zivver

To: Ben Hargreaves
Cc: Sarah Davies

A new standard for healthcare communications

Whitepaper

Table of contents

01

Integrated care systems everywhere

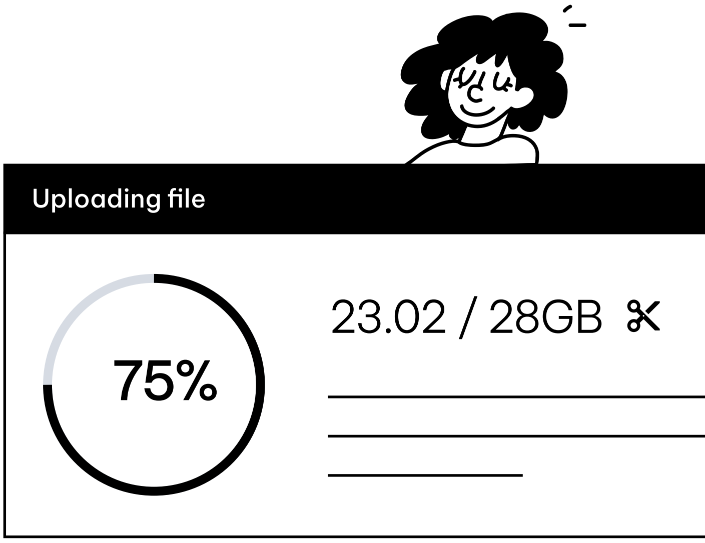
One of the most significant lessons learned from the COVID-19 pandemic is the need for people to be supported in a joined-up way across local councils, the NHS, and voluntary and community organisations. In the past, divisions across these organisations have meant that too many people experienced a poor patient experience with disjointed care.

With the NHS Long Term Plan stating that all parts of England would be served by an integrated care system from April 2021 – "the biggest national move to integrated care of any major western country"[1], the healthcare sector has a great opportunity to strengthen its organisations by collaborating to overcome shared challenges.

Integrated Care Systems (ICSs) embed the level of collaboration needed for effective partnership working, supporting local services to respond to the challenges of the pandemic – and beyond. The ambition is to remove traditional divisions between hospitals and family doctors, between physical and mental health, and between NHS and council services. This will lead to improved population health, reduced inequalities between different groups and will help communities thrive. Partnership working across the healthcare sector is now an integral part of ensuring the health and care system is on a stronger footing.

Partnership working can be complex and requires strong leadership at all levels. But the prize is clear: strong communications can help to build effective partnerships, smarter, more transparent ways of working and more engaged staff – all of which will help integrated care systems to achieve their aims of more joined up care and better outcomes for the public.

Furthermore, the NHS Confederation is launching a new network to support ICS communications professionals to come together to share ideas, best practice, and learning. It joins other forums for ICS leaders which have been established by the NHS Confederation, including forums for chairs, executive leads, programme directors, workforce and mental health leads[2].



[1] The journey to integrated care systems in every area, NHS England
[2] www.nhsconfed.org/news/new-network-ics-communication-and-engagement-leaders-launched

02

The crucial role of communication

> “We believe that effective communications and engagement play a crucial role in supporting integrated care systems, and the partners that make them up, to achieve stronger relationships, more open and transparent ways of working… ultimately, better outcomes for the public.”

Daniel Reynolds, Director of Communications and Membership Operations at the NHS Confederation

To make these partnerships work, effective communications need to be the glue that holds everything together. It is critical to recognise the strategic importance of the way communications are exchanged and to ensure this information is being managed in seamless, secure and simple ways.

Enabling effective and tailored patient care now inevitably involves many different individuals across healthcare, all needing to share patient information across multiple organisations and to the patients themselves. From medical reports, invitations to screenings, medication reviews and vaccination appointments to x-rays, MRI/CT and laboratory test results, the types of communications that healthcare practitioners exchange comes in many forms.

