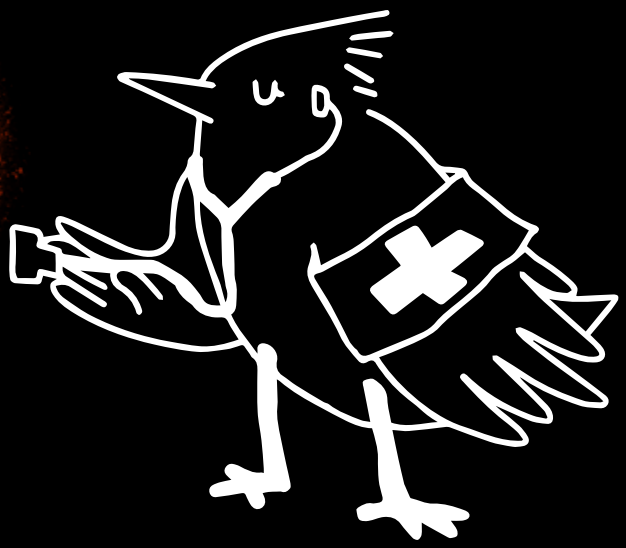
freedom to focus

Improving patient care:
Is email the answer to more secure digital comms?

care less



Foreword by:
Liam Cahill, Advisor to national bodies,
frontline providers and lecturer on digital disruption in health

Including contribution from:
Tania Palmariellodiviney, Information Governance
and Data Protection Specialist

zivver

Contents

Research approach
In March 2022, we conducted interviews with a selection of global healthcare professionals using the specialist market research consultancy, Insight Avenue. For this paper, we will focus specifically on our UK insights.

Expert contribution

Liam Cahill
Advisor to national bodies, frontline providers and lecturer on digital disruption in health

change

When it comes to care, we all know that standing still is not an option. There are very few services I can think of that will not see radical change over the next decade, and few that are not facing incredible pressures right now.

The prospect of what we can achieve with technology in healthcare is exciting and offers enticing opportunities that we all wish to see, both in providing care and as patients ourselves. But often, when it comes to the detail of where to start and how to find a balance between progress and risk, this can feel like a dichotomy for system leaders.

Healthcare is a communications business, and in most services better communication will tangibly lead to better outcomes. Whether this is in reducing care silos, better supporting self-management, or freeing up time to provide more complex care through efficient support of those with more routine needs.

But without the right technology to support communications outside of physical care settings, there is only so much we can achieve. Connecting with patients in their day-to-day lives, in more and more valuable ways, will be critical to achieve the ambitions outlined in the NHS Long Term Plan.

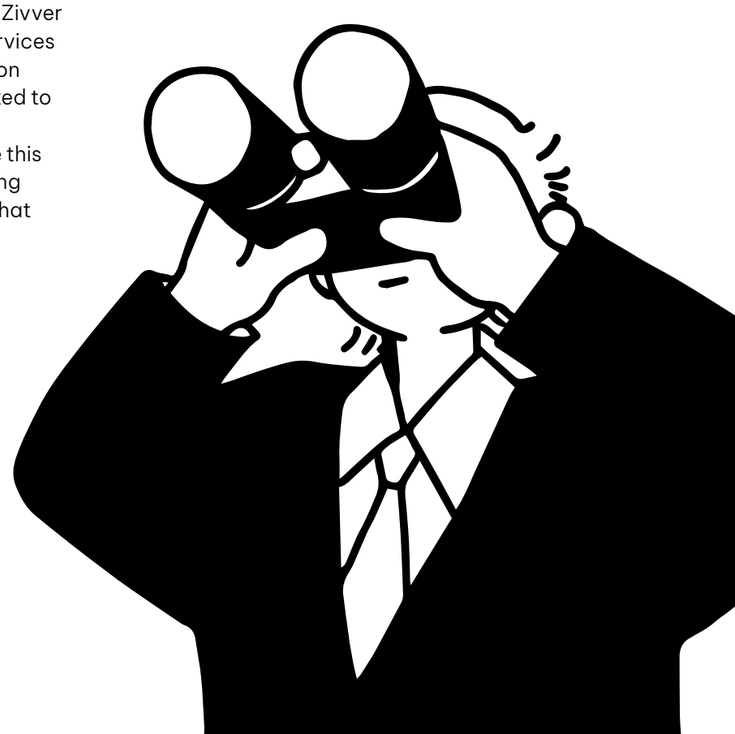
So how do we make great strides in communication across services and with patients right now? This is a simple question, but if you're a digital leader you'll know that there appear to be few genuinely easy wins, often risking greater fragmentation, sprawl, inaccessibility, change programmes and pressure for services already operating at the limit.

