Hawsons Chartered Accountants
Latest News

April | 2024

Healthcare Insight

In this issue:

Hawsons

Big firm expertise,
small firm personal attention

Hawsons Chartered Accountants
Latest News

Scott Sanderson
Partner

Introduction

Welcome to our latest healthcare newsletter. Since our last edition, the government announced its Spring Budget where an additional £2.45 billion of day-to-day funding to support the NHS was announced. However, other healthcare areas including care homes and pharmacies have not received any significant additional government funding or support de-spite struggling over their immediate future.

In this edition of the newsletter we will discuss:

- Care England launch plan to solve care home recruitment crisis
- Pharmacy First Launch - Almost half the UK were not aware
- GP contract referendum
- BVA launch 'Return to Work' toolkit to tackle staffing problem

If you have any questions about the contents of these articles, please do not hesitate to contact us.

Scott Sanderson
Partner

Care England launch plan to solve care home recruitment crisis

Overview

In response to the pressing need to tackle the ongoing recruitment and retention challenges faced by the adult social care sector in England, Care England has taken a proactive step forward by introducing an end-to-end solution. As the largest representative body of independent providers of adult social care in the country, Care England's initiative aims to alleviate the strain on care providers and local authorities grappling with staffing shortages.

Recruitment and retention challenges

The adult social care sector has been grappling with unprecedented challenges in recruiting and retaining qualified professionals, exacerbated by demographic shifts and a surge in demand for care services. According to Care England and Hft's 2023 Sector Pulse Check report, workforce costs emerged as the most significant financial pressure for adult social care providers. The ramifications of staffing shortages have been profound, with 44% of providers forced to reject new admissions in 2023, over half resorting to increased agency usage, and 18% shutting services altogether. In addition to this, the introduction of impending measures that will reduce the flow of international recruits into the care sector.

Care England's Partners with four organisations to enhance recruitment and retention

In light of these multifaceted challenges, Care England has forged partnerships with four organisations—Care Character, Care Friends, Jobtrain, and Vivup. Individually, these entities have demonstrated the capacity to enhance recruitment and retention rates within the sector. However, by synergising their efforts, they collectively offer a holistic solution capable of addressing the sector-wide vacancy rate, enhancing the quality and development of carers, reducing turnover rates, and substantially lowering costs for providers.

Care Pharmacy First Launch - Almost half the UK were not aware

What is the Pharmacy First Initiative?

Health leaders across England are celebrating the much-anticipated launch of the Pharmacy First service, marking a significant step forward in healthcare accessibility and efficiency. With over 90 percent of pharmacies onboard, the government heralds this initiative as ground breaking, aiming to alleviate pressure on GP services by providing pharmacists with pathways to assess and treat patients with common conditions.

What does the Pharmacy First initiative aim to achieve?

The Pharmacy First service aims to revolutionise patient care by empowering pharmacists to address minor ailments promptly, effectively, and conveniently. By leveraging the expertise of pharmacists and the accessibility of community pharmacies, the initiative seeks to free up an estimated 10 million GP appointments annually. This approach aims to enhance patient experience and optimise resource allocation within the healthcare system.

The majority unaware of Pharmacy First

Despite the enthusiasm among healthcare leaders, a recent survey conducted by YouGov and pharmacy technology platform Charac revealed a notable gap in public awareness regarding Pharmacy First. Shockingly, nearly half of the respondents who utilise pharmacies were unaware of the scheme's imminent launch. Moreover, only 23 percent indicated pharmacies as their primary point of contact for minor health concerns prior to the initiative's introduction.

Perhaps the most difficult challenge will promoting the Pharmacy First Initiative to patients and changing patient behaviour so they see pharmacies as a primary point of contact for any minor health concerns. However, in this regard the survey revealed a promising trend. Following exposure to information about Pharmacy First, the proportion of patients expressing intent to seek assistance from pharmacies before consulting GPs surged to 56 percent. This indicates a considerable shift in patient behaviour and highlights the potential of the initiative to reshape healthcare-seeking habits positively.

