



A guide of MediCapt FAQs

© PHR Updated April, 2021

Table of contents

Data Management **3**

Data Security **6**

General MediCapt Use **9**

MediCapt Printing **13**

Addendum **14**

Managing MediCapt Login Access Information **16**

MediCapt Integration **18**

1.0 Data Management

1.1 Where is MediCapt data stored?

Currently MediCapt data is stored on– Amazon Web Services (AWS) by Amazon one of the leading Cloud Service provider in the world.

1.2 What is a server and where is it located?

Server - a computer or computer program which manages access to a centralized resource or service in a network. Examples Mail server (Gmail, Yahoo etc), Application Server (a computer hosting Electronic Medical Records that captures patient information in a Facility)

The MediCapt Server is located at premises managed by the cloud provider.

1.3 What is the cloud and where is it located?

Cloud - in **computing** is a general term for the delivery of hosted services over the internet.

Benefits of cloud computing:

- Tried and tested infrastructure and technology
- Shared expertise
- Reduced costs based on economies of scale
- High availability
- Scalability (automated)
- More Secure
- Location transparency
- Opportunity for Integration with multiple devices and platforms

1.4 What happens when patient information is accidentally deleted from the app? Is there back up? Can we recapture it?

You can only delete incomplete records. There is always a confirmation required before this action can be taken. If one confirms then the record is permanently removed.

There is no option to delete or edit an already submitted record.

Cloud database is backed up regularly and forms part of the services agreement. Rarely do we get outages from the AWS or the major cloud services providers because of the clientele hosted.

1.5 What happens when data is lost from the tablet?

Data can only be lost if the information on the tablet was not synchronized with the online database and there was damage to the tablet.

If data was synchronized then a backup in the cloud exists and can be retrieved on a new tablet.

1.6 What happens when data is lost from the cloud (after Syncing)?

AWS cloud hosting is one of the top 3 in the world in offering these services. Apart from having an elaborate backup strategy they have multiple sites across different continents that ensures that they meet the industry standard of availability.

For data to disappear from the cloud it means one of the following:

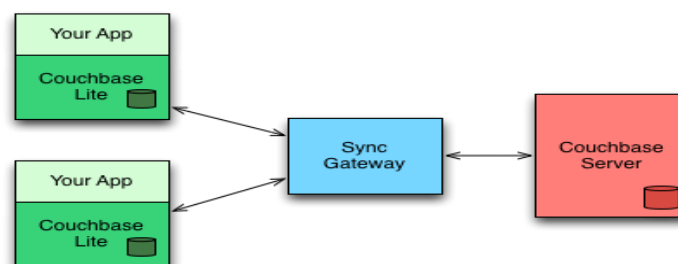
- They did not have backups and could not recover after a failure
- All their alternate server locations experienced failure at the same time

A chance of this happening is very low¹ according to their online Durability and Availability statement.

1.7 How do we retrieve data once it is lost?

If due to unavoidable circumstances the cloud database fails then data shall be restored from the last known successful automated backup. This is done at intervals of xHours.

Once the data is successfully restored, synchronization (bi-rectional) with tablets will update the cloud database with the changes that might be missing from the restored database.



¹ <https://docs.aws.amazon.com/whitepapers/latest/aws-storage-services-overview/durability-and-availability-3.html>

Amazon EBS volumes are designed to be highly available and reliable. EBS volume data is replicated across multiple servers in a single Availability Zone to prevent the loss of data from the failure of any single component. Taking snapshots of your EBS volumes increases the durability of the data stored on your EBS volumes. EBS snapshots are incremental, point-in-time backups, containing only the data blocks changed since the last snapshot. EBS volumes are designed for an **annual failure rate (AFR)** of between **0.1 and 0.2 percent**, where failure refers to a complete or partial loss of the volume, depending on the size and performance of the volume.

1.8 Can you access entered data if you’ve uninstalled the app before syncing?

Yes/No

Yes – previous submitted and Synced will be available after re-installing the MediCapt app again.

No – If there was any data that was not synced before uninstalling. This will be lost data and must be re-entered.

1.9 How do you retrieve data from the app? And for what purposes?

To retrieve data from the app’s Main Menu and select:



Edit Incomplete Records – To continue editing the records that have not been submitted.