For patient interactions, the new plans to utilize the NHS App are exciting, but may take a few years to materialize. And I know from personal experience that shifting to chat in digital spaces is a huge endeavor, especially across shifting boundaries that span beyond the traditional healthcare domains.

This is a big strategic quandary, and one that begs the question: if changing the format and regularity of how we interact with our patients (and each other) is such a huge necessity, and the expected mediums aren't here, aren't currently viable or aren't secure or failsafe enough, what are we supposed to do now?

I believe that Zivver offers a great evolution to the world's most used, but often problematic, medium: email. In particular, when I'm working with providers to consider how we can find new ways to securely communicate with our patients, the blend of security options along with the accessibility and flexibility Zivver offers could offer immediate ways for frontline services to start improving their service, with little disruption and rapid turnaround, so those services aren't asked to take their focus away from their patients.

It is therefore my great privilege to introduce this healthcare whitepaper, and I look forward to seeing what your services achieve with the capabilities that Zivver offers.



The NHS is no stranger to adversity. Up against challenging financial targets, staff face a barrage of cost and time barriers that can hamper progress and damage productivity. And one such hurdle is the implementation of an effective digital communications system to ensure efficient collaboration across the board.

In being tasked with integration, and across providers of different shapes and sizes, local systems need to ensure that patient care is joined up, and providers are effectively working together to enable people to live healthier lives. Efficient and secure comms are critical to achieving this. Unfortunately, this isn't typically the reality, with the lack of cohesion leaving staff struggling to sync up.

The after-effect of the pandemic means that the NHS needs to find ways to address the patient backlog – with digital identified as one of the most critical ways to achieve this. On top of this, busy healthcare professionals don't have time on their side, so there's growing urgency for a better way of working through using technology.

But what all this really comes down to is how the NHS can provide better patient outcomes. Encouraging different providers to work together for the good of the patient is all very well, but it throws a new challenge into the mix: how do they share sensitive information about their patients safely and securely?

Few would disagree that the stakes are currently high, and the NHS must find practical ways to ensure that new ways of delivering care put great communications right at the center of that ambition. Through building upon what healthcare staff already know and trust, but bringing in new capabilities and better security, local systems are best placed to bring their staff together to meet the current and future care challenges they face.

The snapshot

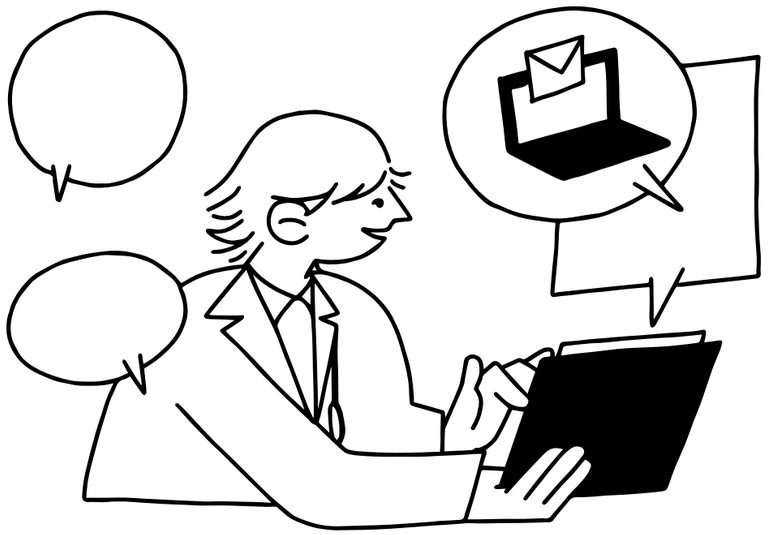
Time to talk

Healthcare communications have had an overhaul. Throughout most ICSs there are now myriad new channels, apps, and technologies aimed at improving communication across the board.

