BREAK GLASS INCIDENT PROCEDURE
(Accessing Sensitive Results Protected by Security)

Reference No:	UHB 115	**Version No:**	1	**Previous Trust / LHB Ref No:**	N/A

Documents to read alongside this Procedure	IT Security Policy, DPA Policy, Health Records Policy, Records Management Policy, Freedom of Information Act Policy

Classification of document:	Corporate
Area for Circulation:	Clinicians UHB Wide
Author/Reviewee:	Corporate Governance, Senior Information and Communication Manager
Executive Lead:	Medical Director
Group Consulted Via/ Committee:	Information Governance Committee
Approved by:	Quality & Safety Committee
Date of Approval:	20th September 2016
Date of Review:	20th September 2019
Date Published:	15th March 2018

Version Number	Date of Review Approved	Date Published	Summary of Amendments
1	14/06/12	27/06/12	New Procedure

Contents Page

BREAK GLASS INCIDENT PROCEDURE

(Accessing Sensitive Results Protected by Security)

1 INTRODUCTION

The term “Break Glass” in this procedure refers to the practice of enabling access from within the Clinical Portal Patient Record application, to sensitive results (such as HIV) or opening the record of a patient who has withdrawn their consent which restricts access to their record. When this occurs, there is a need to breach the security that exists to ensure patient information is protected, safeguarded and held securely. To “break-glass” therefore is a quick means of temporarily allowing individual’s access in exceptional circumstances such as in an emergency situation, or to inform the patient of their sensitive test results.

Consideration should also be given in the overall risk management process specifically considering any security risk created by this capability and care quality risks associated with denial of access to patient information.

The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. In the case of the NHS, the most sensitive of our data is patient record information.

In practice, this is applied through three cornerstones - **confidentiality, integrity and availability**

- Information must be secured against unauthorised access - confidentiality
- Information must be safeguarded against unauthorised modification - integrity
- Information must be accessible to authorised users at times when they require it - availability

There are four sets of circumstances that make disclosure of confidential information lawful

- where the individual to whom to information relates has given consent
- where disclosure is in the overriding public interest
- where there is a legal duty to do so, for example a court order
- where there is a statutory basis that permits disclosure such as approval under Section 60 of the Health and Social Care Act 2001

Therefore, under common law, a healthcare provider wishing to disclose a patient's personal information to anyone outside the team providing care should first seek the consent of that patient. If disclosure is made which is not permitted under common law the patient can bring a legal action not only against the organisation but also against the individual responsible for the breach.

Any unauthorised access of personal information is considered to be in breach of the Data Protection Act (DPA). Organisations have a duty to report DPA breaches to the Information Commissioners Office (ICO) and the Information Commissioner now has the necessary authority to penalise organisations for breaches, these can result in substantial financial penalties being incurred. There is an obligation placed on everyone to ensure adherence with the Data Protection Act in respect of confidentiality of personal data.

All persons who use patient records should be aware of their responsibility for facilitating and maintaining confidentiality of those records. Systems and processes should ensure that employees only have access to those parts of the record required to carry out their role.

There must be adequate systems in place to control and monitor access to patient information in order to comply with legislative requirements, and the appropriate regulations, to ensure that we effectively protect the confidentiality, integrity and availability of sensitive and confidential information.

Accessibility to information must be restricted to ensure that only individuals who have a need to, or right of, access are able to do so and also that the access is lawful and for the treatment of a patient. There will however be occasions when information will need to be accessed such as in an emergency situation or when legitimately treating the patient that will require access to the sensitive results contained behind the Break Glass. It is a legislative requirement to have such a procedure in place. The UHB Break Glass procedure will also detail the process to be followed for monitoring, reporting, auditing of break-glass incident and will cover:

- Valid reasons being provided for initiating the break-glass access
- Detailed documented audit trail records
- The requirement to complete any reviews that may be identified

The break-glass process is intended to specifically cover for emergency situations and to protect the privacy of the patient whereby test results are deemed sensitive. The glass should not be broken without due consideration and only by staff directly involved in the treatment of the patient.