Submitted Records – To retrieve submitted records and either Print or Add an Addendum

Backend – Reporting, Monitoring, Justice, Government/External Lab, Police, Health Ministry

1.10 Does the print-out come in triplicate or only one copy?

The clinician has control over the number of pages and what pages to print. Depending on current protocols clinicians need to print the numbers of copies required. In Kenya Three copies, one (1) to the survivor, One (1) to the Police and One (1) copy for filing at the facility registry with all access protocols observed.

2.0 Data Security

2.1 How is MediCapt protected against hacking?

There are several layers of protection of MediCapt data i.e. local, transmission and hosting.

Local:

The data on the tablet is encrypted SQLCipher² and cannot be accessed by other application except through MediCapt.

To access MediCapt one needs to be authorization. You must supply a valid username and password.

Transmission.

On the cloud server there are settings that ensure that MediCapt users can only access the application at their local facility. This is done by using the unique facility IP Address for accessing the internet. This means that a user cannot access MediCapt from another location even if they have a valid username and password.

The selection of MediCapt printer is based on guarantees of secure transmission from tablet to printer using Direct Wi-Fi³. This means one cannot intercept communication from MediCapt to printer when printing the PRC Form

Communication from MediCapt app to the cloud database is through a secure connection.

Hosting

Regular security audits are conducted by external auditors to ensure that there are no vulnerabilities at the hosting of MediCapt data in the cloud. This is coupled with AWS imposing strict standards to ensure physical infrastructure is kept secure.

² **SQLCipher** is a security extension to the SQLite database platform that facilitates the creation of encrypted databases. It uses the internal SQLite Codec API to insert a callback into the pager system that can operate on database pages immediately before they are written to and read from storage.
<https://www.zetetic.net/sqlcipher/design/#:~:text=SQLCipher%20is%20a%20security%20extension,to%20and%20read%20from%20storage.>

³ **Wi-Fi Direct** enables you to setup your **printer** to communicate directly with your computer or another device i.e. Smartphone or tablet, without requiring a **wireless** router or access point.
<https://www.epson.eu/viewcon/corporatesite/kb/index/1891#:~:text=Wi%2DFi%20Direct%20enables%20you,wireless%20router%20or%20access%20point.>

2.2 Who has control of the server?

AWS on its part of hosting the cloud database ensures security and availability of the physical infrastructure.

Once MediCapt solution is handed over to a facility they will be responsible for the administrative functions on the backend as well as configuring users and IP Address access setup.

2.3 Can somebody else log in to my MediCapt account? Can someone insert details from another facility pretending to be from my facility?

For someone to access MediCapt you must have shared their username and password either intentionally or otherwise.

A clinician is assigned to one facility. This means that MediCapt user cannot enter information for a facility they have not been assigned.

Additionally one cannot use MediCapt outside the facility location i.e. from another location if they do not share the same internet connection.

Facilities are supposed to implement MediCapt user protocols that ensure a user cannot access the system when they no longer work at the facility.

2.4 What happens if the original clinician is away? Can a colleague access my information?

In MediCapt the clinician that starts with the survivor must complete the process and submit the form. One can only access information on survivors they have seen.

2.4 How secure are images on the app?

Images captured in MediCapt are encrypted on a local database and not stored as images in phone folder. This means that even if one loses the tablet the images can only be accessed through MediCapt and not using any other application on the tablet.

2.5 Can we use the app using our personal email?

Not recommended but if alternatives are a problem then yes one can use their personal email.

2.6 What relationship does email have to MediCapt?

For standard communications on MediCapt and help users if they forget their passwords. MediCapt uses a valid email to ensure only the valid user receives communications to authenticate the password change.

2.7 If you sign in as a particular user, does it auto-populate your information and signature? If yes, can that pose a security problem?

Current version only auto-populates the facility a user is assigned not their signatures.

2.8 What happens if the technology fails? And the lack of network connectivity in some areas?

If technology fails then users can revert to the manual data intake forms. That said this will be an exception rather than a norm.