In fact, 51% of healthcare workers report that their comms channels have increased in the last two years.

While on the surface this might seem like a progressive move, the reality for workers is less positive. From increasing stress levels (31%) to reducing their ability to focus and do their best work as they are interrupted more frequently (31%), this sharp increase has thrown up more challenges than it solves.

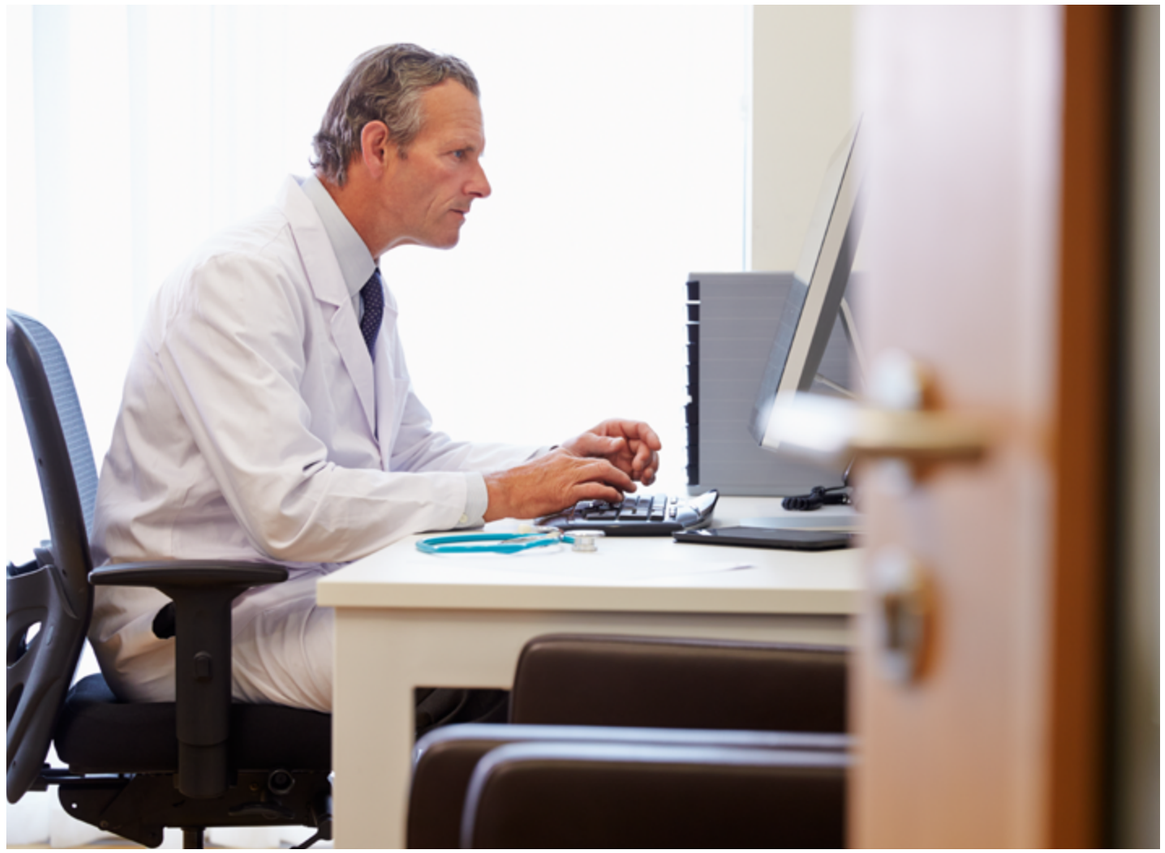
Healthcare workers can feel overwhelmed by choice, unsure of the best method to use, and are therefore more likely to make errors. Plus, with patient care taking up most of their time and energy, they just don't have the space to learn how to use new tech.



