IG Toolkit V12.3 Cyber Enhancements to the IG Toolkit Incident Reporting Tool

Change Release Note

Friday 27th February 2014 Go Live

The External Information Governance Delivery Team has been working on a commission from the National Cyber Security Programme (NCSP) and with stakeholders in the Department of Health (DH) since September 2014. Testing and feedback has come through the Health and Social Care represented IG SIRI Design Group.

The commission is to enhance the functionality, content and guidance within the SIRI Incident Reporting Tool to cover related cyber incidents. The aim is to facilitate the reporting of significant cyber security related serious incidents requiring investigation (Cyber SIRI). The information obtained will be utilised to inform the national network of SIRO's and steer future direction in cyber security across the Health and Adult Social Care sector.

Incidents should either be classed as an IG SIRI, a Cyber SIRI or both. It envisaged that IG personal will report incidents in partnership with their IT colleagues alternatively IT colleagues can report incidents independently.

There is no interest to report every single log entry from a firewall or Intrusion Prevention System and incident is something you consider worthy of investigation. Please see checklist guidance and Publication Statement for further detail and examples.

The cyber incident reporting tool functionality will not impinge on existing processes to report IG SIRI's. This continues as normal.

This release includes the following updates to the SIRI Incident Reporting Tool:

Please note:

- *HSCIC Cyber Security Viewer (a small team of HSCIC Information Security Subject Matter Experts (SMEs). Monitoring cyber security activity across the sector nationally).*
- *Incident Reporting User (IG Toolkit registered Incident Reporting User).*
- *Incident Support Manager (HSCIC External IG Delivery Team).*

The Incident Reporting Tool and these changes will not be visible to public viewers of this website or registered users without the appropriate role/permissions allocated. Contact your local organisation administrator or IG lead if you feel you need access.

Change Log Ref.	Requirement Title	Change description
IGT/V12.3/CS/1	Ability to classify type of incident	As an Incidents Reporting User you are able to signify the type of incident and distinguish between IG SIRI and Cyber Security SIRIs.

Change Log Ref.	Requirement Title	Change description
IGT/V12.3/CS/2-1	Ability to search by type of incident	As an Incidents Reporting User or Incidents Support Manager you are able to search by type of incident in order that you can quickly distinguish between Cyber Security SIRIs and IG SIRI incidents.
IGT/V12.3/CS/2-2	Changes to Search Export Depending Upon Type of Incident Searched For	As an Incidents Reporting User or Incidents Support Manager when you export search results the exported incidents will only contain the columns pertaining to the type of incident you are reporting on in order to avoid having many redundant columns when reporting on a particular type of incident.
IGT/V12.3/CS/2-3	Identifier to indicate type of incident	As an Incidents Reporting User or Incidents Support Manager you are able to tell from the identifier for an incident what type(s) of incident it is and can easily distinguish between IG and Cyber security incidents. For example: IG SIRI ID prefix = IGI Cyber SIRI ID prefix = CSI Both IG and Cyber SIRI – IGICSI
IGT/V12.3/CS/2-4	Search by Incident Type to include Both option	As an Incidents Reporting User or Incidents Support Manager you can search for incidents which have both an IG SIRI element and are also Cyber Security Related in order to quickly identify those Cyber incidents which lead to a data loss.
IGT/V12.3/CS/3	Don't display IG SIRI Specific fields if Incident is not an IG SIRI Incident	As an Incidents Reporting User you do not see or have to record IG SIRI specific information for Cyber Security only incidents in order that the data recorded is streamlined and appropriate to the type of incident.
IGT/V12.3/CS/4	ICO not able to view Cyber Security incidents	ICO Users are unable to view Cyber Security related incidents unless they are also an IG SIRI Incident. The ICO will see that there is a Cyber related aspect to the SIRI but they will not have view of any detailed information unless requested from the organisation if under investigation regarding an incident.
IGT/V12.3/CS/5	Addition of new fields to Incident Subject Details section	As an Incidents Reporting User you can enter additional subject details for an incident in order that you can better record the nature of the incident.
IGT/V12.3/CS/6	Addition of new Cyber Security tab to search screen	As an Incidents Reporting User or Incidents Support Manager you can see a new tab on the search screen dedicated to searching for fields pertinent to Cyber Incidents only in order that you can quickly identify Cyber incidents of interest.