Consequently, there is an increasing need for information and communication technologies to enable health services and initiatives in delivering improved communications.
If information is the lifeblood of healthcare, then communication systems are the heart that pumps it.

The landscape for communication channels and the way health and care organisations access and use them is continually evolving, but some constants prevail.

Email continues to be the main information conduit for healthcare and, as a result of the pandemic, email usage is increasing. Healthcare practitioners, administrators and stakeholders are increasingly relying on the use of email to exchange information across organisations and to communicate with patients. It's a communication route that we are all familiar with and many organisations have significantly cut the cost of appointment letters as part of a trust-wide initiative to drive digital efficiency. However, security, confidentiality and data protection have been considerable challenges for healthcare, especially in this era of increased remote working and rapid movement to the cloud. The key challenge of email is not only ensuring security is of the highest standard, but that the process of sending and receiving email is streamlined and user-friendly. Obtrusive technologies which demand a change in processes are not the answer; instead, there is an urgent need for effortless technology that optimises processes, empowers staff and improves the patient experience.

As digital innovations advance, it's critical for the healthcare sector to re-evaluate the functionality, security, and accessibility of their email communications to ensure that providers have the most future-proofed solutions at their fingertips.

03

Evaluating healthcare email functionality

A number of healthcare organisations have already implemented email solutions in addition to the use of standard email to enable a two-way, secure flow of information.

Used by 80% of healthcare practitioners, NHSmail enables users to send data securely to email addresses which meet the same standards of accreditation required. When considering the functionality, usability, and compliancy factors of email systems, there are a few essential tools to consider:

- Encryption
- Large file transfer
- Human error prevention
- Integration and user-centricity

Encryption

NHSmail allows users to exchange information with insecure or non-accredited email services via the NHSmail encryption feature. Currently, when NHSmail users need to send encrypted emails, they must manually add the word [secure] in the subject line of a message. This feature must be used when sending any personal or confidential information to a non-secure email address, such as a patient email address. When a patient receives an encrypted email, they will need to register for the service if they haven't done so already. Only after logging in are they able to view and reply to the email.

On the surface, this may appear to be a simple process, but concerns have emerged. Across some healthcare spaces, practitioners have acknowledged that some of their patients have found the process of accessing encrypted emails cumbersome. Consequently, practitioners are bypassing the encryption part of the email sending process, highlighting a myriad of security concerns.

Large file transfer

File sharing is a necessary activity across healthcare. For example, Subject Access Requests (SARs) hold the entirety of data held on a patient, and are therefore highly sensitive and often very large files. The NHS estimates it takes 30 days to fulfil a SAR, and with trusts sending hundreds each month (sometimes by post) it can be a costly and time-consuming process which raises legitimate security concerns; those sending files by email often need to send multiple emails to fulfil one request due to its file size, which is not efficient or user-friendly.

Zivver enables users to safely send up to 5TB within Gmail, Outlook, or NHSmail, with the benefit of advanced zero knowledge encryption. The highly secure platform allows the sender to set 2FA controls, password protect files, and provides a supremely simple experience for the receiver, without the need to create a Zivver account to access files. Additional functions mean the sender can also view when the SAR has been received and downloaded by the patient, as well as setting expiration periods to control file access.

Integration & user-centric

The best security solutions are tools that your staff want to use, resulting in wider adoption. When software seamlessly integrates with current systems and processes, people aren't disrupted or left frustrated.

In this way, staff can communicate securely without changing their way of working. Additionally, easy integration helps staff comply with data protection regulations such as GDPR.

← →

Empowering employees to be their organisation's greatest defence

Many reports highlight that the leading causes of data incidents are consistently attributed to human error. Health and care organisations require a 'human error prevention' tool to eliminate risks such as sending information to the wrong recipient, adding the wrong attachment, exposing recipient information via the To or CC fields, when BCC should have been used, or unauthorized access to data has occurred, usually due to weak passwords and lack of two factor authentication. As such, it's vital for organisations to utilise innovative technologies to empower their people to avoid those seemingly small mistakes which often have the largest consequences.