The survey, which involved 2,028 participants from England, Wales, and Scotland, underscores the importance of robust communication strategies to disseminate information about novel healthcare services effectively. While the concept of utilising pharmacies as frontline healthcare providers is not new, there remains a significant portion of the population unaware of the comprehensive services pharmacies offer.

2024 Ransomware Trends

The cyber security criminals aren't giving up, and they're not just doubling down either. They are now tripling down. They even have virtual "ransomware supermarkets" for criminals to pop in and buy ransomware in a box with a set of instructions so even more criminals can lurk inside your network for weeks on end, planning their attack to maximise the havoc to your business. In this article, we look at some of the ransomware attack trends of 2024.

Current ransomware attack trends that will continue into 2024

In this section, we identify current ransomware attack trends that are expected to continue into 2024.

Supply chain attacks

Supply chain attacks do not just attack a single victim, they usually infiltrate an entire organisation compromising its suppliers or service providers. These attacks exploit the interconnected nature of modern supply chains, leveraging trusted relationships to gain unauthorised access to valuable data and systems. Once inside, attackers deploy ransomware, a type of malicious software that encrypts files or systems, rendering them inaccessible until a ransom is paid. Whilst this is not a new trend these types of ransomware attacks will likely continue. This is because the attackers will usually demand a large ransom because of the types of organisations they target, making it a very lucrative type of ransomware attack.

Triple extortion ransomware attacks

Triple extortion ransomware attacks operate on a three-pronged strategy, combining traditional encryption-based ransomware tactics with additional methods of extortion. The three elements typically include:

- Data encryption
- Data theft
- Reputational damage

In this type of attack, the attackers will seek to infiltrate the victim's network to disrupt operations before stealing sensitive information and demanding huge ransoms knowing that the threat of public exposure could tarnish the reputation of the organisation.

Continued overleaf

2024 Ransomware Trends (continued overleaf)

Ransomware as a service (RaaS)

These days, ransomware attackers don't even need to code their ransomware. RaaS is a pay-for-use malware that provides attackers the correct coding to launch and maintain a ransomware attack which now gives more individuals the opportunity to launch a ransomware attack.

Attacking unpatched systems

Ransomware attacks exploit vulnerabilities in computer systems to infiltrate networks and encrypt critical data, rendering it inaccessible until a ransom is paid. Software companies announce the vulnerabilities they have fixed including the background to what the problem is, and the criminals use that information to set up automated scans across the internet for vulnerabilities.

Phishing attacks continue and are even more sophisticated

Phishing ransomware attacks typically begin with a deceptive email or message designed to lure unsuspecting users into clicking on a malicious link or downloading an infected attachment. Once the victim interacts with the phishing content, an innocent-looking payload is deployed onto their system which can then download the ransomware and set it up without the user knowing anything about it.

After a period of planning, the criminals set the ransomware off encrypting critical files and locking users out of their data. In some cases, ransomware variants may also exfiltrate sensitive information before encryption, providing the criminals with additional leverage to coerce victims into paying a ransom. Whilst this is now a very well-known method of ransomware attack it is still one that is used regularly by attackers and there are no signs of phishing attacks ending.

Ransomware trends for 2024 and beyond

We are now going to explore some new ransomware trends that are expected to evolve into 2024 and beyond.

Attack methods that will evolve to exploit cloud and VPN infrastructure

It is to be expected that ransomware attacks on VPN infrastructure exploitation will become more sophisticated. This will present significant challenges for organisations that use VPNs for remote working and secure communications. The likely attack methods will be on outdated software with security vulnerabilities, weak passwords and multi-factor authentication.

2024 Ransomware Trends (continued overleaf)

Generative AI could become a huge issue

It is predicted that 2024 will be a huge year for the implementation of AI to help organisations operate more efficiently. However, the rise of generative AI could make it easier for attackers to create more advanced phishing campaigns more efficiently, which means they will be able to target more individuals and organisations with their attacks.

How to mitigate against ransomware attacks?

1.Employee education and awareness

One of the most critical components of ransomware mitigation is educating employees about the risks of cyber threats, including phishing scams and social engineering tactics commonly used by ransomware operators. Regular training sessions and awareness programs can help employees recognise suspicious emails, links, and attachments, empowering them to take proactive measures to prevent ransomware infections.