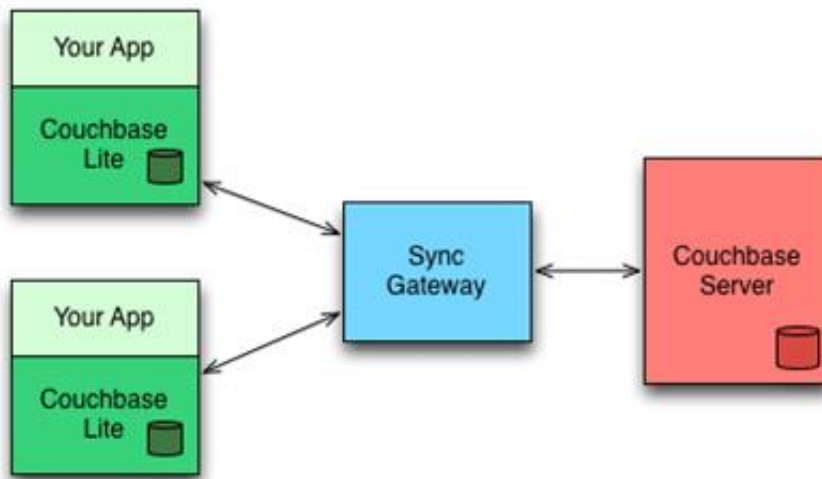
MediCapt Synchronization requires minimal time to synchronize if done frequently. Thus even for a link that is intermittent in availability it is possible to synchronize data.

One can also use shared mobile phone internet access to facilitate the synching, however this shall require coordination with the MediCapt admin to allow the new IP location do synch data.

3.0 General MediCapt Use

3.1 Synchronization

Database synchronization is the process of *establishing data consistency* between two or more databases, automatically copying changes back and forth. Harmonization of the data over time should be performed continuously. Pulling out from source (master) **database** to destination (slave) is the most trivial case.



3.2 How will I know if synchronization has taken place?

Synchronization takes place in two phases when using MediCapt. *The tablet must have Wi-Fi enabled for synchronization to happen.*

3.2.1 The first place the synchronization takes place is when the user starts MediCapt application just before and when the Login screen is displayed.



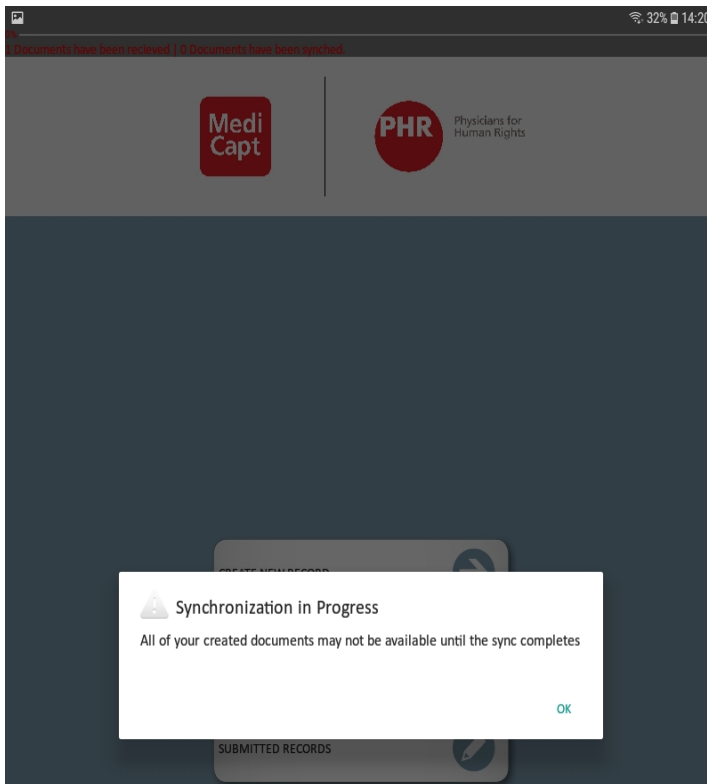
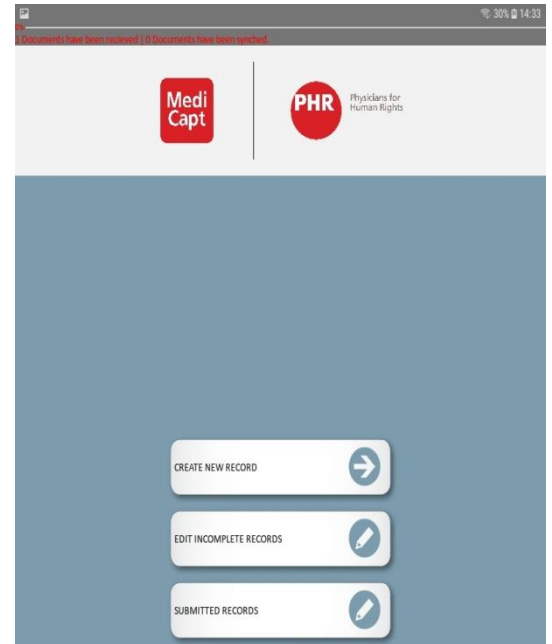
There will be a “brief” display of synchronization activity the top of the screen indicated in red, yellow or green colours. This initial synchronization takes a very short time and it is possible for a MediCapt user to miss it altogether.



