Standards for Identity Checking for Asynchronous Online Primary Care Providers

06 February 2019

This document has been created and collated for the Care Quality Commission (CQC) by a group of asynchronous Online Primary Care Providers.

This includes contributions from:

Health Bridge Ltd (Zava)
Boots Independent Medical Agency (IMA)
Lloydspharmacy Online Doctor
Assured Pharmacy
Index Medical Ltd (Dr Fox)
Treated.com (HR Healthcare Ltd)
iPrimary Care Ltd (Vala)
The Independent Pharmacy

Provider	Name of Provider Sign Off	Role	Date Signed Off
Health Bridge Ltd (Zava)	James Davies	Chief Operating Officer	06/02/19
Boots IMA	Claire Nevinson	Senior Manager	06/02/19
LloydsPharmacy Online Doctor	Matthew Nimmo	Head of Operations	06/02/19
Assured Pharmacy	Robbie Toan	Director	04/02/19
Index Medical Ltd (Dr Fox)	Tony Steele	Medical Director	06/02/19
HR Healthcare Ltd (Treated.com)	Daniel Atkinson	Clinical Director	06/02/19
The Independent Pharmacy	Ant Boysan	Director	06/02/19
iPrimary Care Ltd (Vala)	Shellane Crisostomo	Co-founder	04/02/19

Background and Context

In January 2017 the CQC commenced a round of inspections of online only primary care providers. The CQC acknowledged at the time the variety of service models offered by providers. Following the first round of inspections of registered online primary care providers in England by the CQC (and coordinated inspection activity with the General Pharmaceutical Council where services fell under their regulatory responsibilities), the CQC, along with other UK regulators of primary healthcare issued a letter 24th August 2017 which outlined the themes from the inspections. **Identity of patients was included as an area of concern**. This letter highlighted concerns that offering no confirmation of identity, or reliance on credit card checks in isolation was not sufficient and had significant limitations. The letter suggested that prescribing for potentially unknown patients makes the identification or escalation of safeguarding concerns unreliable and can hinder accurate communication with other healthcare professionals and the safe transfer of clinical information.

The Annex to this letter explained the need for identity checking to facilitate handover of care, communicating with other health care providers, supporting the safeguarding of adults at risk and vulnerable children. With providers to be asked to demonstrate the protocols used to identify and verify the patient at the start of the first and subsequent consultations and to explain how providers protect against patients using multiple identities.

The CQC has asked providers to demonstrate that they have assured themselves that the patient is who they say they are for the purposes of safe and effective care and treatment, and how the provider manages any perceived risks, including safeguarding of vulnerable children and adults at risk of abuse and neglect.

At this point in time, there was **no agreed national standard** for confirmation of online identity for health services. This lack of standardisation and approach was further recognised in March 2018 when CQC published its end of inspection review report The state of care in independent online primary health services Findings from CQC's programme of comprehensive inspections in England.

In this report the CQC inspectors acknowledged that there has been a **lack of clear guidance** for online providers on the issue of identity checking and that, even with checks in place, it is difficult to eliminate the associated risks entirely. In particular this report identified the difference in approach and risk between those services offering real time video consultations and those providers offering questionnaire based asynchronous risk assessments where identity checking was reported as an area for improvement.

This document gave examples of providers **using external organisations to verify patient details** through national databases and carrying out an effective risk assessment, which concluded that the medicines prescribed were 'low risk'.

The CQC accepted the difference in approach between those providing a questionnaire-based interaction with clinicians, usually for a fixed range of conditions and medicines, and those providing real-time interactive health care by video or telephone consultations.

Against this background, this document sets out the collective views and risk based assessment of **asynchronous online primary care providers**. This paper, and the suggested standards contained within do not apply to those providers offering video consultations or other forms of online interaction where the risk profile and service structure may be different.

GDPR and collecting patient's identification

When collecting any additional data from patients providers always need to consider the rights of the individual when collecting this data. This includes both General Data Protection Regulations as well as health specific.

General Data Protection Regulations set out seven key principles to the collection of data that must be considered and justified.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Caldicot Principles. These include consideration of:

1. Justify the purpose(s) for using confidential information
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data

External Identity Reference Verification (credit reference) standard

On the basis of the end of inspection review, those asynchronous providers that had no system in place to verify identity or that did not have risk assured system in place have sought to implement systems that verify against external databases, using **Experian, Equifax, Lexis Nexus and Onfido** databases to verify patient identities. The use of these external databases provides validation of name, age, date of birth, address and helps to mitigate the risk of children using adult only services.

