Health Ally September 2020



Change to CABS FCA account details

Following the Mid Term Monetary Policy Statement issued by the Governor on 21 August 2020 followed by Exchange Control Directive RV176 dated 24 August 2020, our bankers have sought clarity from RBZ regarding subscription payments made into our Nostro accounts.

As Alliance Health, our funds are transitory in nature (i.e. we use them to settle Claims payments) hence our bankers have confirmed the need to change our current **bank account type** and operate new **Transitory domestic FCAs** which are exempt of the 20% conversion as required by RBZ.

What does the above mean for you as a member?

With immediate effect our **CABS FCA account numbers have changed** and you must use the following bank account details when making subscription payments.

1129560821NORTHERN MEDICAL AID SOCIETY1129560880ALLIANCE MEDICAL

Nostro FCA Transitory Account Nostro FCA Transitory Account

What about Stanbic clients?

The Stanbic FCA account numbers are **NOT changing**. Stanbic will continue using the same accounts and convert them to **NOSTRO FCA Transitory Accounts** (they use a different platform to CABS and they have the facility to retain the same account numbers). You may continue to utilise the current account details for payments.

Claim processing made faster

We are constantly looking for ways to improve our service and make sure that you have the right level of support at all times. To this end, we are excited to let you know that we will soon launch a biometric enabled claim switching system that allows your claims to be sent electronically to us from the service provider, *in real time*.

Reasons to smile:

- Instant processing of your claim requests
- Quicker turnaround times on claims payments
- Reduced paperwork between you, service providers and Alliance Health.

The claims switching system will be available for NMAS and Northern Alliance members initially, with all other packages to follow in due course.



Staying safe in a growing digital world

Technological advancement brings with it many new ways of doing business remotely and digitally. However, it also poses a threat on the security of our interactions online. Many people have been subject to a number of cyber-security threats without knowing it.

Phishing email alert!

In the past couple of weeks, there has been an upsurge in the occurrence of phishing and spoofed emails. Email domains continue to fall victim to "spoofing" due to the volatility of the scammers. It is everyone's part as a computer user to be wise and not to fall prey to such emails. Here are a few tips on email security:



1. Don't trust the display name of who the sender is

Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look

at the email address to confirm the true sender.

2. Look but don't click

Hover your mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.



3. Check for spelling errors



Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.

4. Be careful of attachments

Attackers like to trick you with a really juicy attachment. Do not open suspicious attachments.

NB: Our Harare and Bulawayo offices are now open from 8.15am till 4.30pm for your convenience.

24Hour Call Centre Voice calls Claims submission: callcentre@healthzim.com General enquiries:

WhatsApp clientservices@healthzim.com

08677000716 / 0712 347 879 0772 126 120 / 0778 244 129