NHS
Northumberland, Tyne and Wear
NHS Foundation Trust

Security Management Policy - Practice Guidance Note Reliance Protect Identicom Lone Worker Protection System		
Date issued **Issue 7- Jun 17** **Issue 8 – Sep 17**	Planned review **Dec 2017**	**SM-PGN-09** (Part of NTW(O)21 Security Management)
Author/Designation	**Tony Gray – Head of Safety and Security**	
Responsible Officer / Designation	**Tony Gray – Head of Safety and Security**	

Contents

1 INTRODUCTION

1.1 The 'Identicom Device' you are using is a lone worker device disguised as a standard identity card holder, worn on a lanyard or lapel clip. Identicom™ is the device that provides a discreet means of alerting the 24/7 manned Reliance Alarm Receiving Centre (ARC) to a situation. Whether the worker is facing physical or verbal abuse, ARC staff listen in to and record everything that takes place during the incident, the ARC staff initiate the most appropriate response based on incident severity.

1.2 Meeting police guidelines, the simple operation of the Identicom device delivers all of the functions necessary for a rapid, safe, appropriate response:

- Signal strength and battery can be quickly checked as part of your dynamic risk assessment
- Amber alert to record your location and appointment details puts you in total control
- Single, easy to find, red alert button to call 24 hour monitoring centre
- Lanyard rip alarm can automatically trigger red alert
- Audio link and amber alert recording ensure appropriate and rapid response

1.3 The device uses mobile phone technology so is dependant upon good network signals. They are supplied with Vodafone Sim cards. The device, like any other mobile phone device, requires charging to ensure optimum working.

1.4 The ARC is manned with trained operatives who listen into the red alert calls via the microphone on the device, play back the amber location message to confirm your whereabouts and send a police response if necessary.

1.5 They will inform colleagues or supervisors of the situation, or simply archive recordings for use in future legal action or to support changes in working practices if a police response is not needed.

1.6 Information recorded from any red alert can be used in evidence in court to prosecute an individual charged with committing any offence against National Health Service (NHS) staff.

1.7 The device will be supplied with a box which has the entire relevant associated serial and mobile phone numbers which staff should keep safely together. The contents include:

- A user guide
- A device battery charger
- Three replacement plugs for the rip chord facility
- A lapel or waistband clip

2 LONE WORKING PROCEDURES (SM-PGN- 02 - Lone Worker)

2.1 It is important to use the Indenticom lone worker devices in conjunction with existing lone worker protection systems (such as buddy or diary systems), patient clinical risk assessment, and information gathering processes, including the briefing and updating of any change in a patient's circumstances.

2.2 The importance of these systems is to ensure managers have up to date information of where their staff are at any given time in case an accidental activation of a device or a full emergency situation where the user has not left an amber location message.

2.3 No unplanned visits should be made without informing the buddy, the department diary system or leaving information with the escalation contact.

3 ESCALATION CONTACT LISTS

3.1 Managers must ensure that a series of robust telephone escalation contact numbers are provided for each Identicom user. The Identified telephone contact person should be made aware of what information they are expected to provide the ARC operators with during an emergency activation. The operators will contact each number they have been given in a sequence until they establish the whereabouts of the individual, a 24 hour manned reception who has access to diaries or work schedules is ideal for this.

3.2 **St Nicholas Hospital switch board can act as an emergency contact point (On Call Manager's see Appendix 4)**

3.3 Team managers must ensure that if our switch board operators are to be used within an escalation process that they are aware of what they are expected to do. They must know what information they are expected to pass on to ARC in the event of an emergency.

3.4 It is advisable that each team manager ensures that they include this requirement within the contents of this protocol and should include the following information:

3.4.1 The switchboard will need to be contacted prior to the visit. They will need your full name, and your team or department name, the full postal address and postcode of the home you are visiting, and if necessary, a description of the property you are visiting, for instance it may have a name rather than a number.

4 AMBER LOCATION MESSAGE

4.1 An amber location message should be left before entering any premises either in your vehicle or on the pavement, if it is safe to do so.

- **Example:**

"This is (lone worker's name), I am visiting No 1 Main Street, Gosforth, Newcastle upon Tyne, NE3 3XT, I am expecting this visit to last one hour." You may also vocalise any concerns you have around this visit e.g. previous challenging behaviour or violence and aggression.

