



Technical assurance framework










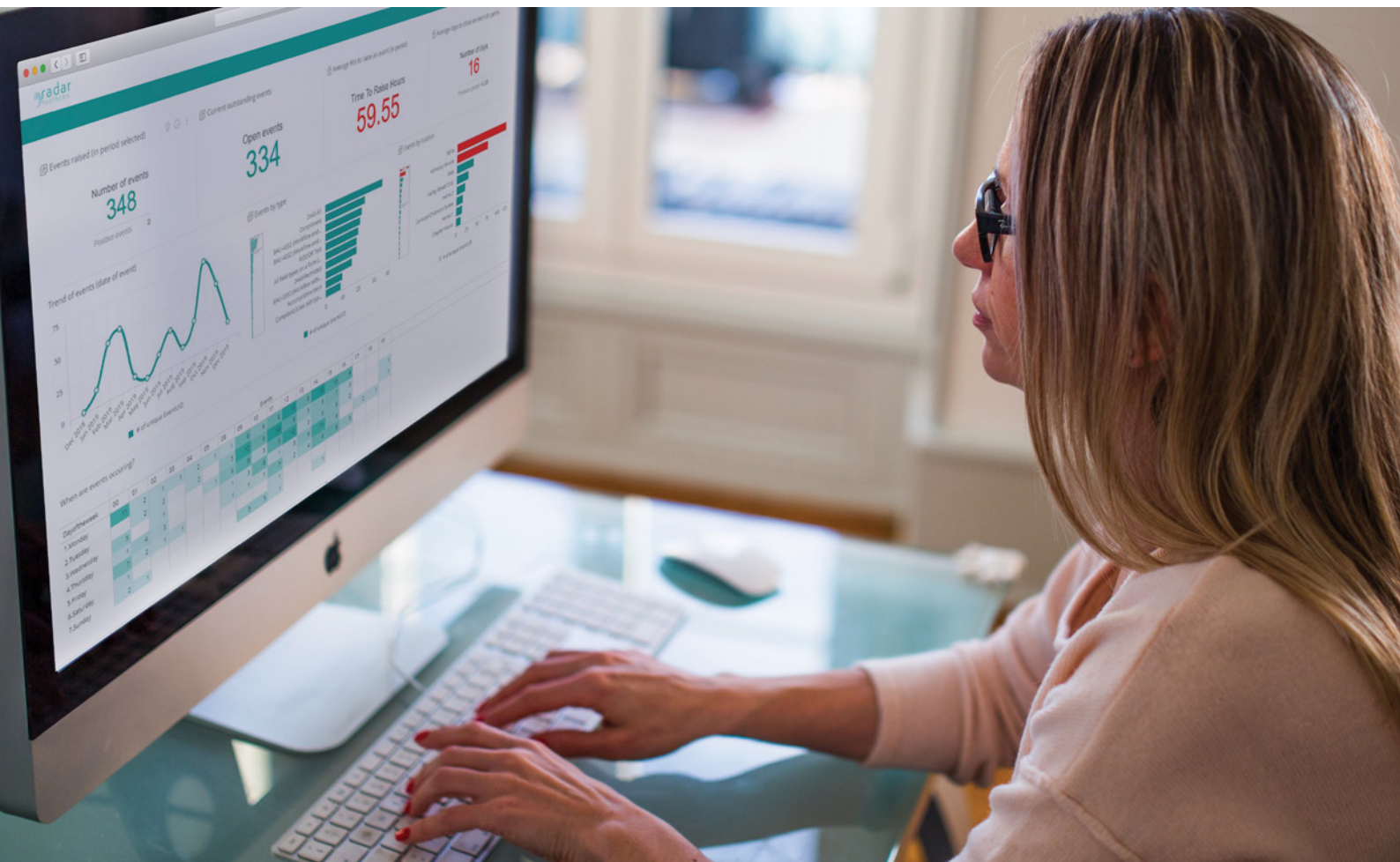
Executive summary

- Our hosting and support service include 24/7, 365 monitoring with a proven pedigree in healthcare IT and communications.
- Hosting centres are Tier 3 designed, located across five UK data centres (including Reading, London, Cambridge & Harrogate).
- Access to features is determined by the permissions granted to each users' role, this ensures that data and features are only access by appropriate users. Hosting utilises SSL certification among other security layers, with the option of an N3 connected service.
- Our data protection obligations are all outlined in our software license agreement in line with GDPR legislation.
- Radar Healthcare has been developed as a 100% web based solution so that there is no direct impact when your IT strategy results in upgrades or version changes to your various devices. This means that there are no enforced hardware overheads to the continued use of Radar Healthcare.
- Radar Healthcare can provide SSO via SAML 2.0.
- Radar Healthcare provide standard integrations for interoperability- potential data for integration may include some or all the below;
 - * Patient Administration System (PAS). Admission, Discharge and Transfer (ADT), electronic patient record (EPR), Staff/User details (HR), Medication lists, Care planning software, eLearning providers
 - * You own your data. The system architecture ensures the data is both protected and securely stored for the duration of the contract. Accessibility to all data held in Radar Healthcare is available at all times
- Radar Healthcare is application penetration tested by a 3rd party at least every 12 months to ensure any application vulnerabilities are detected and resolved.
- Copies of the reports are available upon request.



Contents

 Hosting	4
 User management	6
 System requirements	7
 Integration/Interoperability	10
 Release management	12
 Business continuity and disaster recovery	13
• Corporate disaster recovery plan	13
• Hosted service partner disaster recovery	14
 Security/penetration testing	15



Our hosting and support service include 24/7, 365 monitoring with a proven pedigree in healthcare IT and communications.

Our hosting provider Redcentric (www.redcentricplc.com) is a leading UK IT managed services provider.

All its hosting centres are Tier 3 designed, located across five UK data centres (including Reading, London, Cambridge & Harrogate).

These data centres provide geographically dispersed, highly secure computing environments with 24 hour A/C power, UPS with emergency generator backup, ventilation, air conditioning & computer monitored climate control for heating (HVAC); and fire detection & suppression. Redcentric hold a range of accreditations and are a specialist provider of N3 and HSCN connected services to health and social care in the UK.

Data centre certifications include:

- ISO27001 Certified (British Standards Institution)
- ISO9001 Certified
- ISO14001
- ISO 22301
- ISO 20000
- PCI Compliant for hosting services at Harrogate and Reading Data Centres
- Authorised to process HM Government data protectively marked 'Official-Sensitive'
- Cyber Essentials Certified
- PSN Network accredited
- PSN Gateway service access
- CAS – Telecommunications
- HSCN - Crown Commercial Service framework (also called RM3825)