2.Implement robust email security measures

Since many ransomware attacks originate from phishing emails, organisations should deploy robust email security solutions to detect and block malicious messages before they reach end-users inboxes. Advanced threat detection mechanisms, such as machine learning algorithms and sender authentication protocols, can help identify and neutralise phishing attempts in real time, reducing the likelihood of successful ransomware infections.

3.Regular Software Patching and Updates

Keeping software and operating systems up to date with the latest security patches and updates is essential for mitigating the risk of ransomware attacks. Vulnerabilities in software applications are often exploited by threat actors to gain unauthorised access to systems, making timely patching updates a critical defense mechanism against ransomware exploits. Organisations should establish robust patch management processes to identify, prioritise, and apply security updates promptly.

4.Implement Access Controls and Privilege Principles

Limiting access to sensitive data and systems through access controls and privilege principles can help prevent unauthorised users from modifying or encrypting critical files in the event of a ransomware attack. By restricting access to only those individuals who require it to perform their job functions, organisations can reduce the attack surface and mitigate the potential impact of ransomware infections.

2024 Ransomware Trends (continued overleaf)

5. Backup and Disaster Recovery Planning

Implementing robust data backup and disaster recovery mechanisms is essential for mitigating the impact of ransomware attacks. Organisations should regularly back up critical data to offline or cloud-based storage repositories and test their backup restoration procedures to ensure data integrity and availability in the event of an attack. A comprehensive disaster recovery plan should outline the steps to be taken to restore operations and minimise downtime following a ransomware incident.

6. Network Segmentation and Intrusion Detection

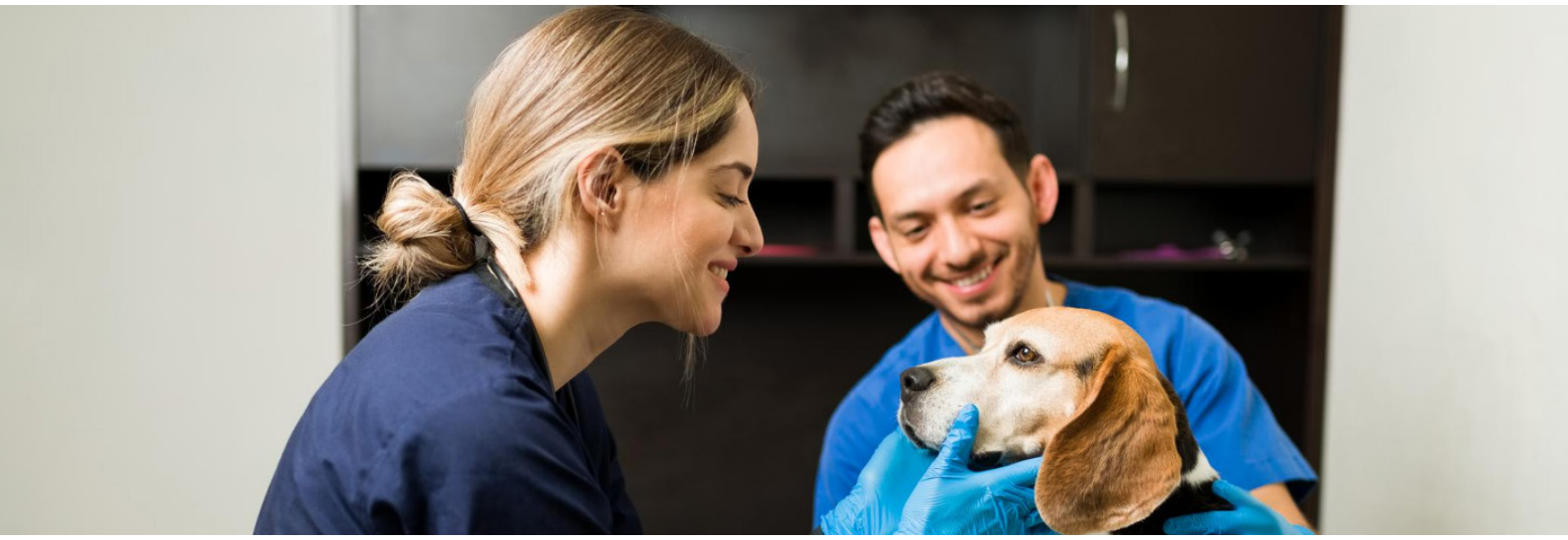
Segmenting networks and implementing intrusion detection systems can help contain the spread of ransomware within an organisation's infrastructure and detect anomalous behaviour indicative of a ransomware attack. By isolating critical systems and monitoring network traffic for signs of malicious activity, organisations can identify and respond to ransomware threats more effectively, minimising the impact on their operations.