Ultimately, it's vital that healthcare workers have access to the right comms systems to be as productive as possible. For example, undertaking time-consuming logistical work – like sending appointment reminders and referrals via the post – takes time and energy away from core tasks. Not to mention the security issues that can arise, such as sending out the wrong sensitive information – which has a knock-on effect of slowing down vital care.

A key finding from our research states that 99% of healthcare professionals globally want to be free to focus on their core role in the coming year. After all, patient care is at the forefront of all they do. But they don't necessarily have the tools and support in place to do that – yet.

99% of healthcare professionals globally want to be free to focus on their core role in the coming year.



Rethinking security

The integration agenda offers a progressive and much needed transformation for the NHS. And within ICSs, email is considered a reliable, tried and tested platform – for good reason. In fact, it could be the progressive tool of choice in today's communication landscape. Yet currently, data breaches are still happening.

In the last two years, 30% of our respondents have sent the wrong attachment in error, 27% have hit **reply all by mistake**, and 20% have sent sensitive information via email that they probably shouldn't have.

Concerningly, only 23% say they worry about data security and that they might send something they shouldn't. This leaves 77% who are apparently unaware of the risks. This potential oversight could hold the key to the increasing risk of security breaches – and an increasing headache for IT leaders.

Clearly email is being championed as the preferred form of communication. However, what ICSs need is a better understanding to make it the secure tool for today: while in the meantime, the ultimate solution continues to evolve.

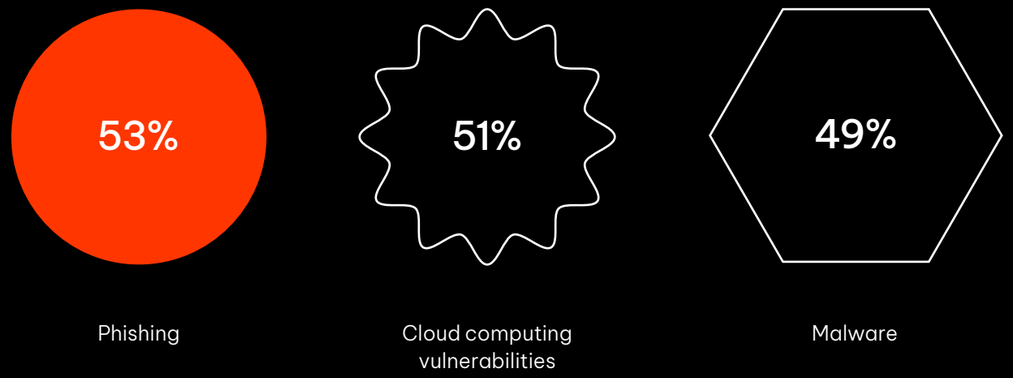
What does IT think?

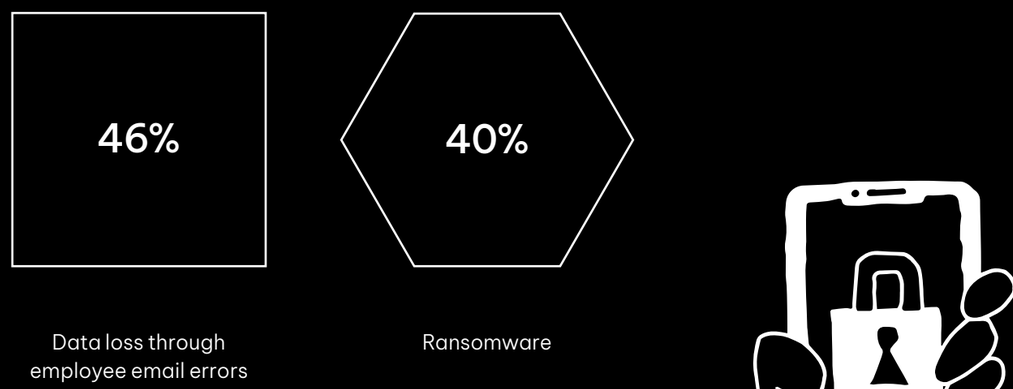
64% of healthcare organization IT leaders have experienced security threats in the last two years. Out of the threats faced, they're most concerned about the following:

It's clear that IT leaders are very aware of the risks. And they also know that security measures can hamper employee productivity. But do they know what to do about it?