Only with the right tools can employees be the data protectors they want to be, embedding a trust-wide 'security first' culture to support the ICSs approach.

04

Zivver’s secure communications platform

Zivver integrates with existing healthcare emailsolutions (NHSmail, Outlook, Gmail, Microsoft Office 365), supercharging email security with advanced encryption and unrivalled security functionality.

Zivver's secure email technology protects sensitive data before, during and after sending:

1

Before sending

Zivver scans the email as it is being composed (including attachments within a particular size) and warns the sender if sensitive or personally identifiable information is included. Zivver also alerts the sender to potentially incorrect recipients, misuse of Cc/Bcc, and more.

2

During sending

Unlike standard email clients, Zivver utilises advanced asymmetric zero-knowledge encryption; emails cannot be intercepted in transit, and Zivver does not hold your encryption keys. Strong authentication methods can be used to ensure only the intended recipient can access their data (e.g. 2FA).

3

After sending

Messages can be revoked or set to automatically expire. Senders also benefit from visibility of message performance, and can view when messages have been received and opened.

Superior, smart, and simple technology to make achieving communications security effortless.

05

Why healthcare providers choose Zivver

In recent years, the NHS has been the subject of a number of high-profile data breaches. The Information Commissioner's Office reported the healthcare sector suffered 214 reported data incidents from Jan-March 2021 – more than any other sector. 30% of these incidents were due to incorrect recipients or misuse of BCC.

Source: Information Commissioner's Office, ico.org.uk/action-weve-taken/data-security-incident-trends/

Secure send is ON OFF

Business rules ○

Two-factor authentication ●

Outlook integration ○

01

For healthcare providers sending sensitive information via email

The problem:

For time-poor healthcare staff, security needs to be simple.

The solution:

Zivver alleviates pressure by recommending best practice to the user, automated workflows and machine learning. The moment users begin to compose messages, Zivver observes the subject, body, and attachment of the email and alerts the user to potential errors:

Sensitive information?

Zivver suggests sending securely.

Incorrect recipient?

Zivver alerts the user before they hit ‘send’.

Cc instead of Bcc?

Zivver recommends best practice.

Zivver also automates the whitelisting of domains to ensure emails are safe in transit and are delivered as regular emails to NHS.net and other DCB1596 accredited domains; for non-accredited domains, verification methods are enabled.

← →

02

User-friendly for patients

The problem:

Email is accessible and reliable but not always secure.

The solution:

Zivver is designed to be user-friendly for both the sender and the receiver:

- Advanced zero knowledge encryption protects emails in transit
- Patients don't need to create Zivver accounts to access secure emails or attachments
- Two-factor authentication and password protection ensures emails and attachments are accessed by only the intended recipient

03

Share large files and fulfil subject access requests (SARs) with ease

The problem:

The number of SARs is rising; standard email limits file sizes, making it difficult to share documents securely and easily.

The solution:

Zivver's platform enables the safe sharing of files up to 5TB directly from your email client, including Outlook, O365 or Gmail. The platform encrypts files and enables password protection and 2FA - and we don't hold your encryption keys. Patients and third parties can access emails easily with no cumbersome platforms or portals involved. Senders can also monitor emails after sending, and view when a SAR has been received and downloaded.

04

Automate communication workflows and increase security

The problem:
Many trusts still invest time and money manually sending appointment reminders, referrals and letters via the post.

The solution:
Zivver Mail Submission add-on integrates with Electronic Patient Records and other source systems to automate the secure electronic sending of letters, driving significant cost savings. Zivver automatically utilises details held within the systems to add a verification method for recipients (e.g. the patient's mobile or NHS number).