Accreditations include:

- PCI Compliant for hosting services at our Harrogate and Reading Data Centres
- Authorised to process HM Government data protectively marked 'Official-Sensitive'
- PSN accredited for the provision of Infrastructure as a Service
- Accredited to connect to and supply services over Janet into all connected institutions and organisations
- Accredited to store patient data for and behalf of the NHS
- Independent aggregator of IGSoC Version 14 with a score of 100%
- Code of Connection approved (3rd party N3 hosting provider onto the N3 network by HSCIC)
- Compliant Commercial Third Party (NACS Code YGMAP)
- NHS Health (and Health & Social Care Information Social Care Centre)- accredited N3 & HSCN ISP
- Information Governance Statement of Compliance (IGSoC)
- GCloud approved supplier
- Janet Telephony framework (JTPS) approved supplier

This solution provides our customers with the confidence that their system will operate at the most critical of times, providing the following principal benefits:

- **Fully managed service.** We will take responsibility for full system delivery inclusive of hardware, software and technical resource
- **System resilience.** The off-site solution provides full resilience and accessibility even in the event of catastrophic failure of your internal system
- The specialist hosting centres are fully equipped and managed 24/7 to provide a support service capable of delivering very high uptime supported by a formal SLA
- **Data retention.** Off-site storage of data provides full data recovery capability

Redcentric more detailed service includes:

- Full physical security controls such as manned security, CCTV, ID access cards and man-traps in place
- Full system monitoring is in place 24/7 365, manned by the Redcentric support team. The software agent monitors Processor, Memory, Disk, Availability, and Services. Alerts generated by the software agent will automatically raise an incident within Redcentric's service desk. Redcentric investigate the alert and corresponding fault
- Backups to offsite locations are taken as follows: Database transaction logs every 15 minutes, each individual database every 24 hours, servers imaged every 24 hours. Disaster recovery as a service is also provided using the backups as mentioned above
- Downtime, where planned and unplanned, has an agreed communication plan with the client to ensure clear communication channels are defined and followed
- Server management including operating systems, database and application software updates when appropriate, are managed by Redcentric on at least a monthly basis. Any updates are first tested on the test environment to ensure no adverse impact before applying to the production environments
- Anti-virus is managed by Redcentric using Sophos, this includes On access scan, Tamper control, Device control and auto update
- Regular contract performance reviews are held with Redcentric to ensure the services are in line with the contractual requirements, along with discussions around any advances in the services offered by Redcentric, to ensure we fully benefit from all their considerable expertise and experience
- Full change management controls and procedures compliant with ISO9001 are in place ensuring that any changes are controlled in a defined and traceable manner