3.3.2 The second synchronization activity occurs just after the user has logged into MediCapt.

When synchronization happens at this point proceeding with another activity might not work until synchronization is complete.

Once the synchronization activity stops then the device will be in sync with the cloud database.



3.3 Can I use MediCapt without Wi-Fi?

Yes. It is possible to work with medical without Wi-Fi but at some point synchronization has to take place to ensure the tablet is in sync with the cloud MediCapt database. In which case Wi-Fi must be active?

3.4 Can I work on MediCapt with Wi-Fi activated?

If Wi-Fi is not a challenge one can always use MediCapt with Wi-Fi turned on through a survivor interview. With Wi-Fi turned on synchronization happens in the background and all **data**, even if **not yet submitted**, will be updated in the cloud MediCapt database.

3.5 When is the best time to synchronize the MediCapt tablet with the cloud database?

This is dependent on the availability of the Internet at the facility. Where possible synchronization can be done on a daily basis at the end of the day. Each facility needs to be aware of the performance of their internet and synchronize when the internet traffic is not congested.

3.6 Must I use MediCapt on the same device throughout? Can I be able to use another device?

It is possible to use another device to capture PRC 363 data in MediCapt. However when one uses a new device all the data belonging to the user must be downloaded from the cloud database to enable synchronization to work correctly.

The time taken to for this new device to synchronize will be more compared to the device the user has been using. This might affect work especially if the internet traffic is high.

Unless the device is out of order and cannot be used, users should use the devices assigned to collect survivor PRC 363 information.

If the device is not working correctly please channel the issues through your local *HRIO/ICT* support team in accordance to the laid down protocols.

3.7 What shall I do if the device I am using fails in the middle of seeing a survivor?

If one was connected to the Wi-Fi when using MediCapt on the faulty device then the information that was captured before the tablet stopped working will be available and can be accessed on the new device. However if Wi-Fi was not activated then the user must re-enter all the information on the new device.

If one is not sure if Wi-Fi was activated before the device failure, on the new device retrieve incomplete records once logged into MediCapt.



To avoid this problem from occurring please ensure your device has adequate charge before starting a new case.

Ensure the device is kept according to the guidelines given on taking care of the Android tablet.

Contact *HRIO/ICT* office staff as soon as you realize device has a problem.

3.8 What can happen if there's no Wi-Fi at the facility?

As stated in the previously Wi-Fi is required to be able to synchronize with MediCapt cloud database. But in the event Wi-Fi is not available MediCapt can still be used and synchronization done when Wi-Fi becomes available.

Note: - If anything happens to the tablet that renders it unusable all data that had not been synchronized shall be lost.

4.0 MediCapt Printing

4.1 Do I need Wi-Fi for printing?

MediCapt printing uses Wi-Fi Direct technology but does not require the internet to work. Even when the internet Wi-Fi is down MediCapt printing will still be able to work.

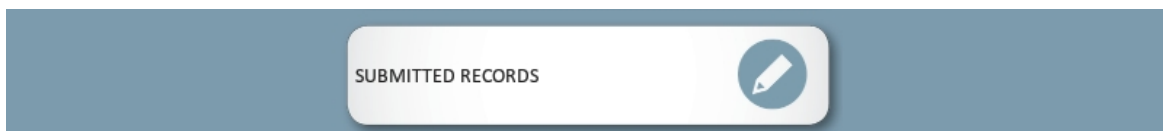
4.2 What do I do if survivor needs the PRC form but the printer is taking too long?