You may want to leave the message using the phonetic alphabet for the address and postcode, please see **Appendix 2.**

5 WHEN THE DEVICES SHOULD BE USED

5.1 The devices should be used before every visit, the signal status check battery and network facility should be used to ensure coverage. Prior to the visit, an amber location message should be left.

5.2 If for any reason the device cannot support the visit due to low battery strength or poor network coverage staff should assess the risk involved with the visit and return to base if any element of risk exists.

5.3 Any risk to your personal safety

5.3.1 In certain circumstances, the Identicom device receives a police response to a red alert activation from the ARC. It is therefore important that staff use the system responsibly. They should activate the red alert button if they have been the subject of a physical assault, have been taken hostage or feel threatened to such a degree that efforts to de-escalate the situation have failed and they are in imminent danger. Or if the information recorded involves a threat to personal safety either then or in the future.

5.4 Alarm receiving centre (ARC)

5.4.1 The operators in the ARC are trained to listen to the context of the dialogue of the visit and escalate the emergency to a police response if staff request this or if staff are in any immediate danger.

6. RESPONSIBILITIES OF TEAM MANAGERS

6.1 Team managers will be expected to monitor their teams' usage of the Lone worker devices and manage those staff who are clearly not using their device. They will be expected to manage the redeployment of the devices when staff leave the organisation change job roles or no longer require a device.

- To ensure staff adhere to this protocol and associated guidance
- To ensure staff use the Identicom devices and monitor their use
- To ensure the Identicom devices are maintained for effective use
- To ensure Reliance are informed of changes in staff personal profile or emergency contact detail if staff move department or leave the organisation
- To ensure staff report any incidents of violence and aggression in line with Trust's policy and practice guidance notes, NTW(O)05 – Incident Reporting
- To ensure staff report any loss, damage or malfunction of the Identicom device allowing managers to arrange for a repair or replacement with the Reliance services desk
- To enforce Trust policy; NTW(HR)04 – Disciplinary, in cases of misconduct or misuse

- To manage the usage and redeployment of any devices, please see the Redeployment pro-forma. (Appendix 3)

7 RESPONSIBILITIES OF STAFF

- To use the Identicom device in line with this protocol and training provided
- To ensure the device is fully charged
- To cancel accidental red alert activations as per procedure
- Not to misuse, damage or effect the performance of the device
- To follow the department lone worker guidance/policy
- To report any incidents of violence and aggression promptly in line with the Trust's policy, NTW(O)05 – Incident Reporting and practice guidance notes
- To report any malfunction damage or loss of the devices
- Not to loan or transfer their device to another or borrow another's device
- Repeated incidents of damage or loss may result in disciplinary action
- To hand in their device if they leave the organisation and no longer need it (**see Appendix 3**)
- To ensure their Escalation Contact and User Profile Information is maintained with current information and changes communicated to Reliance via the Lone Worker Device Co-ordinator

8 STAFF REDEPLOYMENTS AND SECONDMENTS

8.1 When a member of staff who is in possession of a Lone Worker Device moves team within the Trust's employ they are entitled to retain their Device under the following circumstances:

- The user is a Community Psychiatric Nurse

or

- An Individual Staff Risk Assessment has been completed by the new manager to prove the continued need for a Lone Worker Device and submitted to the Lone Worker Device Co-ordinator together with updated Escalation Contact and User Profile forms to reflect the new role and team

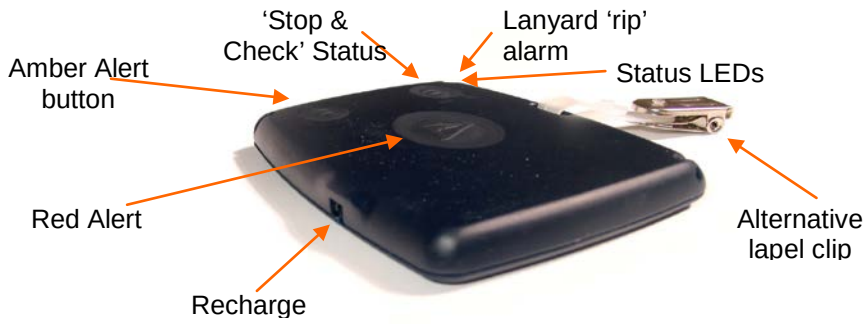
9 FUNCTIONALITY OF THE IDENTICOM DEVICE

9.1 The Identicom device uses mobile phone technology and is fitted with a SIM card which has a mobile telephone number and has the ability to send text messages and emergency alerts. The device requires charging by means of mobile phone style charger which is provided with the device, the battery will give up to eighty

hours of use once fully charged. **After charging the device is live it will need to be switched off when not in use to maintain full battery strength.**

