hscic Health & Social Care Information Centre

Information Governance Toolkit Incident Reporting Tool

Publication Statement

The Information Governance Toolkit is a product and service managed by the Health and Social Care Information Centre (HSCIC) Information Governance External Delivery Team.

Therefore, the main HSCIC Publication Scheme and information about your rights under the Freedom of Information Act 2000 applies and can be found at the corporate web links below:

http://www.hscic.gov.uk/foi

http://www.hscic.gov.uk/about-us

The purpose of this statement is to inform IG Toolkit Users and members of the public of our intent to publish data on **Serious Incidents Requiring Investigation (IG SIRI)** self-reported on the secure IG Toolkit Incident Reporting Tool. With regard to the transparency and open data agenda the statements below offer detail on who we are, what information we collect, who we share information with and what we will publish.

Who we are and what we do

We are the Health and Social Care Information Centre External Information Governance Delivery Team. Our products and services are delivered upon commissions from the Department of Health (DH) and NHS England (NHSE) with regards to IG assurance in the Health and Adult Social Care setting. We currently discharge IG standards, subject matter expert (SME) advice and best practice guidance in relation to DH Policy, government initiatives and relevant legal obligations which Health and Social Care Providers and Commissioners are subject to. The IG Toolkit platform is the mechanism used to disseminate our portfolio of work and monitor Health and Social Care IG compliance/performance. For further information on the IG Toolkit click here.

Who we share information with and why

We maintain commitments (by Memorandum of Understanding and through DH commissions) with other key stakeholders such as the Care Quality Commission (CQC), Monitor and the Information Commissioner's Office (ICO) to share intelligence in support of national agendas and improving sector standards/services. A series of reports are sent to these Bodies on published IG Toolkit assessment scores.

IG Toolkit registered organisations and users with Incident Reporting Tool permissions have access to this system to self-report IG and Cyber Security serious incidents requiring investigation (IG SIRIs and Cyber Security SIRIs) for Organisations which they are responsible and accountable for.

A limited number of HSCIC staff have routine access to all or Cyber Security only data held on the Incident Reporting Tool in order to support our SME service.

A small team within the ICO have routine read only access to severity Level 2 IG SIRI records held on the Incident Reporting Tool and facilities to run reports. The ICO will occasionally (ad-hoc) request information from the HSCIC on lower severity IG SIRIs or Cyber Security SIRIs (where the incident also involves a data breach) to assist with their case assessments, complaints or investigation processes.

Severity Level 2 Cyber Security SIRIs will only routinely be reported to HSCIC and DH (not to the ICO).

Small teams within HSCIC External IG Delivery, the IG Alliance, DH, NHS England and the ICO will receive notification emails for severity level 2 (reportable) incidents recorded on the Incident Reporting Tool.

IG SIRIs which may be of interest to regulators such as NHS England, Care Quality Commission, and Monitor etc. will be escalated when appropriate.

The Department of Health will brief Ministers regarding significant SIRIs, as and when appropriate.

The purpose for sharing intelligence with key stakeholders is for supporting, guiding, assisting the investigation of breaches, performance monitoring and improving standards within providers, commissioners and suppliers of health and adult social care services in England. Therefore, information and analysis on SIRI near misses and all severity levels (0.1.2) may be shared with interested national bodies for this purpose.

What we publish or plan to publish.

- All information recorded as severity Level 2 (since 01 June 2013) under a 'Closed' IG SIRI on the IG Toolkit Incident Reporting Tool will be published quarterly (by date of closure) by the Health and Social Care Information Centre (HSCIC).
- Organisations must therefore check the content recorded within the IG Incident report before closing the record to ensure that you do not include any information that you would not normally provide or publish yourself if requested under the Freedom of Information Act 2000.[1] [2] Therefore, ensure information recorded is

[1] http://www.legislation.gov.uk/ukpga/2000/36/contents - the Legislation
[2] http://ico.org.uk/for_organisations/freedom_of_information - ICO Guidance

both factual, accurate and does not include any person identifiable data, essentially appropriate for publication.

- An auto closure feature will automatically close incidents where no updates to an 'open' record have been undertaken within the last 90 days. Relevant incident reporting users will be notified by email 10 days in advance of planned auto closure and within 24 hours after closure. Further details are described in Appendix A of the 'Incident Reporting Tool User Guide'.
- Other IG SIRIs marked as 'Open', 'Withdrawn', 'Level 2 (TBC)', 'Duplicate' or occurred before 01 June 2013 will not be published by the HSCIC.

    As only Level 2 IG SIRIs are mandatory to report via the IG Toolkit Incident Reporting Tool currently, details of near misses, Level 2 (TBC), Level 0 or 1 IG SIRIs should be obtained from local organisations. Organisations are advised to publish IG SIRIs in line with the 'Checklist Guidance for reporting, managing and investigating Information Governance and Cyber Security SIRIs' document.

- Cyber Security SIRIs will NOT be published by the HSCIC nor expected to be published by organisations impacted due to particular FOIA exemptions that require consideration on a case by case basis.

- Closed Level 2 IG SIRIs self-reported across Health and Adult Social Care will be published on a quarterly basis. Closed IG SIRIs - means an IG related incident that has been investigated by the local organisation and resolved but may still be subject to ICO investigations or actions. This can be found on the IG Toolkit Publications page.

Help

Further information on the data we collect regarding IG and Cyber Security SIRIs and the requirements/expectations of Health and Adult Social Care services with regard to reporting can be found within the two guidance documents noted below and available from the IG Toolkit website:-

- 'Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation' accessible from the IG Toolkit Knowledge Base , from the Publications page or on the Incident Reporting landing page when logged in.

- 'Incident Reporting Tool User Guide' accessible from the IG Toolkit Help section or the Incident Reporting landing page when logged in.

If you have any questions for the External IG Delivery Team please direct them to us via our IG Toolkit helpdesk service - 'Contact us'.