PRC forms must be printed in triplicate, signed and stamped for them to be valid. One copy is issued to the survivor; another copy is for law enforcement and a third copy is for filing at YFC. It is important to discuss with it survivor and indulge their patience even as printing takes place. Printing all three copies at the same time is the ideal situation and this should be encouraged at all times.

It is possible to print one copy and issue to survivor and print the other two copies later. However this might lead to inconsistency especially if clinicians forget to print the other copies.

4.3 Can I reprint a submitted PRC Form if one is misplace or the survivor requires another copy?

Yes it's possible to re-print a submitted PRC Form within MediCapt. Follow the usual procedure of retrieving submitted records print the copy.



4.4 Can I give my tablet to ICT team for them to print the PRC form on my behalf?

Patient information confidentiality must be maintained at all times and considering the sensitivity of the SGBV cases clinicians should be there when the PRC forms are being printed.

5.0 Addendum

5.1 I realized that I have been a mistake in one of the heated phones what can I do to rectify?

Yes it is possible to make correction to already submitted forms. This can be done through adding an addendum. MediCapt provides for four (4) areas to capture data under its addendum:

- **General comments** - can be used to enter additional comments related to a submitted PRC for or write comments to correct an entry in the submitted PRC Form e.g. correct Date of Birth, gender of perpetrator etc.
- **Chain of custody** - to capture information if survivor was unaccompanied by police during examination but police came later.
- **Laboratory Samples for National Government Lab** - Capture information relating to samples sent to National Laboratory services for analysis
- **Counselling Form** – used for capturing subsequent visits by survivor for counselling

5.1.1 Select to retrieve submitted records from the menu.

5.1.2 Move to the last step (28/28) using the short cut menu.

5.1.3 Click on Review.

5.1.4 At the bottom of the display select “ADD ADDENDUM”



Before submitting the PRC form, clinicians have an opportunity to review what has been captured, especially when survivor is out for lab tests. The focus should also be placed on information that can otherwise affect adversely the outcome of a court case if it introduces a contradiction to other data or when wrong information captured.

Submitted addendum is attached to the original PRC that was submitted.

5.2 How do I print the addendum?

5.2.1 Select to retrieve the submitted record.

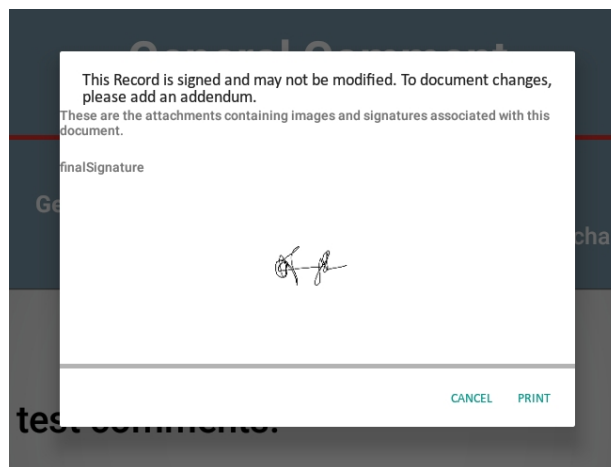
5.2.2 Move to the last step (28/28) using the short cut menu.

5.2.3 Click on “Review” button

5.2.4 Click on the desired Addendum

5.2.5 Move to the last page of Addenda and click “Review” button

5.2.6 Click Print.



6.0 Managing MediCapt Login Access Information

6.1 I forgot my password for MediCapt Login, what do I do?

MediCapt has a new feature where users can get assistance if they forget their password. This feature requires Wi-Fi activated and internet access to complete the process.

The following is the procedure:

