 2016.
[25] E. L. Trist and K. W. Bamforth, "Some social and psychological consequences of the longwall method of coal-getting," *Hum. Relat.*, vol. 4, no. 1, pp. 3–38, 1951.
[26] V. Venkatesh and F. D. Davis, "A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies," *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, 2000.
[27] L. Wittich, H. Rödiger, T. Rombey, A. Brecher, L. Kraft, S. Sgraja, V. Stein, and C. Henschke, "Navigating the complexities of digital health technology implementation: Barriers and facilitators," *Implement. Sci. Commun.*, 2026.
[28] World Bank, Digital Procurement and Governance in Public Sector Systems, 2021.
[29] World Health Organization, *Data Quality Review Framework*. Geneva, Switzerland: WHO, 2017.
[30] World Health Organization, Strengthening Health Systems Through Improved Data and Procurement. Geneva, Switzerland: WHO, 2020.
[31] World Health Organization, *Cybersecurity in Healthcare: Protecting Patient Data*. Geneva, Switzerland: WHO, 2021.