05

Encourage trust-wide cyber security awareness

The problem:
Compulsory security awareness training is increasingly treated as a tick-in-the-box exercise in ensuring compliance.

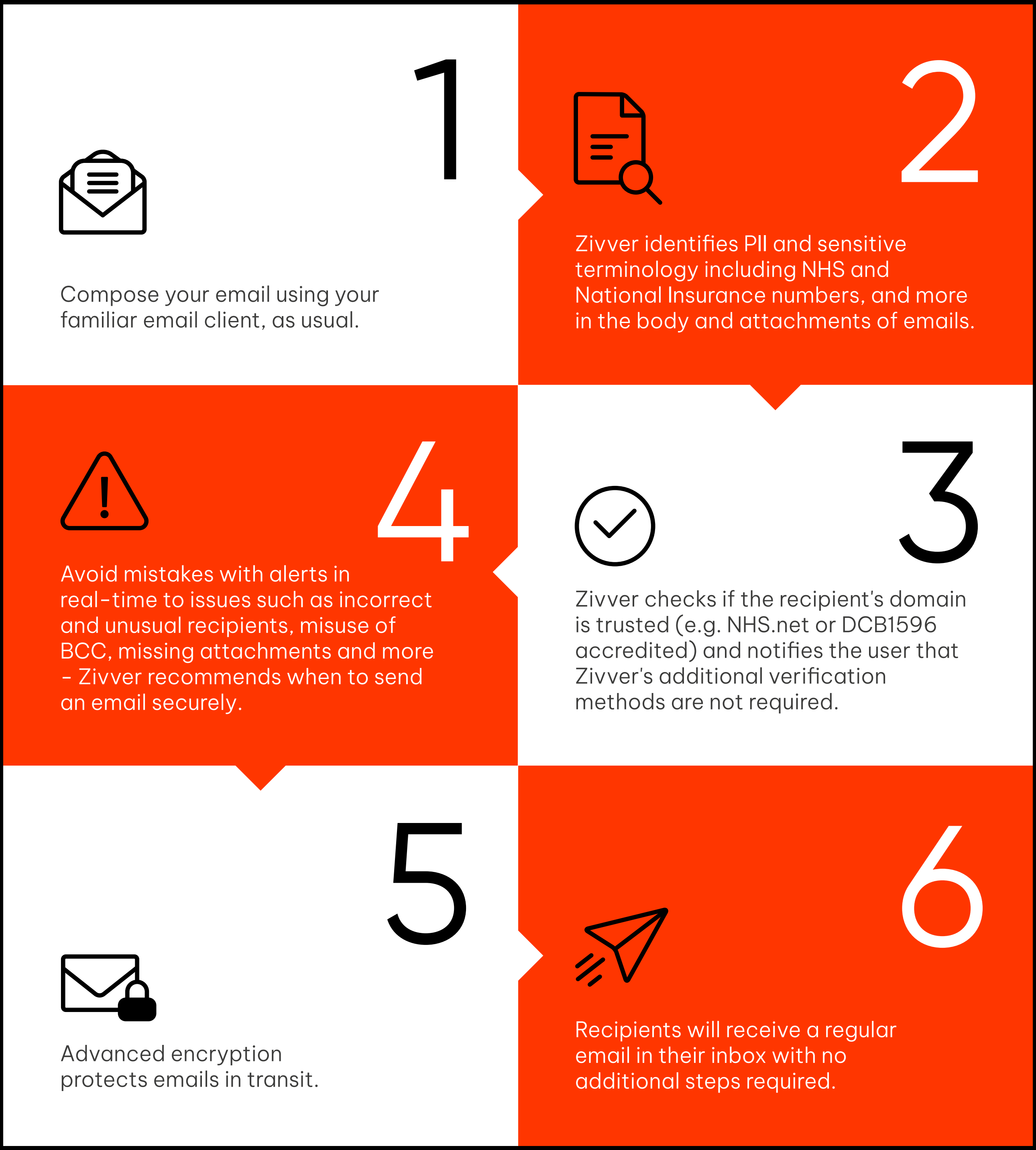
The solution:
Zivver educates users in email best practice in real-time, making security decisions on behalf of the user. Smart machine learning is constantly learning from user behavior.