9.2 The device has a 'stop and check' facility which gives battery strength and network coverage supported by Vodafone.

9.3 The device can be worn on the lanyard or on a clip attached to a blouse shirt or waist band, the device has rip cord facility which, when pulled, automatically sends a red alert activation to the ARC.



9.4 The device is supplied with 3 Lanyard Rip plugs. If the original plug becomes damaged, a new plug should be fitted; this is a simple process and will be covered in the training session.

10 CHARGING THE DEVICE

10.1 The Identicom device should be fully charged before use, it will take approximately six hours to fully charge the device. Plug in the three pin plug to the mains power supply and then connect the charging cable to the recharge connection point in the base of the device and switch on.

10.2 When charging, the device will give a flashing visual display on its reverse side of red, amber and then a constant green light when fully charged. If the red light remains on the device will require servicing.

10.3 The annual cost to recharge the Indenticom is 6 pence per annum; this will obviously be dependent upon current energy costs.

10.4 In car chargers can be purchased directly from Reliance at £12.00 per unit, please contact Reliance Service desk on 0800 840 7121 who will assist with the purchase. Your team manager will need their department budget code to do this.

11 SWITCHING THE DEVICE ON OR OFF

- To check the Identicom is on, press the status button for two seconds, if the LED's do not flash the device is off

- To switch on the Identicom device, press the status and amber buttons together until the LED's start flashing, the device vibrates briefly to confirm it is on

- To switch the device off, press the status and amber buttons together until the device vibrates twice

12 BATTERY AND SIGNAL STATUS

12.1 To check the Identicom device battery level and phone signal strength before a visit and to ensure you are effectively covered, press and hold the status button until the LED's start to flash red. After a short while, the battery and signal strength will stop flashing and indicate using the traffic light system:

- **Green - Good**
- **Amber - Low**
- **Red - Poor battery or signal strength**

12.2 If either LED is red, you should not rely upon the Identicom device in an emergency situation. If the battery LED is amber the unit should be charged.

12.3 **Network Problems**

12.3.1 Where staff experience problems with Network coverage, they can be described on **Appendix 1** to inform others in the team of the problems in that area. The Reliance Service Desk on 0800 840 7121 need to be informed of these black spots or network problems so that Vodafone can then instigate work to improve their network coverage.

13 AMBER ALERTS

13.1 An amber alert is a voice message that records your current location with the Alarm Receiving Centre (ARC). Typically you would record your voice message in the car or in the street before you enter the premises.

13.2 Press the amber alert button for at least one and a half seconds. The device will give three short bursts of vibration, the battery and signal LED's show constant amber whilst the device is connecting; they then flash amber to indicate that you can now leave your message. The dialogue box will remain open for twenty four seconds.

14 RED ALERTS

14.1 The red alert button should be pressed for one and a half seconds. The device will give three short burst of vibration to confirm the alert it has been activated. The Identicom device will then open a voice call and enable the microphone, so that the ARC can listen into the call and record the dialogue. If staff need a police response they should clearly request this by using words like: "I need a police response straight away".

14.2 **Clearing red alerts**

- Press the red alert button for two seconds. The device will give two short bursts of vibration, you must then state that you are safe thus standing down the red alert.
- A back up call to the Reliance Service Desk (0800 840 7121) cancelling the red alert would be also be advisable.

15 REPORTING FAULTS OR DEVICE FAILURES (Reliance Service Desk)

15.1 Reliance offer a fully managed end to end service for reporting and issues please contact the Service Desk by telephone on 0800 840 7121 Fax 01977 801356 or by e-mail Servicedesk@relitech.co.uk. You can click on 'contact us' on their website at **www.relianceprotect.com**

15.2 The Reliance Service Desk will resolve problems with faulty SIM cards or devices. Normally they will be replaced on a next day delivery service which is dependant upon what time they receive your call.

15.3 Staff must complete a Web-based Incident Reporting Form including a full description of how the device has failed and in what circumstances the failure has occurred.