Without clear and consistent guidance from the CQC on the issue of identity, the industry has adopted identity verification against an external database as the standard for asynchronous consultations. Providers have invested significant time and resource into adopting this approach on advice outlined in the report and on advice from subsequent reinspection.

External Credit reference checks also have the ability to perform **a mortality check** and that the identity has credit active data. In some cases providers are coupling this with the fact that the medicine is sent by recorded delivery to the name and address that has been matched to the identity meaning the risk of providing to non-verified identities is extremely low.

This reference checking **verifies an identity exists**, but does not necessarily establish that it belongs to the person making the order. People might want to use another person's identity because they are under 18 to get around frequency checks, or because they require services for a family member (such as a wife ordering ED medication on behalf of a husband). This reference checking alone does not mitigate against this risk.

Credit reference identity checks become stronger ID verification if delivery is to the **verified address of the patient only,** or the patient collects in person from a location where physical identification must be provided, such as in a Post Office or a community pharmacy (where protocol would require ID - this is the route that has been adopted by some providers).

There are clear technology challenges to implementing this for all patients, and significant risks to the accesses for some patients where this is implemented. The additional barrier that identity checking creates is something that has been considered in recent BASHH/FSRH guidance.

BASHH/FSRH Standards for Online and Remote Providers of Sexual and Reproductive Healthcare Services

On 25th January, BASHH/FSRH published their Standards for Online and Remote Providers of Sexual and Reproductive Healthcare Services. This standard sets out the BASHH position on identity, and does not support the CQC position in all cases.

> *One of the main themes highlighted by the CQC was regarding the need for proof of identity (including age) for users of non-face-to-face services. The FSRH and BASHH feel it is imperative that the level of clinical excellence, safety and care delivered through remote services is not compromised. They do not support the creation of obstacles which may prevent users from accessing these services and which do not currently exist in terrestrial services i.e. proof of identification or UK residence.*

As a result, for sexual health services provided online, providers believe that they **do not always require proof of identification** in cases where they would not be required in a normal face-to-face setting.

For the purposes of this document, providers believe that the most appropriate definition of sexual health services to be that which has been defined by the World Health Organization.

> *"…a state of physical, emotional, mental and social well-being in relation to sexuality; it is not merely the absence of disease, dysfunction or infirmity. Sexual health requires a positive and respectful approach to sexuality and sexual relationships, as well as the possibility of having pleasurable and safe sexual experiences, free of coercion, discrimination and violence. For sexual health to be attained and maintained, the sexual*

> *rights of all persons must be respected, protected and fulfilled". (WHO, 2006a)*

As such, providers believe that this definition covers all aspects of sexual experience including Erectile Dysfunction (ED) and Premature Ejaculation (PE). Indeed, the NHS advise the public to visit a sexual health clinic if suffering from ED. For PE, NHS identify this is as a common sexual problem in men and specifically that PE is one of three main ejaculation problems, while the SPC for a PE treatment links it to "other forms of sexual dysfunction, including erectile dysfunction".
This is further supported from the Health Education England report "Improving the delivery of sexual health services" (September 2018), which recognised sexual dysfunction.

> "*Sexual and reproductive health services include care in contraception, sexually transmitted infections, HIV services, sexual dysfunction, sexual assaults, abortion, genital dermatology, community gynaecology and post-reproductive health issues such as menopause*."

NHS Digital create an NHS Standard

The CQC issued a letter in late 2018 explaining that NHS digital has published DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services (29 June 2018) which will 'form part of our inspection approach from April 2019'. Providers agree with the CQC that in areas of higher risk prescribing, or where long term continuous care and monitoring is required, then it is appropriate to apply the NHS standard and confirm with both an external database, a proof of identification, and visual inspection.

However, the blanket approach to using this standard across all online providers is inconsistent with the risk assessment based approach to providing care, and the implementation of the standard appears disproportionate to the risks involved. The blanket implementation of this standard creates a moral hazard for patients, which will encourage them to use unregistered providers that sit outside of the CQC's jurisdiction. There is significant cost to implementation, which requires months of development work. Providers also believe that for the supply of low risk medications a balance needs to be struck between accessing treatment and the barriers that identity checking may present.