One strategy is to think as much about outbound security failures as external threats. Arguably, IT leaders are in prime position to put the right processes and support in place – so they must consider what tools they can access to make that happen.

Security threats healthcare organizations are most concerned about





Embracing email

Despite dalliances with alternatives, email is evergreen. When faced with an influx of new comms solutions, healthcare staff raise concerns about new tools that may affect their systems of care, exclude colleagues or be incompatible with how other colleagues in care work, preferring to opt for what's familiar. Especially across the multiple providers of an ICS who need to send information quickly, securely, and often between different systems.

88% of employees rely on email to get their job done, and 81% see it as the most secure way to send sensitive information. It's clear that email – when deployed correctly and safely – is likely to be the most productive and efficient means of communication across an ICS.

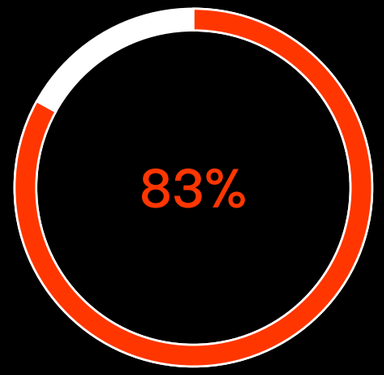
And as for email's security status, it's possible to mitigate that risk. Meaning that, although non-compliance is difficult to completely put a stop to, there are solid actions IT leaders can take.

Solving security

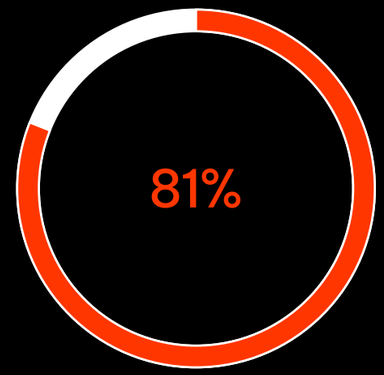
Employees want to feel secure sending emails. But IT professionals want staff to be more on the ball to reduce the risk of errors. How can the two peacefully co-exist?

NHS Digital's executive director of cyber operations **Mike Fell says**:

> "Good security practices are our shared responsibility and being cyber aware can significantly reduce the chance of cyber events affecting people's care."



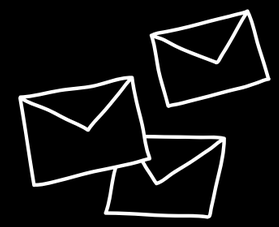
of IT leaders think employee email security errors can be reduced with smarter email data security



of healthcare professionals don't think that security is the employees' responsibility

It seems that the answer is to implement practical solutions that protect busy healthcare workers from making security lapses, reducing the risk of human error, enabling stronger encryption, and leaving IT leaders feeling reassured

Ultimately, employees should be better supported by technology, not the other way around.



Delving into digital

Accelerated by the pandemic, digitization has impacted many healthcare services.

However, limited digital skills and access to digital infrastructure can be an issue for many staff when facing huge demand, and resource shortages across the board. Shifting to new technologies can often feel like an overwhelming and unviable distraction.

Plus, for many patients, whose access to digital may be hampered by limited digital skills, financial circumstances, or physical or cognitive challenges, using apps that require connected smartphones can make those services inaccessible.

But this doesn't mean it's totally out of reach. Being progressive means moving towards a stronger and better solution for all. It's important to assess the situation at face value, and this means addressing key comms and security issues today, while considering how the bigger picture can be realized later down the line.