Cyber insurance

Even if you've protected your business to the highest level your budget will allow, that protection can still be breached. The mindset has to be one of planning both to prevent the criminals from accessing your network and planning for what happens if they do. Cyber insurance coverage needs to be checked annually to make sure you have the right type and level of coverage so that if your data is exposed your business is protected. As an example, if customer records are exposed, buying identity theft insurance can be very expensive.

Conclusion

To conclude, the ransomware criminals aren't giving up and A.I will only help criminals to work smarter and faster and make phishing attacks more plausible. It doesn't take much imagination to see how criminals could use A.I to take the voice from a YouTube video of your CEO and use that in a social engineering phone call to one of your employees so, if you haven't done it recently, now is the time to review your protection and recovery against ransomware.



BVA launch 'Return to Work' toolkit to tackle staffing problems

For veterinary practice, recruitment and retention have long been persistent hurdles. Fostering positive workplace environments is pivotal not only in attracting fresh talent but also in enticing skilled professionals back into the profession. To confront this issue head-on, the British Veterinary Association (BVA) has unveiled a 'Return to Work' toolkit tailored to assist its members in re-entering veterinary workplaces and to aid employers and managers in integrating these 'returners' seamlessly into their teams.

Recruitment and retention statistics

Recent data from BVA's Voice of the Veterinary Profession Autumn 2023 survey revealed that 17% of veterinarians are actively contemplating leaving the profession within the next five years, while an additional 19% remain uncertain about their future in the field. These statistics underscore the urgent need for employers to consider avenues for better supporting their staff and potential returners alike, with the aim of enhancing recruitment, retention, and overall job satisfaction within their teams.

Why are veterinarians stepping away from the profession?

Various factors prompt veterinarians to step away from their careers, with one of the most prevalent being the addition of a new child to the family. Insights from BVA's Voice of the Veterinary Profession Spring 2023 survey reveal that one in three veterinarians has taken parental leave at some point during their career. Of note, female veterinarians are more likely to take such leave (40%), yet the level of support they receive from their employers during their absence and subsequent return to work is notably lower compared to their male counterparts.

BVA toolkit

The toolkit has been launched as part of the BVA's Good Veterinary Workplace and encompasses support for both veterinary professionals seeking to re-enter the workforce after a hiatus and the employers and managers welcoming them back into their ranks.

The toolkit is exclusively accessible to BVA members and the resources encompass comprehensive guidance for employees, managers, and employers, supplemented by downloadable checklists tailored to each party's needs. Additionally, a series of case studies will delve further into the challenges and rewards of returning to work. This initiative complements BVA's existing suite of supportive materials designed to address various workplace issues, including pay, flexible working arrangements, and menopause. The recently launched BVA employment hub further provides swift access to support and guidance on common queries encountered in veterinary workplaces.

GP contract referendum

All members of the General Practitioners' profession affiliated with the British Medical Association (BMA) have been asked to participate in a pivotal single-question referendum. The referendum seeks to gauge their acceptance of the General Medical Services (GMS) contract proposed for the year 2024/25.

Running from 7th to 27th March, the referendum poses a straightforward query: Do you approve of the 2024/25 GMS contract for general practice as presented by the government and NHS England, Yes or No? Participation in the referendum is open to all members of the General Practitioners' community under the auspices of the BMA, encompassing partners, salaried GPs, locum GPs, and GP registrars.

Purpose of the referendum

During a BMA webinar held on 6th March, Dr. Katie Bramall-Stainer, Chair of the BMA England's GP committee, clarified that the referendum serves as a gauge of sentiment across general practice and is not a ballot concerning industrial action. However, she announced that the BMA plans to host focus groups with GPs during June and July at various roadshows to explore potential forms of industrial action for the autumn. Dr. Bramall-Stainer outlined several prospective actions for GPs later in the year.

