QES Proposal

Manchester Safeguarding Partnership

PREPARED BY

EMMA BARRAND

Sales and Marketing Manager

Version 3.0

02/07/2020

PROUD SOFTWARE PROVIDERS

Contents

1 QES Experience

QES specialise in developing online software systems for Health, Local Authorities and the Police. With over 16 years' experience in delivering successful applications, and in excess of 250,000 users, we have vast experience of multi-agency data sharing through the use of case management and surveillance systems.

QES are the safeguarding experts for software solutions, and we are proud to offer a Holistix Safeguarding suite of out-the-box products and the ability to successfully develop tailor-made systems. See below for just a few of the systems we have developed:

- Holistix eCDOP
- Holistix Suicide Surveillance
- National Child Mortality Database (NCMD)
- Holistix Case Review: Adult, Child, Domestic Homicide, MARAC, LeDeR
- Holistix eLADO
- Holistix Section 11
- Holistix eLearning

We are passionate about implementing safeguarding solutions that can make a difference. It's a specialist area for us, having already successfully delivered over 140 children's and adult's safeguarding tools across the UK.

2 eCDOP System

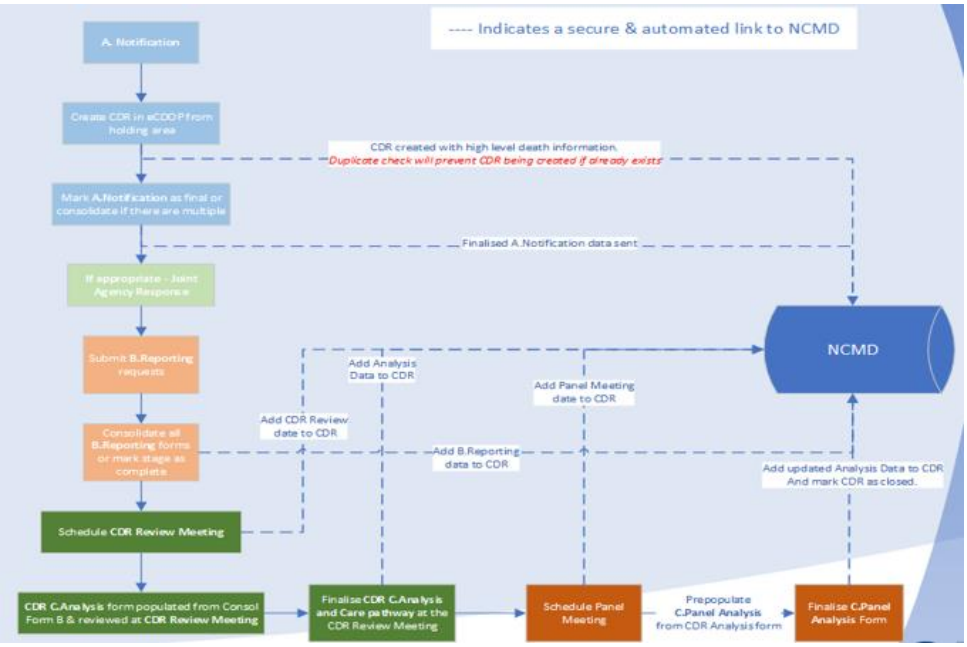
eCDOP is a secure, flexible and web-based solution which allows the Child Death Review (CDR) process to be fully managed efficiently, with effective sharing of multi-agency information. The system provides a secure way of connecting your network of partners in your CDR arrangements. The system has evolved and flourished, originally designed by Kent LSCB, and it is now successfully being used by 123 Local Authorities and their CDR partners across England.

Please see below for some of the main functionalities and benefits of the system:

- eCDOP is automatically connected to the National Child Mortality Database (NCMD), and the statutory data is instantly transferred at each of the required stages. See below for a diagram of this.
- All statutory forms and workflows from the Working Together 2018 are adopted in the eCDOP system. By using eCDOP, you will be compliant with the national CDR guidance.

