Care Quality Commission

Doctor Care Anywhere Limited

Doctor Care Anywhere

Inspection report

3rd Floor, The Corner Building
91-93 Farringdon Road
EC1M 3LN
Tel: 0330 088 4980
Website: www.doctorcareanywhere.com

Date of inspection visit: 14 November 2017
Date of publication: 11/12/2017

Overall summary

We carried out an announced focussed inspection on 14 November 2017 to ask the service the following key questions: are services safe and effective?

Our findings were:

Are services safe?

We found that this service was providing safe care in accordance with the relevant regulations.

Are services effective?

We found that this service was providing effective care in accordance with the relevant regulations.

CQC inspected the service on 24 May 2017 and asked the provider to make improvements regarding their arrangements for checking patients' identities, sharing information with patients' registered GPs and access to patient records for patients aged 11-18 years. We checked these areas as part of this focussed inspection and found the service had taken prompt action to put in place effective processes to address the areas identified for improvement during the previous inspection.

Doctor Care Anywhere provides consultations with GPs via online conferencing. Patients pay either a subscription to the service or purchase a one-off consultation, and the service also holds contracts with large companies to provide GP consultations to their staff and with insurance companies for the benefit of their members. Patients are able to book appointments at a time to suit them and with a GP of their choice via an online portal. GPs, working remotely, conduct consultations with patients and, where appropriate, issue prescriptions.

Our key findings were:

- The provider had effective systems in place to check the identity of patients, which included checking photographic identity documents.
- The provider had processes in place to ensure that young people, who were assessed as having capacity to make decisions about their care, could keep their medical records private from their parent/guardian. These arrangements complied with national guidance.
- The provider had processes in place to collect information about patients' registered GPs, and encouraged patients to provide consent for information to be shared with their registered GP. In cases where patients did not provide consent, GPs would make a decision about whether it was in the best interest of the patient to provide treatment.
- The provider had introduced a system for information sharing with the GPs who worked for them, most of whom worked remotely. All GPs working for the service had access to an online platform which was used for information sharing, online discussion, and peer support. We also saw evidence of this platform being used for educational purposes, such as group discussions about case studies.

Professor Steve Field CBE FRCP FFPH FRCGP

Summary of findings

Chief Inspector of General Practice

Summary of findings

The five questions we ask about services and what we found

We always ask the following five questions of services.

Are services safe?

At our previous inspection on 24 May 2017 we found a breach in Regulation 17 (good governance) of the Health and Social Care Act 2008 (Regulated Activities) Regulations in respect of access to patient records for patients aged 11-18 years. We also found that the provider needed to ensure they had arrangements in place to verify patient identity and that only those patients with appropriate responsibility are able to access records relating to registered children, and that where appropriate patient information is shared with the registered GP.

These arrangements had improved when we undertook a follow up inspection on 14 November 2017. The service is now providing safe services.

- Following the previous inspection, the service had introduced a process for checking the identities of patients who were nominated family members of existing account holders. This included checking photographic identification.
- Following the previous inspection, the service had amended its policy in relation to the access to medical records for patients aged 11-18 years. The new policy allowed for young people who were assessed as having capacity to make decisions about their healthcare, to request that their medical records were not shared with their parent/ guardian. Young people, who were assessed as having capacity to make decisions about their healthcare, were also able to hold their own patient profile which only they could access.

Are services effective?

At our previous inspection on 24 May 2017 we found a breach in Regulation 17 (good governance) of the Health and Social Care Act 2008 (Regulated Activities) Regulations in respect of access to patient records for patients aged 11-18 years. We also found that the provider needed to ensure they had arrangements in place to verify patient identity and that only those patients with appropriate responsibility are able to access records relating to registered children, and that where appropriate patient information is shared with the registered GP.

These arrangements had significantly improved when we undertook a follow up inspection on 14 November 2017. The service is now providing effective services.

- The service encouraged all patients to provide details of their registered GP and patients were asked during every consultation whether they consented for details of the consultation to be shared with their registered GP. In cases where consent was provided, a copy of the consultation record was sent to the patient's registered GP. Where consent was denied, the service's GP would discuss the benefits of sharing information with the registered GP. The decision to provide treatment to a patient, where there was no consent to information being shared with the registered GP, was made based on whether this would be in the best interest of the patient.