User management

User access/Role based access

Radar Healthcare's internal security and architecture has been designed to the highest standards, operating a comprehensive role-based approach, allowing for permission and access rights to be controlled by the system administrator.

During the implementation phase the system is pre-configured with your business rules, roles and associated permissions, which can be applied to an individual role or on a group basis. Within this framework access to features, modules and confidential content can be managed, with permissions set dynamically through the intuitive administration area.

Data is controlled through the respective role and dashboard configuration to ensure only the relevant amount of data is being presented to the respective user.

Software security

Radar Healthcare supports a range of security features including:

- Activation process
 - * The first email you receive from Radar Healthcare will be your activation email. This allows you to verify your account and confirm that the email address connected to your account is correct. This email is only valid for **48 hours**
- Log on process
 - * Each user receives their own unique log on credentials and can access Radar Healthcare through any internet connected device using our secure network, which is the same as internet banking
 - * Radar Healthcare uses reCAPTCHA by Google on the login page to help ensure that you are a real person logging in (and not just an automated robot!)
- System timeout
 - * If you are inactive for 20 minutes, you are presented with a "time out" warning message. To remain in the system, you simply click the stay logged on button
- Regular forced password changes aligned to applicable security standards

Secure password management

Best practice password management techniques have been utilised throughout Radar Healthcare, including the following:

- Passwords are set by sending an email to the registered email address with a link that is valid for 48 hours
- Account activation can only be performed by a system administrator
- Passwords are required to be at least 8 characters long, with at least 1 number, 1 letter and 1 special character
- If you have forgotten your password, you can request a new password from the Radar Healthcare login page. If the email address you have entered is correct, you will receive an email which will contain a password reset link that will be active for 48 hours. If you do not click the link within this period, the link will expire, and you will need to request a new reset email
- Automatic password expiry forcing a new password to be changed can be enforced, this is configurable

GDPR

Our data protection obligations are all outlined in our software license agreement in line with GDPR legislation.

Product roadmap and feature requests

At Radar Healthcare we value user involvement in the design and specification of our software, viewing an iterative development process as being crucial to the success of the project. To facilitate this, we hold a number of customer workshops during the contract period (reviewing current and future states) and also provide access to our BETA programs. To further support the ethos of user involvement, we operate an online forum section from within the Radar Healthcare Support Portal. The forum provides easy access to review release updates, as well as providing a mechanism for logging development ideas & voting on new feature requests. This gives users a direct route for feeding in requests, asking questions about Radar Healthcare and sharing best practice with other users, which helps with engagement and uptake of the system.

Additionally, our account managers provide customers with a roadmap of any major feature releases over the next 12 months. These software releases are scheduled based on how early the value can be released to the customer and as such are not fixed to a specific time frame (e.g. Quarterly) This means that the customer benefits from the release as soon as available as opposed to waiting for an arbitrary calendar date.

System requirements

Radar Healthcare has been developed as a 100% web based solution so that there is no direct impact when your IT strategy results in upgrades or version changes to your various devices. This means that there are no enforced hardware overheads to the continued use of Radar Healthcare.

Additionally, Radar Healthcare benefits from being developed as a responsive website. Responsive web design (RWD) is an approach to web design which reacts to the size of the user's screen, optimising the browsing experience by creating a flexible and responsive web page specific to the devices and window/screen size accessing it.

Web browser access

Radar Healthcare supports a variety of the most frequently used internet browsers, as detailed below. This range of compatibility means that there is no additional overhead or "hidden costs" to implementing Radar Healthcare.