- The system and transfer of multi-agency data is completely secure and GDPR compliant, with no risk of sensitive data being compromised.
- National standard annual report data generation tool incuded
- Provides a centralised location for the full end to end case management of a case, providing secure and organised access to information.
- CDRs can electronically receive notifications via an online, publicly available form, then instantaneously distribute secure details of death to their respective partners, saving valuable time in the notification process.
- Reporting Forms are issued to agencies at a click of a button, with mandatory fields for improved data completeness and quality of data returns. There is also an automatic chasing feature, saving CDOPs the manual task of constantly sending reminders.
- Rapid Response Meetings, CDRMs and CDR panel meetings can be organised and managed online through the system. This includes electronically inviting and managing attendance, sharing forms and case information securely with version control, and storing agendas, minutes and actions.
- CDR coordinators, or the lead clinicians, can easily access the analysis form to complete this via eCDOP during the CDRM.
- The forms in eCDOP all pull forwards, to avoid double data entry. For instance, the notification form transfers data into the reporting forms, and reporting form into analysis form. This has been proven to save the recipient time, and subsequently improves the quality of data.
- The efficiencies in the process provides more time for the team to focus on other areas of child safeguarding, such as engagement or campaigns. The system has been reported to have reduced time spent from 2 days per week to 2 hours.
- Various efficiency features are available in the eCDOP system, such as automatic chasing of reporting forms, anonymisation of panel meeting forms if desired, consolidation of both the notification forms and reporting forms, triggering alerts to lead clinicians for approval of rapid response meeting minutes, etc.
- The CDR team have instant access to real time data through an interactive dashboard, providing the ability to proactively monitor trends and react to emerging issues more quickly.

2.1 eCDOP to NCMD data transfer diagram:



3 The Proposal

3.1 Overview

The National Pricing Model for the eCDOP system is based on the number of child deaths cases per year. The calculations for a quote are based on the last published government report.

It was reported to QES that Greater Manchester are notified of approximately 280 deaths per year. Having checked the last published government report, for the below listed 10 local authorities in Greater Manchester, there were 224 deaths reviewed on the last published DfE website. After discussions between our organisations, we have agreed to price this proposal on the average number of deaths reviewed between the last published DfE report and the last published (2018-2019) report by Greater Manchester on their website (204 deaths reviewed).

- Bolton
- Bury
- Manchester
- Oldham
- Rochdale
- Salford

- Stockport
- Tameside
- Trafford
- Wigan

QES have based the calculations for this quote on 214 deaths reviewed per year, as this is our standard national approach and the average of the two published reports.

We have provided two options in this proposal, depending on whether Greater Manchester wish to use one system for all 10 areas, or whether they split up based on 4 CDRs within Greater Manchester.

Please note, all costings for both options in this proposal are excluding VAT and are annual. The costs include the hosting, maintenance and support of the system, including regular patch upgrades with new functionalities.

Training is also included. eCDOP has an in-built eLearning tool which includes training videos and guidance on how to use the system. A training webinar is also provided to the CDR managers, administrators and lead clinicians to ensure the smooth transition onto eCDOP.

3.2 Option 1

Option one is based on 4 CDR partners using 4 separate eCDOP systems. We have found these 4 CDR partnerships via the respective websites, but if these require changing please let QES know and we will make the relevant amendments to this proposal.

Please find the individual costs for each of the 4 areas below.

- Bury, Rochdale and Oldham (average of 50.5 deaths reviewed) = £8141
- Manchester (average of 55.5 deaths reviewed) = £8977
- Stockport, Tameside and Trafford (average of 43.5 deaths reviewed) = £7305
- Bolton, Salford and Wigan (average of 64.5 deaths reviewed) = £9813

There will be individual administrators and system users for each of the 4 systems. These users will not be able to access the data from other eCDOP systems, only their own. The 4 systems will not be linked to each other in any way.

3.3 Option 2

Option two is based on one joint eCDOP system for all 10 local authorities and their CDR partners within Greater Manchester.

The cost of one joint eCDOP system for all 10 areas is: £28,811

This will involve all 10 areas using one joint system. This will allow for collaborative panel meetings, and the option to view dashboard reporting on an individual, multiple CDRs or whole Greater Manchester level.

Within this option, there is the functionality to add restrictions to what administrators can see. For instance, multiple administrators could see data from across the whole of Greater Manchester, or alternatively you could have Manchester admins only seeing Manchester cases and another administrator only accessing Bury, Rochdale and Oldham cases. Regardless of the security set up here, administrators will still be able to access joint reporting and joint panel meetings as required.