Doctor Care Anywhere

Detailed findings

Background to this inspection

Doctor Care Anywhere provides consultations with GPs via video conferencing. Patients pay either a subscription to the service or purchase a one-off consultation, and the service also holds contracts with large companies to provide GP consultations to their staff and with insurance companies for the benefit of their members. Patients are able to book appointments at a time to suit them and with a GP of their choice via an online portal. GPs, working remotely, conduct consultations with patients and, where appropriate, issue prescriptions or make referrals to specialists; consultation notes are available for patients to access. The service has also developed a portal which allows patients to monitor data about their health and track symptoms; this information is available to consulting GPs at the service as part of the patient's medical record.

At the time of the inspection the provider had submitted a registered manager application, as the previous registered manager had recently left the organisation. A registered manager is a person who is registered with the Care Quality Commission to manage the service. Like registered providers, they are 'registered persons'. Registered persons have legal responsibility for meeting the requirements in the Health and Social Care Act 2008 and associated Regulations about how the service is run.

Why we inspected this service

We carried out a comprehensive inspection of Doctor Care Anywhere on 24 May 2017, and asked the provider to make improvements regarding their arrangements for checking patients' identities, sharing information with patients' registered GPs and access to patient records for patients aged 11-18 years. The service provided an action plan in respect of these issues shortly following the initial inspection.

We carried out this inspection under Section 60 of the Health and Social Care Act 2008 as part of our regulatory functions in order to check that the service had followed their action plan and that the changes they had introduced following the initial inspection were effective and well-embedded. This inspection was planned to check whether the service was meeting the legal requirements and regulations associated with the Health and Social Care Act 2008.

How we inspected this service

Our inspection team was led by a CQC Lead Inspector accompanied by a GP specialist advisor.

During our visits we:

- Spoke with a range of staff.
- Reviewed organisational documents.
- Reviewed a sample of patient records.

This was a follow-up inspection, focussing only on areas where the service was found to be failing to comply with regulations during the initial inspection in May 2017. This inspection looked at two of the five question we usually ask to get to the heart of patients' experiences of care and treatment:

- Is it safe?
- Is it effective?

Are services safe?

Our findings

At our previous inspection on 24 May 2017 we found a breach in Regulation 17 (good governance) of the Health and Social Care Act 2008 (Regulated Activities) Regulations in respect of access to patient records for patients aged 11-18 years. We also found that the provider needed to ensure they had arrangements in place to verify patient identity and that only those patients with appropriate responsibility are able to access records relating to registered children, and that where appropriate patient information is shared with the registered GP

These arrangements had improved when we undertook a follow up inspection on 14 November 2017. The service is now providing safe services.

Information to deliver safe care and treatment

The service held contracts with several large companies to provide GP consultations to their employees. Those who were eligible provided consent for their employer to pass their details to the service, who would then create a personal account for the employee. The service relied on identity checks performed by the patient's employer to verify their identity for the initial account set-up, and thereafter, patients accessed the service by entering personal log-in details.

Some of the service's corporate contracts included use of the service by patients' family members. Registered account holders could set-up profiles for children aged under 18, which could be viewed by the main account holder only. At the time of the initial inspection, the service did not check that the main account holder had parental responsibility for the children they were adding to their account. Following the initial inspection, the service provided evidence that they had amended their policy to require evidence of parental responsibility to be provided before a child could be registered to use the service.

During the re-inspection, we viewed the service's computer system and saw evidence that systems had been put in place whereby accounts for dependents of registered patients could only be activated once the registered patient had provided evidence of parental responsibility (such as the child's birth certificate or passport).

In cases where registered account holders wanted to add an adult family member to their account, the account holder would nominate the family member to register with the service, and the system would send the nominated person an invite to set up their own account. Once set up, the account was linked to the main account holder, but could not be viewed by them. At the time of the initial inspection, the service did not carry-out any identity checks for patients who set up accounts in this way. Following the inspection, the provider reviewed and amended their policy to require nominated family members to provide evidence of their identity prior to them using the service. For those patients who were already registered with the service, accounts were suspended and affected patients were directly notified that they must provide evidence of their identity before they could use the service again. Information was also provided about this on the service's website, including details of how patients could access alternative medical advice should they need to in the interim.