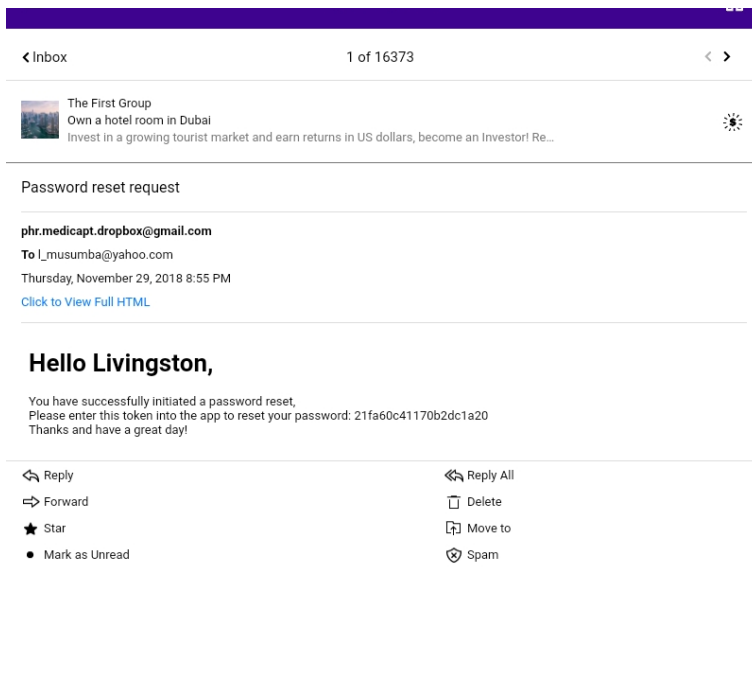
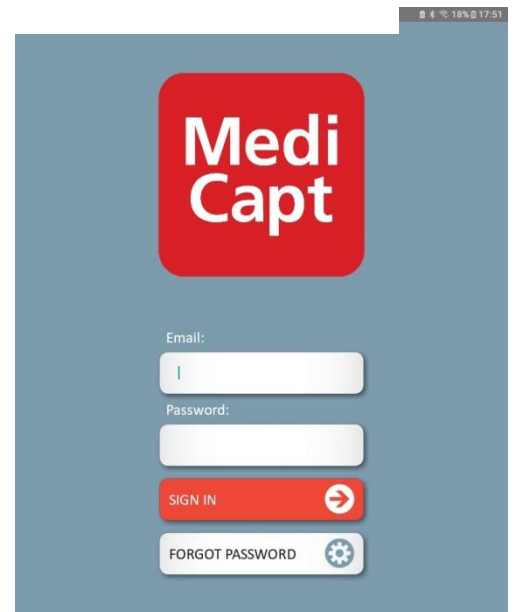
6.1.1 Activate Wi-Fi on the table and ensure internet is working



6.1.2 Start MediCapt and wait for the login screen to appear

6.1.3 Enter your user name (your email account to receive the message from MediCapt)

6.1.4 Log onto your email used for get the token required to change the password.



6.2 How do I change my password?

This process does not require the internet to change ones password.

To do these follow the steps below:

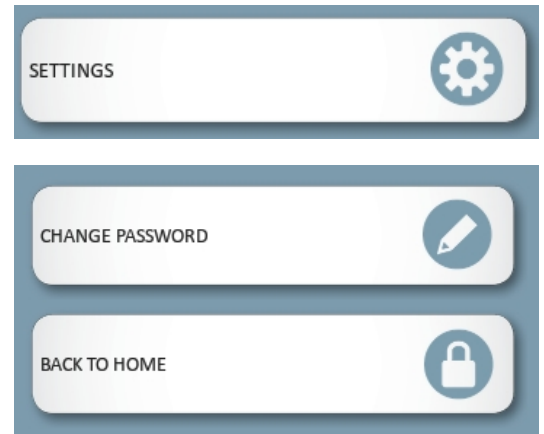
6.2.1 Start MediCapt and log in with your username & password

6.2.2 Next Select **Settings** from the main menu

6.2.3 Select **Change Password** in the sub menu displayed.

6.2.4 Enter the new password as requested.



The change in password becomes effective immediately on the **device**.



Current Password:

New Password:

Confirm New Password:

CANCEL  SUBMIT 

7.0 MediCapt Integration

7.1 How is the system linked to DHIS?

Currently MediCapt is not linked to DHIS but is going to be done in future releases. The next backend reporting release will include the Monthly summary report which will then be used to integrate with DHIS.

7.2 MediCapt integration with EMRs

Integration with EMRs – although there is a standard for interoperability there are multiple vendors at various facilities that will require to be integrated. There is no single version of MediCapt that can integrate with all existing EMRs.

For MediCapt to be integrated with an EMR, the EMR must meet the security standards to ensure that there is no compromise of data in the integration.

7.3 Can MediCapt be used to monitor and track repeat violations within and across facilities?

Current each facility has its own dedicate cloud space to capture their data. There is no integration of data from different facilities.

7.3 What happens with forms that are yet to be transmitted to the police in instances where the survivors are not ready to instigate a criminal case?