4 What are your next steps?

Please let us know what your next steps are and we will do our best to help to facilitate this process in any way we can.

Please see below for a few ways QES can help with the next steps:

- See the system! If you and your team would like a demonstration of the eCDOP system, QES are able to provide this via a virtual webinar. This can be on an individual or regional basis.
- QES can share a business case proposal which can facilitate the procurement process.
- We have other documentation available which can help with your set up process, for example a separate Information Governance document (see the next section for it embedded within this document), or guidance text for partners to help with roll out.
- We can introduce you to other areas of the country who are using the system to share experiences.

The eCDOP system can be made available to your team 3-4 weeks after sign off. The sooner you start the next steps, the less time you have to manually enter data in NCMD.

5 Security

5.1 ACCREDITATION

5.1.1 ISO27001

Certification Number: 14123656

QES are ISO27001 accredited and have been for more than 5 years now. ISO27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

For more information visit the ISO website https://www.iso.org/isoiec-27001-information-security.html

5.1.2 ISO9001

Certification Number: 14131696

QES are ISO9001 accredited and have been for more than 5 years now. ISO9001 sets out the criteria for a quality management system. To find out more information visit the ISO website https://www.iso.org/iso-9001-quality-management.html

5.1.3 ICO Cyber Essentials

Certification: https://apmg-certified.com/PublicOrgLogin/Certificate.aspx?g=8c68e689-7585-421b-9a6f-94db5a5d89b9

QES has recently acquired their Cyber Essentials accreditation demonstrating compliance with ICOs cyber security best practice. To find out more please visit https://www.cyberessentials.ncsc.gov.uk/

5.1.4 NHS Data Security and Protection Toolkit

Organisation Code: 8HP86

QES annually renew their NSH DSPT assessment.

5.1.5 N3/HSCN

QES has an N3/HSCN pipeline established and in use by some of our NHS clients.

5.1.6 CREST

Staff at QES have been trained in CREST accredited Ethical Hacking courses. This helps our development team understand threats and implement preventative measures within our solutions. It also enables us to deliver internal penetration tests of our applications and infrastructure.

5.1.7 GASQ – Global Association for Software Quality

Staff at QES have been trained in GDPR readiness through GASQ.

5.2 GDPR READINESS

5.2.1 Categorisation/Summary

QES are registered Data Processors and not Data Controllers. We are compliant to the standards outlined by the ICO Self-Assessment and have taken the necessary steps to ensure we understand the GDPR legislation and taken remedial steps as part of our Information Flow audit to ensure our controllers data continues to remain secure and safe.

5.2.2 Documentation

An information flow audit has taken place and been documented as part of our GDPR readiness. These informed areas of improvement which have now been remedied, in particular on-site and offsite full device encryption.

An asset register has also been documented as a result of this to better understand the assets within the QES domain.

5.2.3 Governance

QES already has a Data Protection policy as part of our ISO27001 compliance. This policy has been expanded to specifically reference GDPR and the revised expectation of us as Data Processors.

5.2.4 Data Protection Officer (DPO)

QES has had a governance officer for 5+ years who was responsible for ensuring we comply with our ISO standards. This member of staff has been upskilled in GDPR governance (IT Governance EU GDPR Foundation Certified) and assigned as our DPO.

5.2.5 Management Responsibility

Management meetings are held quarterly to review our governance and any policy modifications as a result of GDPR must be approved by them. Weekly GDPR meetings feed a report into our Operational Management meetings to inform management of GDPR activity.

5.2.6 Data Protection Impact Assessment (DPIA)

Impact assessments have now been added to our Requirements documentation and take place on all new Projects we deliver. An impact assessment has been performed on our infrastructure as a result of the Information Flow audit we performed as part of our initial assessment.

5.2.7 Data Protection by design

By introducing a DPIA at the design stage of a project we are ensuring thought is given and documented to the security architecture of the build. Senior members of staff are included in this security review to ensure good practice is being observed.

5.2.8 Training and Staff awareness

As part of our readiness programme, QES has specifically upskilled staff in two areas; GDPR readiness and CREST Technical Application Security testing, enabling us to better understand and implement defensive measures against threats to data security and integrity. All staff have been trained and made aware of GDPR and the ICOs Think.Check.Share guidance.