During the re-inspection we viewed the service's operating system in relation to the system for creating accounts. We saw that patients applied for an account by entering their personal details, and then had to provide photographic identification and a profile photograph. The information entered and the identity documents were then reviewed by a member of the service's customer service team, who would compare the photographs and check the information entered against that on the identity document. Patient accounts were only activated once these checks had been completed.

At the time of the initial inspection, in cases where an account holder had set up an account for a child, the account holder could view details of the child's account, including medical records, until the child reached the age of 18 years. The service's policy stated that access to a child's account by the main account holder could be blocked when the child turned 16 years, but only if this was requested by the young person, and with the permission of the main account holder. This policy was not in line with national guidance relating to access to the medical records of young people, and at the time of the initial inspection the service was in the process of reviewing this.

Following the initial inspection, the service provided a copy of their updated policy on access to young people's medical records to bring them in line with national

guidance. The new policy stated that during consultations with all young people aged 11-16 years, the GP would conduct a capacity assessment. If the young person was found not to have capacity to independently manage their own healthcare, notes of the consultation would be made available to the parent/guardian account holder. If the young person was found to have capacity, they were asked for consent for their medical records to be shared with the parent/guardian account holder, and if consent was declined, individual consultation records were obscured from the parent/guardian account holder. Patients aged 16-18 years were presumed to have capacity, and therefore, they were asked at each consultation whether they consented to their records being shared with the parent/guardian account holder, and they could request for an independent account to be set up without the need for the main account holder to provide permission.

During the re-inspection we viewed the service's operating system and saw evidence of the changes made since the previous inspection. This included the inclusion of a field for clinicians to complete to record whether the young patient had provided their consent for the notes of the consultation to be shared with the main account holder. Completion of this field was mandatory, and the system had been set up so that the consultation record could not be closed unless this field had been completed.

Are services effective?

(for example, treatment is effective)

Our findings

At our previous inspection on 24 May 2017 we found a breach in Regulation 17 (good governance) of the Health and Social Care Act 2008 (Regulated Activities) Regulations in respect of access to patient records for patients aged 11-18 years. We also found that the provider needed to ensure they had arrangements in place to verify patient identity and that only those patients with appropriate responsibility are able to access records relating to registered children, and that where appropriate patient information is shared with the registered GP.

These arrangements had improved when we undertook a follow up inspection on 14 November 2017. The service is now providing effective services.

Coordinating patient care and information sharing

During the initial inspection we found that notes of consultations were available for patients to access, and these could be downloaded by the patient and shared with their registered GP if they chose to do so. We were told that the service had the facility to contact patients' registered GPs to share information about consultations, but at the time of the inspection they did not routinely do so (except in circumstances where staff working for the service had safeguarding concerns). The service did not make it mandatory for patients to provide details of their registered GP.

Following the inspection, the service informed us that they had changed their approach, and in future, patients would be asked during every consultation whether they gave consent for consultation notes to be shared with their registered GP; where consent was given, the service would arrange for the consultation record to be shared.

During the follow-up inspection we saw evidence that the service had updated their consultation record template to include a field prompting the service's GPs to ask patients for consent to share information with their registered GP. This was a mandatory field, and the consultation record could not be closed unless this was completed. Where patients provided consent for details of a consultation to be shared, the service sent a copy of consultation records to the registered GP by post. The service was in the process of considering whether it would be possible for this information to be shared electronically, whilst ensuring the security of patients' confidential information.

In cases where the patient declined to provide consent for details of their consultation to be shared with their registered GP, the service's GP would discuss this decision with the patient to ensure that the patient understood why it would be beneficial for information to be shared. Guidance was in place for the service's GPs in order to support them in making decisions about providing treatment to patients in cases where there was no consent to share information. These decisions were made on the basis of whether providing treatment was in the best interest of the patient. In certain circumstances failure to provide consent to share information would result in the service's GP refusing to provide particular treatments. If there was a lack of consent for the sharing of information in relation to a child this was automatically escalated for urgent review by the Clinical Director of the service.