

1.21.6 Incident Management

Please provide details of how your organisation records, manages and monitors data breaches.

You may wish to refer to previous incidents you have referred to under earlier.

(Maximum Word Count 500 words plus relevant attachments)

Words used = 438

ATTACHMENTS: 1) Breach flowchart; 2) Information Governance related Serious Incidents Requiring Investigation (IG SIRI) Policy; 3) Serious Case Initial Findings – AGENDA; 4) Training Needs Analysis for Information Governance Training

1.21.6.1-Key roles

All staff are responsible for reporting any identified data breaches. The Regional Governance Team notify the Vocare Assurance team, make external referral to CCG/STEIS and CQC [as required], and manage any duty of candour communications.

The Head of Clinical Governance (or deputy) notify DPO, Caldicott Guardian, SIRO and Executive, and will assess incidents for external referral triggers. They will initiate training from learning and complete the annual incident report.

Vocare complies with all relevant IG requirements:

- GDPR
- DPA 2018
- ICO GDPR guidance
- IGA data-protection guidance
- ISO27001:13 accredited,
- Working towards NHSD DCB1596 Accreditation and Cyber Essentials

Accountable officers

- | | |
|--|---------------------------------|
| • Senior Information Risk Owner [SIRO] | Managing Director |
| • Information Risk Owner [IRO] | Head of Corporate Assurance |
| • Data Protection Officer [DPO] | Director of Corporate Assurance |
| • Caldicott Guardian | Medical Director |

1.21.6.2-Policy relating to data breaches

IG reportable incidents will be managed via:

- V-IG P27 Incident policy
- V- IG 757 IG SIRI [Information Governance related Serious Incidents Requiring Investigation] policy, supported by Data Security standards 6 [NHS Digital 20/21].

1.21.6.3-Training

Investigatory staff complete Root Cause Analysis training [external provider].

NHS Data-Security Awareness course is mandated at induction and annually for all staff. Service Managers and the Executive complete DPO-delivered training covering their responsibilities.

1.21.6.4-Recording of data breaches

Any breach detected is recorded on Datix by the identifying staff member. Basic information regarding event and initial actions are recorded [No PCD].

1.21.6.5-Managing data breaches

Notification is sent to the Assurance team. Incidents are graded according to the significance of the breach and the likelihood of serious consequences. Serious Case Incidents Finding (SCIF) meetings define the level for any red-flag incidents.

Breach notifications and investigation outcomes are sent to:

- Head of Corporate Assurance, DPO and Caldicot Guardian
- NHS Digital/ ICO [within 72 hours]
- CQC, CCG [if relevant]
- Those affected [Duty of candour notification]

An investigating officer is appointed and will engage appropriate specialist help [IG, IT, Security, Records Management]. Unless advised by NHS Digital/ICO, investigations are internal.

Findings may determine process changes, development of new guidance, reinforcement of training, individual training/development plan.

Claims management processes are considered and any staff involved are supported through HR processes.

Changes or learning points are fed back to the individual, at team meetings, collective briefings, bulletins, emails, and posters.

1.21.6.6-Monitoring data breaches

All incidents are collated into the Regional Quality Report and monitored by the regional team.

Individual leads are appointed to manage action plans and independent audits [within pragmatic timeframes] resulting from lessons identified during the root cause investigation.

Annual statutory reporting is completed:

- Head of Corporate Assurance - organisational report for data security toolkit submission.
- Head of Corporate Assurance - annual report for ISO 27001 audit purposes.

1.21.6.7-Track record regarding data breaches

Vocare has monitored data incidents since the inception of Datix in 2010. In the last two years only two incidents required reporting to the ICO; no further actions were recommended.