Change Log Ref.	Requirement Title	Change description
IGT/V12.3/CS/7	Ability to search for incidents affecting National Systems	As an Incidents Reporting User or Incidents Support Manager you are able to search for incidents affecting National Systems (where recorded on the tool) in order that you can quickly identify Cyber incidents which potentially have or had a national affect.
IGT/V12.3/CS/8	Incident Reporting Users do not see Source field on incident form, always set automatically to Direct	As an Incidents Reporting User you will no longer see a 'source' field.
IGT/V12.3/CS/9	Hide organisation details on incident form	As an Incident Reporting User you will no longer see organisation details on the Incident Details form. This is an attempt to streamline the appearance of the form.
IGT/V12.3/CS/10	Addition of Cyber Security fields to the General Details section	As an Incidents Reporting User you can record additional Cyber Security specific information in the general detail section in order that the details captured for a Cyber Security incident are complete.
IGT/V12.3/CS/11	Ability to search by new General Details fields	As an Incidents Reporting User or Incidents Support Manager you can search by Cyber specific general details in order that you can quickly identify Cyber Incidents of interest.
IGT/V12.3/CS/12	Ability to record start/end date/time for Cyber incidents only and show duration of incident	As an Incidents Reporting user you are able to record start and end dates/times for Cyber security incidents in order that the duration of the incident can be determined.
IGT/V12.3/CS/13	Ability to record the impact of a Cyber Incident only	As an Incidents Reporting User you can record the impact of a Cyber Incident in order that the effect of the incident upon your organisation or individuals can be recorded.
IGT/V12.3/CS/14	Ability to search by Impact of Cyber Incident	As an Incidents Support Manager or Incidents Reporting User you can search by the impact of an incident in order that you can quickly identify Cyber incidents which have had a particular impact.

Change Log Ref.	Requirement Title	Change description
IGT/V12.3/CS/15	Ability to specify Baseline scale for Cyber incidents only	As an Incidents Reporting User you are able to set the Cyber Baseline Scale for an incident in order that the Cyber level of the incident can be determined.
IGT/V12.3/CS/16	Ability to search by Baseline scale for Cyber Incidents	As an Incidents Support Manager or Incidents Reporting User you can search by the Cyber Baseline Scale of an incident in order that you can quickly identify Cyber incidents which have a particular baseline scale.
IGT/V12.3/CS/17	Ability to specify separate sensitivity factors for Cyber Incidents only	As an Incidents Reporting User you are able to specify sensitivity factors for a Cyber Security Incident in order that the Cyber SIRI Level can be determined.
IGT/V12.3/CS/18	Ability for system to calculate and display Cyber SIRI Level	As an Incidents Reporting User you are able to see the Cyber SIRI Level for the incident being edited in order that you can determine whether or not the incident needs reporting
IGT/V12.3/CS/19	Ability to Search by Cyber SIRI Level	As an Incidents Support Manager or Incidents Reporting User you can search for incidents with a given Cyber SIRI Level in order that you can quickly identify reportable/non-reportable incidents.
IGT/V12.3/CS/20	Notify Later Functionality for Cyber SIRI Level 2 Incidents	As an Incidents Reporting User you are able to choose to notify Cyber Level 2 Incidents at a later date in order that you can obtain internal authorisation before reporting the incident to external bodies. Please note – Cyber SIRI Level 2 Incidents which you choose to notify will be alerted to the HSCIC and Department of Health (DoH)
IGT/V12.3/CS/21	New Level 2 Notification Email for Cyber Incidents	The HSCIC and DoH are informed via email when a Cyber SIRI Level 2 Incident is notified.
IGT/V12.3/CS/22	ICO Notification email not sent unless is an IG SIRI Incident at level 2	An ICO user does not receive notification emails unless the incident is an IG SIRI Incident with IG SIRI level set to 2. ICO will not receive notifications relating to Cyber Incidents.
IGT/V12.3/CS/24	New Level 2 Downgrade Email for Cyber Incidents	The relevant National Bodies are informed via email when a Cyber SIRI Level 2 Incident is downgraded to less than Cyber SIRI Level 2 or when the incident is marked as Duplicate or Withdrawn in order that they know to stop investigating the incident further.

