NHS Greater Glasgow and Clyde Core brief

Thursday 9 August 2018

Introduction

This issue of Core Brief details information on emergency department waiting times, security issue and Counter Fraud Services.

Emergency department waiting times continued improvement

The latest published waiting times figures show NHSGGC recording our third consecutive month of improving performance across the Board's Emergency Departments.

While we continue to strive towards further improving our performance against the national waiting time target, the recorded improvements reflect the hard work and efforts of our clinical teams and local managers.

Communications awareness raising messages reminding people of the importance of using their emergency services appropriately continue to run. Our messages outline that minor ailments or sickness can often be more appropriately treated at our Minor Injury Units, by GPs, pharmacists or by contacting NHS24 on 111.

Security issues

NHSGGC needs to plan for, and respond to, a wide range of incidents and emergencies that could affect health, patient care or the operation of the board.

Major incidents can range from extreme weather conditions to an infectious disease outbreak or a major transport emergency, where psychosocial support could be required. The Civil Contingencies Act (2004) 7 Scottish Regulation 2005 requires NHS organisations to show they can deal with such incidents while maintaining critical services.

We work closely with other partners in the health community and multi agency partners, in planning for and responding to all types of emergencies and major incidents.

To make it easier for staff to find the most up-to-date major incident plan for your site, a 'civil contingencies icon' has appeared on every PC desktop taking you directly to the civil contingencies StaffNet page.

Staff Extortion Scam

Counter Fraud Services received notification that at least four NHS staff members have received an email from a fraudster attempting to extort money through a ‘sextortion scam’. These emails are being sent to both work and personal email addresses.

The scam email confirms either part of the staff member’s password or an old password, and states that unless payment is made the fraudster will send video clips to the staff member’s relatives and co-workers.

If your email account has been compromised in a data breach, you should change your password immediately.

Should any staff member receive an extortion attempt, please report this to the police via the Action Fraud website: http://www.actionfraud.police.uk/report_fraud. If you have received one of these emails and paid the fine, report it to your local police office.

Are your contact details up-to-date? Click here to check

Produced by NHS Greater Glasgow and Clyde Communications