Indeed this is recognised in the standards set out in the Identity Verification and Authentication Standard for Digital Health and Care Services - Specification, pg 6, June 2018:

> *"The necessary security must be put in place, but without making access to digital health and care services so complex or time-consuming that people are deterred from using them."*

Against this background, and in light of the standard, a group of online providers have come together to help create an industry view on how the CQC should approach this areas.

Implementing the NHS Standards : The Case of Asynchronous Providers

The NHS standard, DCB3501, sets out strong criteria for identity checking a validation.

To sufficiently bind a person asserting their identity to an existing medical record, the following is required:

- *An item of official photographic identity (such as a passport or driving licence) from the list in Table 14 in Annex A of GPG 451.*
- *Know that the document appears to be genuine*
- *A physical comparison between the photographic identity and the person asserting their identity, and to link the asserted identity to the medical record.*
- *Examples of ways of carrying out physical comparison may include:*
    - *Being physically present at the point of identity verification*
    - *Online services which enable live comparison of the individual with photographs held on legal documents (such as driving licence or passport)*

If the photographic identity does not include address details, then a further non-photographic piece of Identity Evidence is required. This must include the name and address and be reasonably expected to have been delivered to that address.

The individual is not deceased, by reference to an Authoritative Source such as the Personal Demographics Service (PDS).

There are several challenges for patients and providers with implementing this standard in the private, direct to consumer healthcare space provided by asynchronous providers.

NHS requirements and Providers Implementation

The requirement to prove ID to the NHS Login standard is recognised as justifiable when patients wish to create an online account to access ‘an existing medical record’ – eg: primary care records (highly sensitive data). It is more of a data protection measure than a patient safety measure (although both applicable).

By contrast, creating a *new* online account with an independent medical provider is an entirely different circumstance, where no previously entered sensitive patient data is accessible after creating an account.

As a result, we are seeking agreement with the CQC that in this scenario a lower threshold of identity assurance is appropriate based on risk assessment of the treatment supplied. The data protection aspect in this scenario is when patients need to be authenticated to log-in to the existing account.
Verifying ID to access existing NHS medical records and verifying ID to create a new account to access a limited range of routine treatment online are entirely different

propositions requiring different levels of assurance, and possibly a separate standard that includes different assurance measures.

Implementing this guidance requires a significant investment in IT development, staff training and testing requirements for ID verification along the lines of 'NHS login' and will take many months to fully implement. It is a complex development task and not one that we expect providers to be able to implement ahead of the next round of CQC inspections in April 2019.

Challenges with Identity verification

Providers are also grappling with the effective implementation of the advice to supply identification. Especially as current DVLA advice (D741) when receiving a new driving licence is as follows :

> *"**Protect yourself against identity theft**: Similar to a credit card your driving licence should not be shared, copied or photographed."*

As a result providers are struggling to balance the requirement to gather this data digitally against the needs and protections of individuals.

With recent data breaches affecting many well-known organisations the issue of data protection/security and identity theft is a very real concern felt by patients, and this concern is often expressed to providers where photo ID has been requested. This is different, when the NHS requests such identify:

- As the NHS is a trusted organisation, people have assurance and confidence when providing a digital copy of photo ID than they might have with unknown independent providers, or those that are seen as more commercially focussed.
- NHS Login will (eventually) provide access to all NHS services and departments - multiple independents do not have a centralised ID system.
- Face-to-face vouching is available to the NHS where no digital copy of photo ID is taken, this is not available to independents.
- There is no alternative to the NHS - for patients with ID theft concerns there are many commercial alternatives that do not require submission of photo ID.

No ID verification standard available to non-NHS providers is 100% risk-free and a balance of risk needs to struck.

Minimising the Moral Hazard

Providers put patient care and safety at the heart of what we do. We are deeply concerned about the barriers that identity checking could create for some sections of the public. Indeed, most of the providers offer a telephone alternative to care, which these guidelines do not seem to have taken into account. This creates a conflict between the providers ability to implement the CQC principle of making treatment accessible.

As suggested above, the full implementation of this NHS standard in all treatment areas creates a greater disparity between CQC & non-CQC registered services. The unintended consequence will result in pushing patients towards services with less regulation where the safeguards and barriers to purchase unsafe medications are lower. Indeed, the cost of providing these checks will encourage patients to seek out those that can offer these services without this cost, outside of the regulations. As such, providers want to achieve a solution, which balances the needs of patients, providers and regulators.