Change Log Ref.	Requirement Title	Change description
IGT/V12.3/CS/26	Combined IG and Cyber Level 2 Downgrade Email	Relevant National Bodies which receive both Cyber and IG SIRI Level 2 Notification emails
IGT/V12.3/CS/29	Ability to enter Root Cause Analysis for Cyber Incidents only	As an Incidents Reporting User you can enter the Root Cause Analysis for a Cyber Security Incident in order you're your organisation can track the causes of Cyber Incidents.
IGT/V12.3.CS/30	Changes to Disclaimer Text at top of screen	Additional Cyber lines added to disclaimer. Please note – Users are advised to read this disclaimer again or routinely as a reminder.
IGT/V12.3.CS/31	Changes to context help	Context level help exist per new cyber field in attached document. Click on the ? symbol by the incident form field for help where available.
IGT/V12.3/CS/32	ICO not able to see Cyber Security specific information	ICO users are not able to see information relating to the Cyber security aspect of an incident. This is to encourage use of the tool to record Cyber Security incidents.
IGT/V12.3/CS/33	New Role for Cyber Security Incidents Viewers	A HSCIC user with the role Cyber Security Viewer is able to view Incidents with a Cyber Security element in order that they can keep track of Cyber Security related incidents across the Health and Social Care sector nationally.
IGT/V12.3/CS/35	Changes to Existing Organisation Summary Report	Incidents Reporting User and Incidents Support Manager can view an improved layout for the Organisation Summary report in order that the report is clearer and easier to read.
IGT/V12.3/CS/36	Ability to run Organisation Summary Report for Cyber Security Incidents	As an Incidents Reporting User and Incidents Support Manager you can run the Organisation Summary report for Cyber Security Related incidents in order that you can deliver information on Cyber Incidents to interested parties. This is exportable to Word.
IGT/V12.3/CS/37	Ability to run Date Range report for either IG or Cyber Security Incidents	As an Incidents Reporting User and Incidents Support Manager you can specify which type of incident you wish to run the Date Range report for in order that you can produce different reports for different interested parties on both IG and Cyber SIRIs.

Change Log Ref.	Requirement Title	Change description
IGT/V12.3/CS/41	Indication of mandatory fields on Incident details screen	As an Incidents Reporting User or Incidents Support Manager you are guided by the screen as to which are mandatory fields in order that the incident form can be filled in more easily.
IGT/V12.3/CS/42	Rearrangement of fields on search screen	As a user of the Incident Reporting system you can see the searchable fields in logical groupings in order that it is easier to find the field you wish to search by. Please note – the search tabs have changed from 1. Basic and Advanced to 2. General, Data breach and Cyber Security.

Updated Guidance

The Incident Reporting Tool updates and recommendation to report Cyber SIRIs are also documented within the latest "*Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation*" available from the Incident Reporting Tool tab when logged in or from the IGT Help or Knowledge Base tool found at the 'Resource' tab.

Help on navigation around the tool and using the incident reporting tool can be found in the Incident Reporting Tool User Guide available from the IG Toolkit help page or on the Incident reporting landing page (when logged in).

Help

If you have any queries regarding these enhancements (either IG SIRI or Cyber SIRI) please contact the IG Toolkit helpdesk and quote 'Incident Reporting Tool Query'. Go to the help tab and select 'Contact us'.

External IG Delivery Team

IG Standards and Assurance Directorate

Health and Social Care Information Centre