- Google Chrome (Recommended browser)
- Microsoft Edge - (Chromium version only)
- Mozilla Firefox
- Safari

URLS and ports

Radar Healthcare use the following URLs and ports:

<https://live.radarhealthcare.net/> - Live

<https://staging.radarhealthcare.net> – Customer test/sandbox environment

<https://training.radarhealthcare.net> – Customer training environment (not as standard)

Ports - Specific connectivity requirements for pass through the firewall are Port 443 and port 80

PC hardware and software requirements

Category	Minimum requirements	Recommended
Processor	Computer with a 1.2GHz processor	Computer with a 2.4GHz or higher processor
Memory	1 GB of RAM	4 GB of RAM or more
Display	1024 x 768 resolution	1280 x 1024 resolution or higher
Mouse	Any Microsoft compatible pointing device	Any Microsoft compatible pointing device
Connection	Broadband Internet connection	Broadband Internet connection
Operating system	Windows 7 and above	Windows 7 and above
Browsers	Google Chrome Microsoft Edge - (Chromium version only) Mozilla Firefox Safari	Google Chrome Microsoft Edge - (Chromium version only) Mozilla Firefox Safari
Other requirements	Microsoft Office 97 SR-2b or higher (for exports) Adobe Reader 6.0 (for PDF exports)	Microsoft Office 2007 or later Adobe Reader 9.0 or later

Macintosh hardware and software requirements

Category	Minimum requirements	Recommended
Processor	Mac computer with an Intel processor	Mac computer with an Intel processor
Memory	1 GB of RAM	4 GB of RAM or more
Display	1024 x 768 resolution	1280 x 1024 resolution or higher
Connection	Broadband internet connection	Broadband internet connection
Operating system	Mac OS X 10.6 "Snow Leopard"	Latest Mac OS version
Browsers	Safari Firefox 19 New UI Firefox 19 and Chrome latest version	Safari Firefox latest version or later New UI Firefox and Chrome latest version
Other requirements	Microsoft Office 2000 (for exports)	Microsoft Office 2007 or later

Mobile hardware and software requirements

Category	Minimum requirements	Recommended
Operating system	Requires iOS 12.4 or later. Compatible with iPhone, iPad, and iPod touch.	Latest iOS version, Latest Android version (8.0 and up) NOT Android GO
Devices	Only those devices as certified by Google.	Only those as devices certified by Google.

Accessibility/Design standards

Radar Healthcare understand the importance of engaging with users; capturing and using their experience as part of any on-going product development for Radar Healthcare. The “user-centred” design is integral to the development philosophy of Radar Healthcare, with an iterative process being part of any feature design.

The approach to the design process is based on ISO 9241-210:2010 Part 210: Human-centred design for interactive systems, which is used as the agreed internal standard, with workshops/wireframing/prototyping and Beta testing always undertaken.

UX is tested in Radar Healthcare using the below methods:

- Usability testing
- Heuristic evaluation
- Interviews
- Survey and questionnaires
- Analytics

Radar Healthcare supports the accessibility principles of the World Wide Web Consortium, incorporating the following features:

- All areas of the site have clear text labels or tool tips (where required) which ensure that any iconography/section is understandable
- Colour is used to highlight issues (Traffic light system)
- Icons and labels also adjust to ensure colour blind users are not adversely affected
- Users can use a keyboard instead of a mouse (e.g. Tab button to change field – Enter to select – arrow keys to navigate and to move up and down in a list)
- Browser settings can easily be adjusted and as the site is responsive, the text and layout adjust accordingly
- Radar Healthcare uses plain English descriptions and the sites UI/UX ensures different areas and sections behave in a uniform way

Data consistency

Radar Healthcare utilises a number of features to ensure that data remains consistent within the system:

- The design of forms and workflows incorporate an option to add user configurable data validation for each field. This validation could be a simple mandatory answer or could be a regular expression such as a pre-defined text format of ABC123. This regex can be used for postcodes, ranges of numbers, common formats such as employee ID's etc.
- As well as regex validation controls, calendar and time pickers are used to ensure data validity

Any bulk updates of data, such as employee information, undergo full validation to create an import file. This process shows errors where data cannot be imported and warnings where data has been imported but is possibly incomplete or inaccurate.

Data ownership

You own your data. The system architecture ensures the data is both protected and securely stored for the duration of the contract. Accessibility to all data held in Radar Healthcare is available at all times.



Integration/Interoperability

Radar Healthcare provides an integration service, using industry standard API's.

Radar Healthcare API (data to the customer)

Event data

- Reference
- Status
- Incident type
- Location

Customers API (data from the customer)

- Staff
- Location
- Regions
- Roles
- Unique reference numbers

Bespoke APIs

Radar Healthcare has the capability to deliver bespoke APIs; these however are not part of the standard offer and costed separately.