Patients and the public don't exist in a vacuum and without a mutually agreed standard any provider whose interpretation falls below the CQC's perceived standard would be forced to subject patients to repetitive identity checking processes for their entire patient database, creating further barriers to patients accessing continuity in healthcare provision.

There is a risk that patients will eventually turn away from the regulated sector, as the barriers are too high, and then seek to access the numerous non-regulated and potentially dangerous alternative providers that exist online.

Transmitting video via a phone to prove likeness and 'realness'

In the market place there exist solutions where videos can be used to provide a likeness of a person to a document. For example, the solution available from Onfido estimates the average video file-size to be 100mb. The solution is a significant barrier both in terms of technological know-how of patient, and also internet speed and bandwidth and carries a significant cost. The current Onfido's solution to verify a patient costs around £6 per check.

Providers currently believe that the full implementation of such a tool would have very damaging impact on the health of patients, and negatively discriminate against those people who struggle with technology.

Research shows that this type of ID verification excludes even more patients than online services do currently. The use of such checks requires a relatively new mobile device that can capture video and photos. Many of the older generation or less financially able, tend to use desktop computers without a camera/webcam, which could unwittingly exclude this group from care.

Authentication

The NHS login standard considers the access to the NHS patient record and calls for 'Strong authentication' as requiring 2-factor authorisation (2FA), usually a code sent to a mobile phone as 'something you have' evidence. 2FA presents a significant barrier particularly to many older patients. Indeed SMS based 2FA is considered by many security experts to be a potential weakness as mobile phones can be impersonated. Providers believe patients should be given an informed choice as to whether they wish to use 2FA to secure their account and the route through which they do this. There are other ways in which users can provide other evidence of 'something you have' as a secondary factor. These include browser cookies, payment card pin numbers, IP addresses or previous deliveries. The extent to which this element of the standard is implemented needs due thought and technical consideration from the regulator.

The Path to a Solution

In many areas of primary care patients are not required to provide evidence of identity in order to access services. For example, any purchase of a Pharmacy only (P) medicine over the counter in a community pharmacy is carried out anonymously. These medications are lower risk and no information is transferred to other clinicians about the supply of such medications. Indeed, in accessing sexual health services or accident and emergency departments patients can remain anonymous (see FSRH/BASHH guidance). In these settings, there are good reasons for this anonymity to help ensure that treatment is provided in the interests of public health.

Indeed, there is regulatory inconsistency between the requirements suggested from the CQC and those operated by GPhC registered prescribers. These regulatory gaps and inconsistencies require further attention, and these gaps have been acknowledged by both regulators. Providers are supportive of these changes being made.

The current level of checking (External Identity Reference Verification) gives providers assurances that a person actually exists and that the details they have provided are correct. It also provides assurances that the person is not deceased.

The providers collectively agree with the CQC position that identity can, in many situations, play an important role in ensuring that patients are who they say they are for the purposes of safe care and treatment. However, providers also believe that identity alone should not act as a barrier to patient receiving care, and therefore a proportionate and risk-based approach to identity verification should be applied to treatment pathways.

Providers also agree with the initial view of the CQC that in most cases no confirmation of identity, or reliance solely on credit card checks in isolation is insufficient. However, providers believe that as a minimum the checks against credit reference databases help to validate the existence and identity of the individual. Providing reference against such databases helps to eliminate fraud and validate the true date of birth of people accessing services.

Against this background, the appendix to this document collates a risk assessment of treatments that are commonly supplied by online asynchronous providers who offer a questionnaire-based approach to the supply of consultations, treatments, and services. This risk assessment framework provides a standard that both providers and the CQC can use to help govern the identity checking arrangements that are in place in their services. In order to support the CQCs desire to learn alongside providers who offer new models of care (Shaping the future). Providers have come together to help generate a standard across the online primary healthcare industry to help provide an agreed risk assessment standard for the providers to work towards.

Audit and Monitoring

As with any change made in a system or process, it is important that providers are able to assess the effectiveness of an intervention and continually check if the risk assessment remains appropriate. It is clear that any significant service change will have unintended adverse consequences. In order to ensure the proposal outlined in this analysis continues to be safe and effective, the providers suggest a period of audit and monitoring following implementation.

The providers suggest a monitoring period of at least 12 months, after which ID verification issues are revisited in collaboration with the CQC. At such a point data can be shared about the effectiveness of the interventions based on data and evidence. This can allow for wider public engagement with the standard.