The wealth of benefits that email brings can't be ignored. It enables NHS employees to work effectively, focus more on core tasks and care, and minimizes worry around security lapses. Patients are more likely to access it with or without a smartphone. Plus, it's easier for IT teams to manage thanks to lack of maintenance, and easier to use.

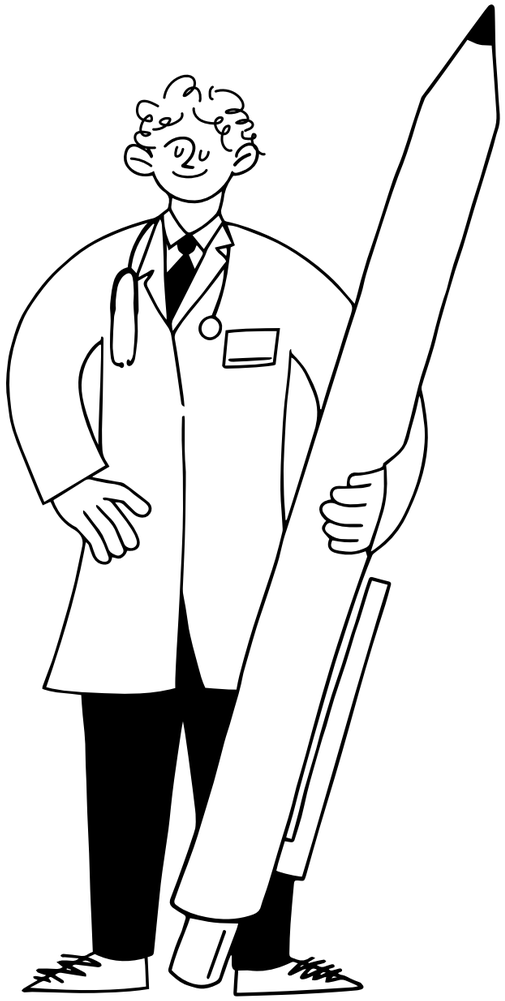
Email is the key to improving patient communication across the NHS.

Prioritizing patient care

Armed with the right tech solution, IT leaders can help staff send sensitive information securely over email. Right here, right now.

Rather than burdening employees with more security protocols and unnecessary comms channels, smart technology solutions layered on top of email serve as a simple yet highly effective way to overcome security barriers and support healthcare workers in delivering the best patient care.

And the best thing is: all healthcare providers across an ICS are already using email. By implementing a layered solution on top of an existing system, no extra training is required. Instead, it's all systems go!



How can this transform the ICS and the care experience?

1

Proactive, preventative care

The patient is at the heart of everything NHS staff do. If staff can communicate effectively and safely with patients, it will mean a more proactive approach to delivering high quality care.

For example, if a Child Speech and Language Therapy team can receive videos of children stammering from parents, they have new efficient options to offer remote support.

2

Clearer communication

Siloed comms channels only mean one thing: poor communication.

By using security-smart email, care delivered between different providers can be clearly communicated, and can transcend one individual organization's system.

3

Better patient access and accessibility

Communicating smoothly with patients in a way that doesn't require a high level of digital literacy means better care across the board.

More accessible than a downloadable app, email can be used via a range of devices, doesn't require complex sign-up processes, and is much simpler for patients whose first language is not English.

It's up to IT leaders to implement the right tools that enable workers to provide the best quality care. But system leaders also need to feel safe in the knowledge that they are progressing in the right direction, making future-ready decisions that impact how their organizations operate and continue to improve on an upwards trajectory.

Expert contribution

Tania Palmariellodiviney
Information Governance
and Data Protection Specialist

secure

And the data breach category of the year award goes to: **"Email Sent in Error"**. Having worked for many, many years in the NHS and in the field of Information Governance, the use of email was an ever-present security issue that gave us a lot of headaches. Root Cause Analysis reports were almost an exact copy and paste each time, with the category stated as *email sent in error.*

Directors would ask us whether we'd done everything we could to tackle the issue. In response, we'd say:

- ✓ Training?
- ✓ Awareness?
- ✓ Repeated offender training?
- ✓ Team meeting attendance specifically around email security?
- ✓ Autofill function risk assessment?
- ✓ Email policy?