> "Zivver's email technology makes doing the right thing easy"
>
> Zivver customer

06

Emailing safely with Zivver – A user experience flowchart

For healthcare providers sending sensitive emails to trusted domains (e.g. NHS.net)



1

Compose your email using your familiar email client, as usual.

2

Zivver identifies PII and sensitive terminology including NHS and National Insurance numbers, and more in the body and attachments of emails.

3

Zivver checks if the recipient's domain is trusted (e.g. NHS.net or DCB1596 accredited) and notifies the user that Zivver's additional verification methods are not required.

4

Avoid mistakes with alerts in real-time to issues such as incorrect and unusual recipients, misuse of BCC, missing attachments and more - Zivver recommends when to send an email securely.

5

Advanced encryption protects emails in transit.

6

Recipients will receive a regular email in their inbox with no additional steps required.

For healthcare providers sending emails to patients & third parties

1

Compose your email using your familiar email client, as usual.

2

Zivver recognises when you are sending sensitive information and recommends when to send it securely.

3

If the email is being sent to a patient (or third party), Zivver's solution identifies this and adds an extra layer of security.

4

As a core function, Zivver ensures that all recipients of Zivver messages go through a 2FA process before accessing their Zivver messages. 2FA options include a one-time code via SMS, or a shared secret password.

5

Your email is sent out of your organisation's domain for authenticity, upholding patient confidence.

6

The patient can then access their email easily and securely by entering their second factor.

8

Zivver's address book remembers patient details, meaning new or previous senders can use the same verification method for future emails to the same recipient.

7

You'll see whether the email has been read and can recall messages at any time.