Appendix 1 - Subject to ongoing work - updates and changes expected - 13-03-2019

Standards for Identity Checking for Asynchronous Providers

In these standards providers use a risk-based scale, which highlights those conditions or areas where identity verification is required.

- *No identity verification required (Low).* The collection of identity verification could have a detrimental impact on patient outcomes for public health reasons (e.g. sexual health assessments).

- *External Identity Reference Verification (Medium)* - Checking the existence of a patient against a credit reference database and using this to confirm the age of the patient. Where people do not exist in a database, verification by identification is required. (e.g, Travel Medication). Supply based on reference delivery address or identity on collection (Post Office or Pharmacy).

- *Credit Reference Verification, Photographic Representation and Identification (High)* – Checking the existence of a patient against a credit reference database and using this to confirm the details of the patient against identification and a likeness comparison of the patient (Complex management, e.g. Asthma, Diabetes, Cholesterol Management)

Risk Assessment by Treatment Areas

Below is a risk assessment framework that outlines the banding of the conditions typically provided (but not fully agreed) by asynchronous providers and our assessment of the risk, and the level of identity checking that is appropriate for these services.

This framework has been agreed upon by providers, taking into consideration the various risk profiles of people in different treatment categories.

Treatment Area/Medicine and Mode of Treatment	**Risk Levels**	**Risk Based Assessment Reasons**
STI testing and supply of test kit by questionnaire	*No identity verification required (Low)*	● Sharing between NHS providers not currently standard ● BASHH/FSRH guidance does not suggest identity checking is required. ● No intervention/prescription being provided ● Increased access to testing widely encouraged for public health reasons ● Widely available from online retailers with no clinical input

Services provided to under 18 year olds eg antimalarials, acne treatment	*No identity verification required (Low)*	● Increases access and availability to under 18 eg in travel where P med is not licenced. (Particularly relevant for families travelling.) ● Limited sharing with NHS required
Erectile Dysfunction (PDE5 inhibitors) and men's health by questionnaire	*No identity verification required (Low)*	● A medicine in this class is available as P meds. In the submission to the MHRA these medications have been recognised as being a lower risk category of medication. ● The medications have a long track record of clinical safety ● NHS advises ED to be treated as a sexual health area. ● BASHH/FSRH guidance suggests that sexual health should be excluded, and additional barriers should not be placed on the service
Premature Ejaculation and men's health by questionnaire	*No identity verification required (Low)*	● Prescribing risk similar to ED ● NHS identifies PE as a common sexual problem in men ● BASHH/FSRH guidance suggests that sexual health should be excluded, and additional barriers should not be placed on the service
Travel Medicine/ Antimalarials by questionnaire	*External Identity Reference Verification (Medium)*	● Many are already P medicines and can be purchased in pharmacies without identity verification ● Usually one-off ● Limited sharing with NHS required
Antibiotics by questionnaire, with or without a face to face element in pharmacy	*External Identity Reference Verification (Medium)*	● Antibiotic custody factors ● Sharing with NHS requirements ● Correct diagnosis and appropriate use within appropriate time frame is vital, ID verification should not result in delay in

		treatment
Hair loss treatment and “lifestyle” medicines (finasteride, norethisterone for period delay, Champix) by questionnaire	*External Identity Reference Verification (Medium)*	● Good safety track record ● Low risk medicines
Minor ailments/common conditions self-managed e.g. hay fever, dry skin, acne,repeat migraine treatments, and others, by questionnaire	*External Identity Reference Verification (Medium)*	● Many available without prescription ● Low risk medicines ● Strong safety track record
STI Treatments by questionnaire	*For further discussion:* *1. No identity verification required (Low)* Or *2. External Identity Reference Verification (Medium)*	● Sharing between NHS providers not currently standard ● Antibiotic stewardship issues may require sharing of data ● Partner notification inconsistencies ● Digital provider ID verification requirements inconsistent with current NHS provider standards
Contraception by questionnaire	*For further discussion:* *1. No identity verification required (Low)* Or *2. External Identity Reference Verification (Medium)*	● Sharing between NHS providers not currently standard ● Digital provider ID verification requirements inconsistent with current NHS provider standards
Complex Disease management (diabetes, cholesterol, asthma, etc) by questionnaire	*Credit Reference Verification, Photographic Representation and Identification (High)*	● Sharing with NHS required ● Chronic treatments