Patient Administration System (PAS). Admission, Discharge and Transfer (ADT), electronic patient record (EPR), Staff/ User details (HR), Medication lists, Care planning software, eLearning providers.

3rd party dependencies

The benefit of Radar Healthcare is that there is no reliance on external systems or services for the daily operation of the software. This means that there are no 3rd party dependencies and associated costs in operating Radar Healthcare and no adverse impact to changes in external systems.

Radar Healthcare utilise best of breed suppliers in the delivery of the overall business operation, ensuring a reliable, robust service:

- Redcentric (hosting provider)
- SendGrid (sends emails)
- Freshdesk (helpdesk)
- Sisense (embedded analytics)
- Jira (work item tracking)
- VSO (code host and building)
- Various 3rd party code packages (e.g. EntityFramework, jQuery etc)

Audit logs

The Radar Healthcare Audit Log provides administration users with the ability to automatically track every action undertaken by users which can then be used to investigate incidents or identify any user training needs.

The audit logs allow the admin user to search on:

- Action plans
- Administration activities
- Logins
- Type of audit
- Documents
- Events
- Notices
- Risk management
- Scheduled tasks
- Workforce compliance

Audit records contain:

- Module or area of product affected
- Details of the user making the change
- Activity undertaken by the user
- The date and time the event occurred
- Pre and post states

An accurate and well-defined audit log provides the evidence to find answers and solve issues.

Single sign on

Radar Healthcare provides standard single sign on via SAML.

SAML is an XML standard that facilitates the exchange of user authentication and authorisation data across secure domains. SAML-based SSO services involve communications between the user, an identity provider that maintains a user directory, and a service provider. When a user attempts to access an application from the service provider, the service provider will send a request to the identity provider for authentication. The service provider will then verify the authentication and log the user in. The user will not have to log in again for the rest of his session.



Release management

Planned maintenance and upgrades

Recognising that software maintenance can be disruptive to daily business routines, we collaborate with our customers to manage the updates and maintenance in an agreed and appropriate way.

- Patches/upgrades and maintenance are undertaken on a periodic basis; typically, every 2 weeks
- All customers are advised of any updates/upgrades, where downtime is typically 5 minutes (when the site is 100% unavailable)
- Radar Healthcare alerts the user to any maintenance/releases as part of the logon process
- Where appropriate, UAT testing and sign off take place for substantial features or specific configuration; this is typically undertaken in the UAT site
- Application availability is tracked and monitored internally and published on request

Down-time

Any downtime of the service is notified in advance and an "out of normal operational hours" downtime period is agreed in order to minimise any impact. System software updates are done as and when required, updated as a minimum every quarter. Downtime can be expected to last between 5 minutes and 30 minutes.

The update is managed by our deployment software and is thoroughly tested before the application is updated.

Exit planning

To ensure an orderly decommission exercise of the system at the end of the contract term, we will follow the process detailed in our exit plans, which cover both the organisation, and where required, the incoming system replacement requirements. We commit to working with a new provider to ensure continuity of service and will provide a full understanding of the data structure allowing access from the data archive. All archived client data and records are formatted to support both manual and advanced programming interface (API) exports.

Radar Healthcare have an existing Escrow licence in place to allow on-going data deposits for data migration during the full licence term.

Warranties/Escrow

Smartgate warrants that the system will meet the functional requirements throughout the licence term.

Smartgate have an existing ESCROW policy in place as detailed below:

Escrow provision through the NCC Group (<https://www.nccgroup.trust/uk>)

Escrow Agreement Number: 62300

Software Owner: Smartgate Solutions Limited



Business continuity and disaster recovery

Corporate business continuity and disaster recovery plan

Radar Healthcare work to a fully documented business continuity plan, which incorporates our disaster recovery strategy (The BCDR plan). It details our capability to plan for and respond to any incident or business disruption, in order to continue business operations at an acceptable predefined level. This includes incidents which may affect our staff, our office buildings, our IT equipment or our processes.

The BCDR plan consists of the arrangements in the event of a serious interruption to our business. Its aim is to minimise disruption of essential activities and any subsequent customer impact. While it is impossible to predict every type of potential incident that may threaten our organisation, it is relatively straightforward to set out a basic plan which can be implemented to cover a wide range of possible actions. The principal emphasis is on the response to the incident and not the cause of the incident. The plan is also flexible; it works irrespective of time of day, time of year or availability of key employees.