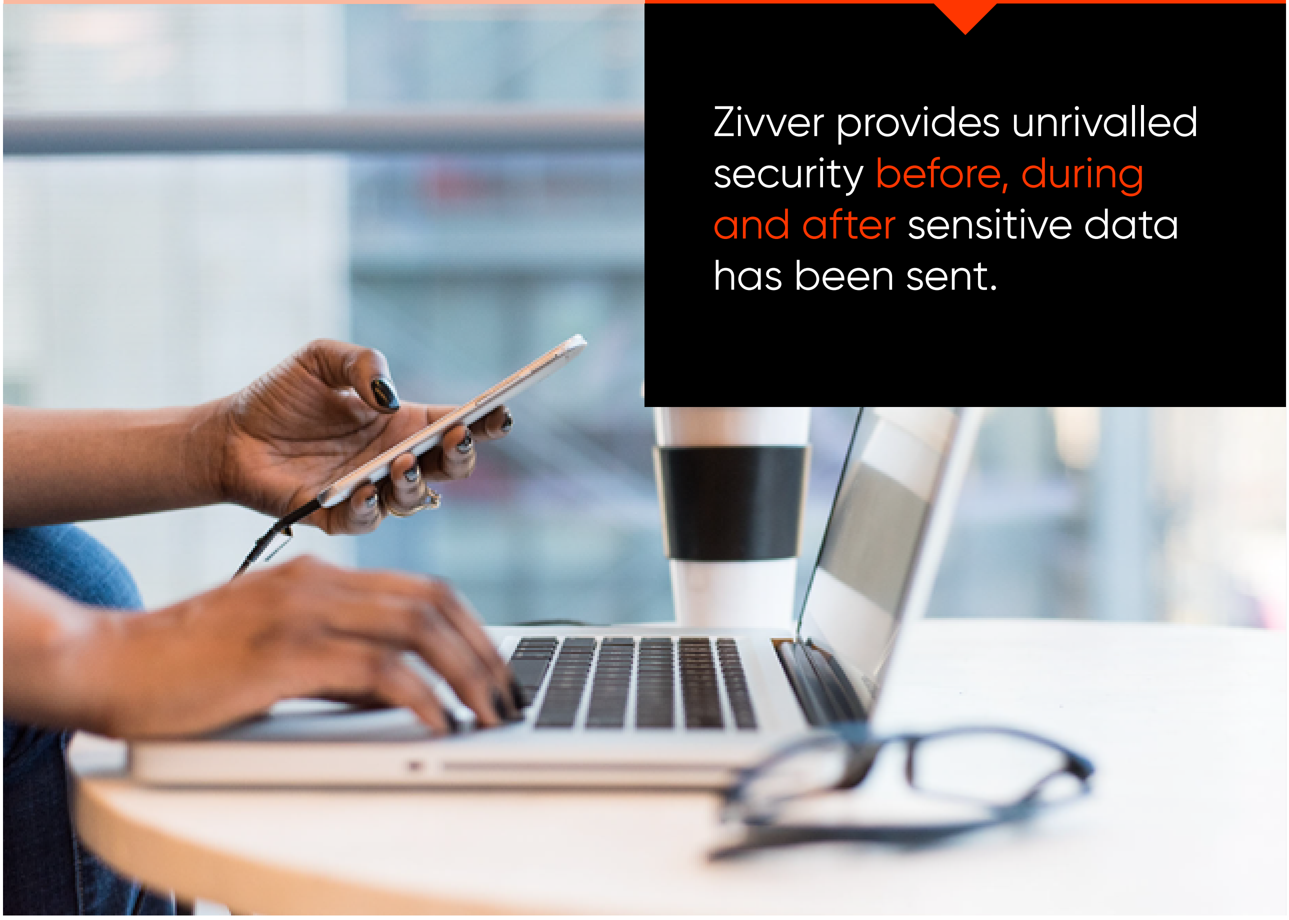
9

The patient does not need to register for an account to access their email.

10

If the patient needs to reply to your email, they can, without creating a Zivver account.