After some years with the same answers and no improvement, I was asked again: *is there more we can do?*

I felt there probably wasn't – aside from sit directly next to each employee about to send an email and ask them:

- ✓ Have you checked that this is the right recipient?
- ✓ Does the autofill button show the correct recipient?
- ✓ Have you checked you have not accidentally included any other recipients?
- ✓ Have you encrypted the email if it contains personal or sensitive data?
- ✓ Have you checked any attachments?
- ✓ Do you mean to be replying to all? Be sure to check if you mean to be replying to all or only intend to reply to the last sender of the email.

Technology has improved over the years, and encryption has become somewhat automated within the NHS. But when staff contact patients or other care providers who don't use the same platform, the recipient then has to carry out certain actions to be able to receive the message. This still does not address the fundamental issue.

Hand on heart, everyone makes this mistake at some point – and when it does happen, we try to recall the message. I find that fascinating, since the process of recalling a message almost always fails.

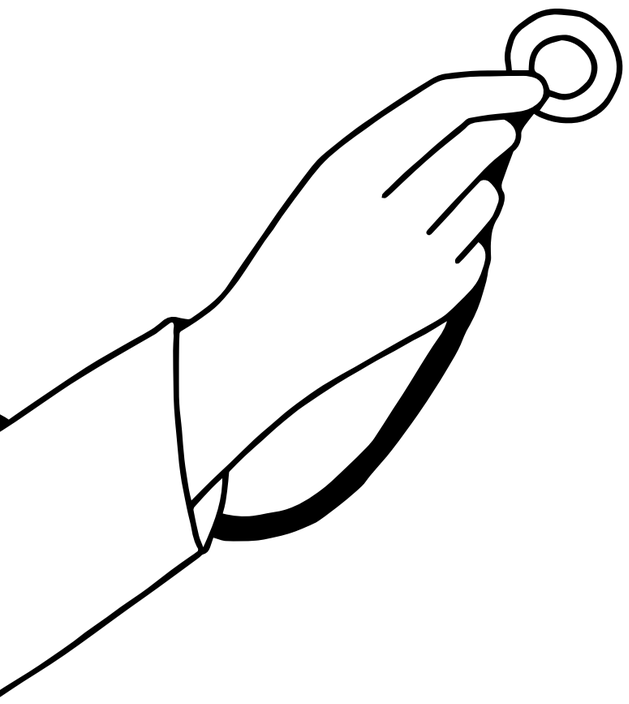
What do people generally do when technology is 'difficult' in their eyes? Well, they work around those issues, which most likely ends up amplifying risk.

So, what would we like to see happen instead?

We need to ensure that our patients feel that ICSs are providing joined-up care. And they should also feel their data is safe and secure, whether in records or when transmitted via email. Crucially, if it goes wrong there should be simpler ways of preventing a misfired email becoming a serious data breach.

If everything fails, we should be able to be confident that we've done everything possible to support our staff in preventing "human error". I'm sure our patients would be much more understanding if we could evidence all the measures we have taken to secure it – and apologize if it still went wrong.

A better system for all



While over the coming years the NHS is working towards greater communications functionality through the NHS App, this will take time. It's important for ICSs to recognise that there is a way right now to provide secure and efficient communications.

Email is a trusted and proven tool. And armed with the right security layer, the NHS and patients can share sensitive information with confidence. This switches the responsibility away from people, and instead onto the supporting tech.

It also has the added benefit of keeping IT leaders assured. Not only by ensuring workers are staying compliant, but also by eliminating extra hassle around having to maintain and manage complex software.

But most of all, it allows healthcare workers to focus on their core role, and to keep patient care the center of everything they do.

zivver

To find out more about how Zivver can help your healthcare organization embrace the next generation of secure digital communications, please visit zivver.com