All QES staff are DBS checked.

5.2.9 Sub-Contractors

QES only use in house staff to implement their products. They do however sub-contract Microsoft Azure to host our databases and web applications in a datacentre in Cardiff, UK. This data never leaves the UK.

For more information on Microsoft Azure's Governance and Security compliance visit their website https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

5.2.10 Operational Base

QES operate exclusively in the UK and all data we process never leaves the UK.

5.2.11 Data Breach

In the unlikely event of a data breach QES will inform the data controller immediately and ICO within 24 hours of its occurrence.

QES has never had a data breach.

5.2.12 Right of Access

QES has established a Rights of Access request form which handles any of the requests now entitled to the data controller under GDPR.

Where possible QES has also implemented technical solutions to process Right of Access requests from within the application.

QES uses a custom-built tool which assists us in identifying unique instances of people across different datasets to help facilitate effective Rights of Access requests.

5.2.13 Data Security Policy

QES already has a security policy documented as part of our ISO27001 compliance. This has been updated to make specific reference to changes made in the GDPR legislation.

Retention policies are in place to ensure QES does not retain information longer than it is required. Which in this case is until the end of the contract period, unless the contract states otherwise.

We also have a mechanism internally for identifying records across the organisation to ensure all traces of the data can be identified and processed accordingly.

5.3 APPLICATION SECURITY and HOSTING

5.3.1 Application Security

Our applications use PBKDF2 SHA256 encryption. To find out more about this method of encryption please view this article https://en.wikipedia.org/wiki/PBKDF2

Two Factor Authentication is also enabled on our applications. In addition to the user name and password users are sent a one-time access code by email when they login. This must also be entered before a user is authenticated with the system.

The application logs extensive audit events which are readily available to administrators of the system through the Administration menu.

5.3.2 Secure Development

QES applications are periodically tested for vulnerabilities by a permanent member of the development team who has been trained in CREST Ethical Hacking and penetration testing as well as continually

tested using our automated testing model through TFS build and release (https://www.visualstudio.com/team-services/continuous-integration/)

Through continuous integration (DevOps and DevSec) we are able to use established tools which specialise in checking for vulnerabilities but also build our own custom tools which run **every time we make a change to the system**.

An example of a few we have integrated;

- SonarQube - a code quality tool which checks for bugs and vulnerabilities in the code in line with OWASP. (https://www.sonarqube.org/)
- OWASP ZAP (Zed Attack Proxy) – Vulnerability scanner (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)
- Custom built – API anonymous scanning – Ensures that there are no vulnerable APIs
- Custom built – Web.config checks – Ensures all security keys are enabled.

Our applications are web based and HTTPS enabled. All transportation of data between application and database at both Azure and QES is done over a TLS1.2 encrypted channel.

QES development team run monthly “Hackathons” whereby we attempt to hack into our applications in a test environment which mimics that of the production environment. The findings of this are then fed into the development sprints for remediation.

5.3.3 Hosting

Location

- Azure primary datacentre is in Cardiff, UK
- Azure secondary (paired) datacentre is in London, UK
- Data never leaves the UK.

Database backups

- Full backups are taken daily
- Differential backups are taken every 2 hours or increase of 5mb (whichever comes first)

Redundancy

- Backups are stored in Geographically Redundant Storage (GRS) offering 99.9999999999999999 (16x9s) redundancy
    - **GRS** replicates your data asynchronously in two geographic regions that are at least hundreds of miles apart. If the primary region suffers an outage, then the secondary region serves as a redundant source for your data. You can initiate a failover to transform the secondary endpoint into the primary endpoint.
- Disk replication to paired datacentre in London happens every 5 minutes

Recovery

- Full datacentre failure
    - Service would be reinstated to within 5 minutes of when the event occurred.
    - Return to service time will be <1 hour

Azure monitor and inform us of any suspicious activity (intrusion detection) on the server and we have built custom proactive monitoring alerts that will notify of immediate or impending service failure.

5.3.4 Data Segregation

All data we store for our clients are held in distinct, separated databases, with unique SQL logins. There is no possibility of any data being shared from other clients as a result of this architectural approach.

5.3.5 Vulnerability Testing

Annual Penetration tests are performed by the NCCGroup on our infrastructure.