The basic principle of this plan is to provide a framework for the organisation to respond to any crisis, whether foreseen or unforeseen. Developing a library of plans for specific emergencies runs the risk that the occurring emergency has not been anticipated, or that an anticipated emergency develops in an unexpected way, meaning that the specific plans are of limited assistance or even rendered useless. Crisis management should align with normal management arrangements, not least because normal services will have to be maintained while the emergency is being handled.



Corporate disaster recovery plan

Our BCDR incorporates the Disaster Recovery plan, containing agreed actions in the event of significant or total loss of our IT infrastructure. All our systems are subject to Disaster Recovery planning exercises, which test that the system design is sufficiently robust to provide uninterrupted service to the users in the event of a disaster. The purpose of the DR exercise is to identify single points of failure and events (flood, fire, power outage etc) that might lead to interrupted service. All of these events are then subject to a risk assessment to identify what steps can be taken to mitigate the risks.

Three core areas are detailed in the plan:

- Radar Healthcare solution - we employ a world leading hosting partner to ensure resilience and continuity of service for the Radar Healthcare solution. The data centre has redundant systems for connectivity, electrical power, air conditioning and fire suppression
- Internet access - all our staff have laptops, mobile phones and broadband access from home, should the office facilities be unavailable
- Telephone – All telephony is carried out using an external network, which eliminates the risk associated with dedicated communication lines. Our telephone system supplier operates a robust DR process

Additionally, as part of the system implementation, we devise a contingency plan with you to ensure that core parts of the solution can be replicated on a pre-defined paper-based system as relevant.



Hosted service partner disaster recovery

As has been demonstrated on many occasions, the most sophisticated systems are dependent on resilient infrastructure to deliver consistent service. To address this potentially fatal weakness, Radar Healthcare is hosted via an off-site hosting service through hosting partners Redcentric, who are a market leader in hosting for public and private health and social care organisations in the UK.

All of the Redcentric's managed hosting services are Tier 3 designed, offered from across five UK data centres. These data centres are geographically dispersed, highly secure computing environments with a range of facilities aligned to our business continuity planning:

- 24 hour A/C power, UPS with emergency generator backup, ventilation, air conditioning & computer monitored climate control for heating (HVAC) and fire detection & suppression. It is monitored 24 hours per day, 7 days per week and 365 days per year to ensure that the internet presence is always available

Redcentric's data centres provide multi-layered security and are ISO27001 and ISO9001 certified and accredited with PCI DSS for Physical Hosting Services.

The solution has the following principal benefits:

- System resilience. The off-site solution provides full resilience and accessibility
- Co-location back up. Dual site capability provides full back up even in the event of catastrophic failure of one site
- Data retention. Off-site storage of data provides full data recovery capability

As required, Smartgate can offer a flexible and additional service to allow for external extract and backup of data, where data can be backed up to a customer's online repository and set as part of the system design. Data can also be extracted via the reporting tools as an alternative option.

To further support this requirement, we have developed the following backup strategy in line with recognised industry standards, following best practice principles as below:

- Servers are fully imaged every 24 hours to allow for disaster recovery
- Transaction log backups of the databases are performed every 15 minutes to ensure we minimise the possibility of any data loss. These are kept for 2 days
- Full database backups are performed every 24 hours, we keep the last 7 days, then 4 x weekly rolling backups, and then 6 x monthly backups
- Changes to this frequency can be requested if required
- All backups are stored in a different location to the hosted servers to ensure we have off site backups



Robust penetration testing

The hosting infrastructure is penetration tested by Redcentric on a minimum of an annual basis.

Radar Healthcare is also application penetration tested by a 3rd party at least every 12 months to ensure any application vulnerabilities are detected and resolved. A copy of the reports are available on request.

The Redcentrics penetration test covers the following areas:

- Information gathering including organisation websites, business social networking and technical websites, checked for sensitive information relating to the web application
- DNS zone transfer
- TCP and UDP port scans
- Network vulnerability scanning
- Manual tests for network vulnerabilities
- Web application vulnerability scanning
- OWASP (Open Web Application Security Project)
 - * Manual tests on sample input fields, parameters, cookies for injection attacks, cross-site scripting, cross-site request forgery, insecure direct object reference, cryptographic issues, malicious file execution, information leakage, and improper error handling
 - * Manual tests on sample pages and links for broken authentication, broken session management, failure to restrict URL access, privilege escalation
 - * Insecure communications
- Click-jacking
- Shared web hosting