Abuse of access

Any suspected deliberate access to sensitive results, or personal information, for purposes other than clinically treating a patient is likely to be considered a disciplinary offence and could result in disciplinary action including dismissal. In addition, such access may also be deemed a breach of patient confidentiality under the DPA and consideration to the UHB's DPA Policy will be made and this may result in a requirement to report the breach to the Information Commissioners Office. Any action taken will depend on individual circumstances.

2 AIM

This procedure will fully detail the process to be followed in the event of a break-glass incident occurring. It also sets out how Cardiff and Vale UHB will ensure that the necessary monitoring, recording, auditing and review process is completed.

3 OBJECTIVES

- To ensure there are adequate clear processes in place for dealing with break glass incident
- To ensure adequate reporting arrangements are in place
- To provide assurance to the Board that we are fully meeting legislative requirements.
- To ensure that patient information is managed and accessed in accordance with the appropriate legislation
- To ensure any potential risks can be identified and thereby reduced.

4 SCOPE

This procedure covers all break-glass incident and staff involved within the process from the initial access to the final audit and review.

The Break-glass functionality prompts the user with a caution notice which will display details of whichever restriction applies, (withdrawn consent or sensitive results), the notice informs that access is restricted other than to staff directly involved in treating the patient. The user can then click the appropriate prompt to obtain the access being sought.

Each break-glass occurrence should be

- attributable to an authenticated user
- time-limited
- audited

This will ensure appropriate accountability for the disclosure.

5 ROLES AND RESPONSIBILITIES

5.1 Medical Director as Caldicott Guardian

- The Caldicott Guardian will ensure that the break glass processes are implemented. He will also ensure that there are adequate systems and individuals in place for monitoring, reporting, auditing and reviewing all break-glass incident

- He will nominate the appropriate individual to issue the non compliance letters to all individuals who have not responded to the break-glass

incident report.

5.2 Clinician/Staff involved at the point of the break-glass incident

- All staff once they have been warned of the break-glass incident occurring have a responsibility to report the break-glass incident to the nominated responsible individual in their area such as the Divisional Manager/Directorate Manager/Clinical Director/Practice Manager.

- Consideration must be given to the Data Protection Act when accessing personal information

5.3 IT Security Manager

- The IT Security Manager will be responsible for producing and distributing reports to the Clinical Governance Representatives in each of the areas and ensuring that reports are returned and monitored

- The returned report will be recorded appropriately and will be used to inform a report for the Medical Director to discuss at the Information Governance Group.

5.4 Nominated area specific individual (DM)

- On receipt of the report from the IT Security Manager the nominated officer must ensure that contact is made either verbally or in writing to each individual clinician (identified within the report as having broken the glass) seeking full details and explanation of the break-glass incident they were involved in. The completed report must then be returned to the IT Security Manager.

5.5 Information Governance Manager/Data Protection Manager

- The Data Protection Manager will be responsible for producing quarterly reports for the Medical Director

- In the event of any breaches being identified this will need to be fully investigated and actioned with notification being made to the Information Commissioners Office if required.

6 RESOURCES

There should not be any additional resources required for the implementation of this procedure. There are processes currently in place and this procedure provides a formal structure to be followed by Cardiff and Vale UHB for break-glass incident.

7 TRAINING

There will not be any training required for this procedure to be implemented as this process is currently being followed within the organisation even though not set out formally.

8 IMPLEMENTATION

The procedure will be implemented from the Medical Directors office by issuing a standard letter to all clinicians. Once approved, this document will also be included within the mandatory induction session that all new clinical staff attend.

9 EQUALITY IMPACT ASSESSMENT

Cardiff and Vale UHB is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups. We have undertaken an Equality Impact Assessment as we wanted to know of any possible or actual impact that this procedure may have on any groups in respect of gender (including maternity and pregnancy as well as marriage or civil partnership issues), race, disability, sexual orientation, Welsh language, religion or belief, transgender, age or other protected characteristics.