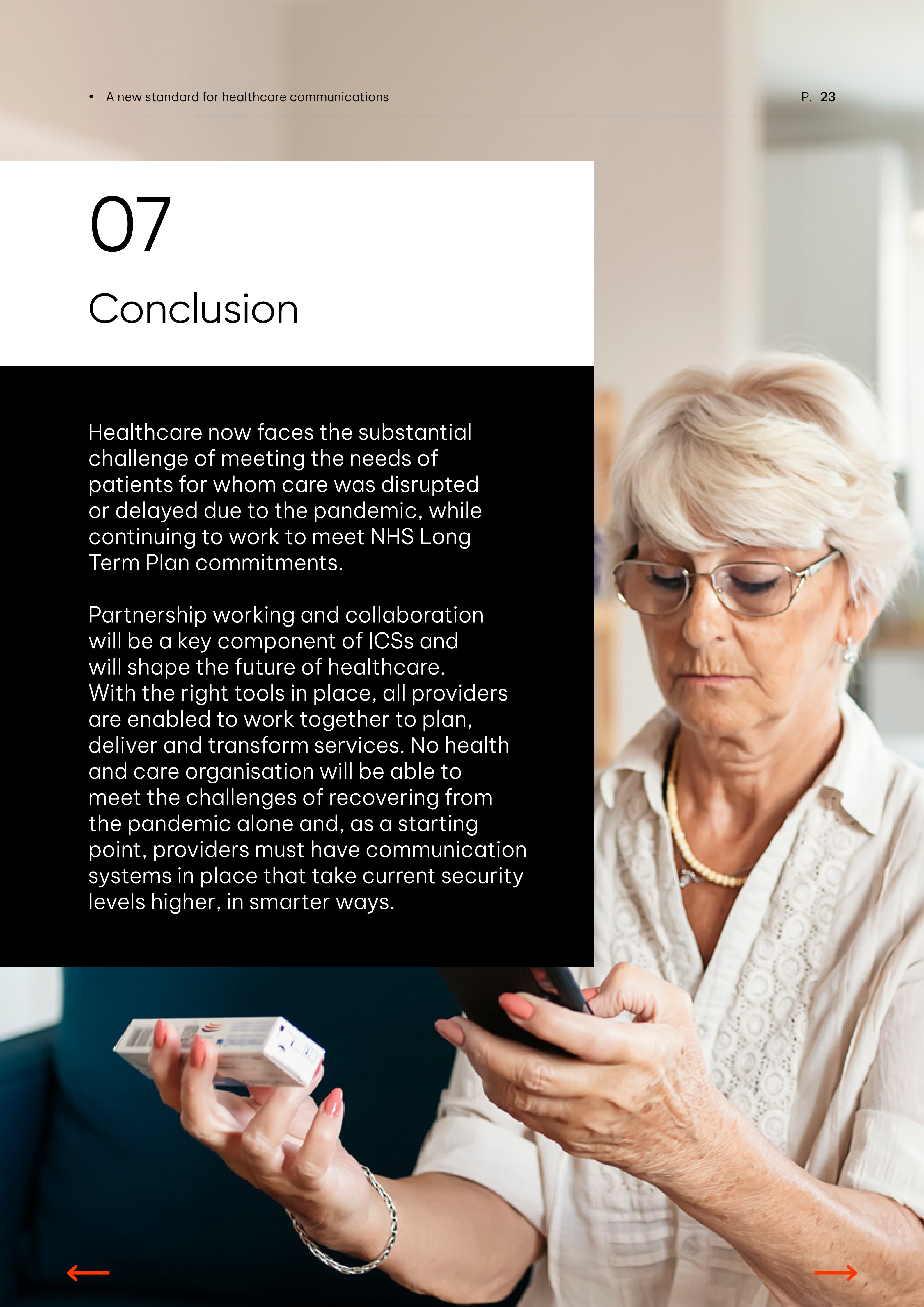
Zivver provides unrivalled security before, during and after sensitive data has been sent.



A secure communication solution

Zivver is an intuitive, user-friendly and secure email solution, complete with the functionality healthcare organisation's need to secure every outbound communication.

> "For a technology that is very complex, Zivver has made the user experience incredibly simple."
>
> Steve Ledoux, Head of IT,
> Douglas Macmillan Hospice



07

Conclusion

Healthcare now faces the substantial challenge of meeting the needs of patients for whom care was disrupted or delayed due to the pandemic, while continuing to work to meet NHS Long Term Plan commitments.

Partnership working and collaboration will be a key component of ICSs and will shape the future of healthcare. With the right tools in place, all providers are enabled to work together to plan, deliver and transform services. No health and care organisation will be able to meet the challenges of recovering from the pandemic alone and, as a starting point, providers must have communication systems in place that take current security levels higher, in smarter ways.

Email will likely remain the most widely used method for healthcare providers to communicate long into the future. But, as email was not designed as a secure communication medium, it is critical for healthcare providers to protect the confidentiality and integrity of email communications for staff and patients.

As healthcare organisations move beyond the pandemic, there is great opportunity for every provider to modernise their email communications, empowering staff to embed security

Zivver’s integrated email communications platform is a key example of digital communications making a significant difference to the healthcare sector, enabling future-proofed, secure healthcare transformation.

GOV NEWS
DIRECT

This paper was built in partnership with GovNewsDirect. GovNewsDirect specialise in facilitating innovative and engaging partnerships between the private and public sector.

zivver

Zivver
Kon. Wilhelminaplein 30
1062 KR Amsterdam, Netherlands

+31 85 016 0555
contact@zivver.com

www.zivver.com

linkedin.com/company/zivver facebook.com/zivver @zivver_en

←