Encouraging non-member GPs to join the BMA to voice their opinions, Dr. Bramall-Stainer emphasised the national significance of the contract and the necessity of a united front within the national trade union. She underscored the imperative for collective input, stressing that disengagement would undermine the cause of general practice.

The referendum, Dr. Bramall-Stainer asserted, provides an avenue for NHS England and the government to hear the viewpoints of GPs on a large scale regarding the proposed contract for 2024/25.

2024/25 proposed contract

The proposed contract, stated for implementation from 1st April, represents the third consecutive imposition and offers only a 1.9% increase in practice funding. This follows years of sub-inflationary increases due to the barrier of the five-year contract agreed upon in 2019.

The BMA has raised concerns over the real-term reduction in funding that the contract imposition will bring in April, rendering the business model of practices unsustainable.

Continued overleaf

GP contract referendum (continued)

Last week, the BMA indicated that practices would require an 8.7% increase in funding merely to restore levels to those of 2019. Dr. Bramall-Stainer reiterated this demand during the webinar, alongside advocating for more substantial increases for certain payments to practices, such as stagnant immunisation payments over recent years.

Furthermore, Dr. Bramall-Stainer disclosed that various 'cost-neutral' proposals put forth by the BMA were rebuffed by the government and NHS England during negotiations. This included, allowing Primary Care Networks (PCNs) to finance GP supervision time for additional role staff using Additional Roles Reimbursement Scheme (ARRS) funds and permitting practices to adopt limited liability partnerships. In urging GPs to express their opinions on the proposed contract, Dr. Bramall-Stainer emphasised the importance of a collective and resounding message from the myriad of voices within general practice.

What was the result of the vote?

Following the closure of the referendum on 27th March, the results shortly followed which revealed that just over 19,000 GPs and GP registrars took part in the survey and 99.2% of them voted no in this referendum. This demonstrates that GPs across the country are overwhelmingly unhappy with the new contract.

The GP committee of the BMA convened on 28th March to deliberate the results and consider there next steps. Subsequently, the committee will publish its vision for general practice in May, serving as a manifesto for the forthcoming general election, ahead of the summer roadshows dedicated to discussing potential industrial action.

Dr. Bramall-Stainer also anticipated the possibility of further negotiations with the government in August or September following the publication of recommendations on pay for 2024/25 by the Doctors' and Dentists' Review Body (DDRB). GPs, previously excluded from this process due to pre-agreed uplifts within the five-year GP contract, will now be covered by the DDRB report.

The timeline for key events is as follows:

- 7th to 27th March: Referendum period
- 28th March: BMA England GP committee convenes to discuss results
- 1st April: Contract imposition
- May: Publication of GP committee's vision for general practice
- June/July: BMA roadshows to discuss industrial action, development of industrial action plan, and anticipation of DDRB pay report
- August/September: Potential further negotiations following DDRB report
- Autumn onwards: Potential industrial action

Get in touch

Healthcare experts

Hawsons has a dedicated team of specialist healthcare accountants in Sheffield, Doncaster and Northampton.

The healthcare sector continues to become ever more specialised, with changes in legislation and funding affecting both clinical and non-clinical matters. At Hawsons our team of specialist healthcare accountants offer professionals advice and guidance that is tailored to their individual needs and requirements, providing a full range of proactive services.

We pride ourselves on the in-depth knowledge and experience our team have developed in a number of specialist areas, across the healthcare sector, including GPs, care homes and pharmacies.

Scott Sanderson
Partner
0114 266 7141
ss@hawsons.co.uk

Sheffield Office
Pegasus House
463A Glossop Road
Sheffield, S10 2QD

David Owens
Partner
01604 645600
davidowens@hawsons.co.uk

Northampton Office
Jubilee House
32 Duncan Close, Moulton Park
Northampton, NN3 6WL

Dan Wood
Partner
01302 367 262
dw@hawsons.co.uk

Doncaster Office
5 Sidings Court
White Rose Way
Doncaster, DN4 5NU

Hawsons