The assessment found that there was no impact to the equality groups mentioned. Where appropriate we have made plans for the necessary actions required to minimise any stated impact to ensure that we meet our responsibilities under the equalities and human rights legislation.

10 AUDIT

Compliance will be audited on a quarterly basis via a standard report to the Information Governance Group. Routine random audits will also be completed as required.

11 REVIEW

This procedure will be reviewed every three years or should any legislative changes require earlier review.

12 DISTRIBUTION

This document will be distributed in accordance with the Cardiff and Vale University Health Board Policy for the Management of Policies, Procedures and all other written Control Documents.

13 REFERENCES / SOURCE DOCUMENTS

Confidentiality:Code of Practice for Health and Social Care in Wales
Caldicott: Priniciples into Practice (C-PIP) (IHC 2008)
Confidentiality and Disclosure of Information :GMC. PMS and Alternative provider medical services Directions 2004
The Protection and Use of Patient Information Guidance from DOH
Section 251 of the NHS Act 2006 formally section 60 of the Health and Social Care Act 2001
NHS Code of practice on patient confidentiality DOH 2003
Information Security Management NHS Code of Practice (DOH) 2007
Nurses NMC - Code of professional conduct
Healthcare Commission Code of practice to Confidential personal information as required by the Health and Social Care (Community Health and Standards) Act 2003
ICO Use and Disclosure of Health Data - Guidance on the Application of the DPA
Information Security Assurance - ISO 27001/2 Information Security Management (formerly BS7799)
WASPI
Records Management Policy
Data Protection Act
Common Law Duty of Confidentiality
Freedom of Information Act
Data Accreditation and Data Quality
NHS Information Governance Guidance on Legal and Professional Obligations (DoH) 2007
National Information Governance Board (NIGB) for health and social care
Caldicott Guardian Manual 2010
DoH Integrated Governance Handbook 2006

14 APPENDICES

(i) Flowchart
(ii) Standard letter to be issued for non compliance

Appendix(i)

Break-glass Incident Procedure Flowchart

- A clinician tries to access a patient record that has either withdrawn consent, thereby restricting access to the record, or has sensitive results.

- A warning message is displayed stating that access will be recorded and an option to continue is provided.

- A report will be produced (by IT Security Department) on a quarterly basis listing all the break glass incident that have occurred.

- The list will be segregated into individual areas and the individual lists will be sent to the nominated individual for each area for investigation/reasons for the break-glass breach. A list of the nominated individual's in each department will be retained and managed by a nominated representative within the Medical Director's office.

- Recipients must acknowledge receipt of reports to IT Security

- The nominated official will contact each of the individuals who have been identified as having broken the glass seeking confirmation directly from them of the reason for the incident and brief details. It is suggested a timescale of two weeks be allowed for the responses with explanations to be returned back to the nominated official.

- The nominated official will review the incident, investigate if required and take any necessary action all identified inappropriate incident must be escalated appropriately, and if necessary to Medical Director

- The nominated official will provide full confirmation details to the IT Security Department for consideration and reporting to the Medical Director as Caldicott Guardian.

- In the eventuality of staff not providing a response this fact will be recorded within the standard report and details will be provided to the Medical Director who will initiate a letter directly to the individual concerned. A copy of the letter to be issued is shown below.

Appendix (ii)

Dear xxxxxxxx

I have been notified of a break-glass incident on dd/mm/yyyy and I have been informed that you were the individual who broke the glass for the patient.

As you are aware all such incident must be reported and recorded to ensure that we fully comply with relevant legislation, such as the Data Protection Act, and unfortunately to date there has not been any communication from you confirming the circumstances surround this unauthorised access.

I would like to draw your attention to the Cardiff and Vale UHB Break Glass Incident Procedure which clearly details that all incident must be accounted for by the individual concerned therefore I would be grateful if you could respond to me at your earliest possible convenience providing full details of the incident.

I look forward to receiving your response within the next few days.

Yours sincerely