# Radformation
# IT Specifications and Requirements

## Function

Radformation software increases efficiency in the radiation oncology workflow.

## Description

**QuickCode** is an application that ensures the correctness of charges captured within an Oncology Information System (OIS) for radiation oncology treatments and related services. After reading all the charges for a course of treatment from the OIS, QuickCode uses medical data to verify that each charge is backed by proper documentation and will bring extraneous or absent charges to the user's attention so they can be addressed.

## Install Location

QuickCode may be installed anywhere the locally-hosted or cloud-hosted Oncology Information System's underlying database can be reached via network connection. It is ideal to install QuickCode on the same computer or server as MongoDB. Any available computer or server may be used - a new computer or server is not required. The end user can access QuickCode via a desktop shortcut, Citrix (local IT to publish), or as an External Application (ARIA® users only).

## Hardware Requirements

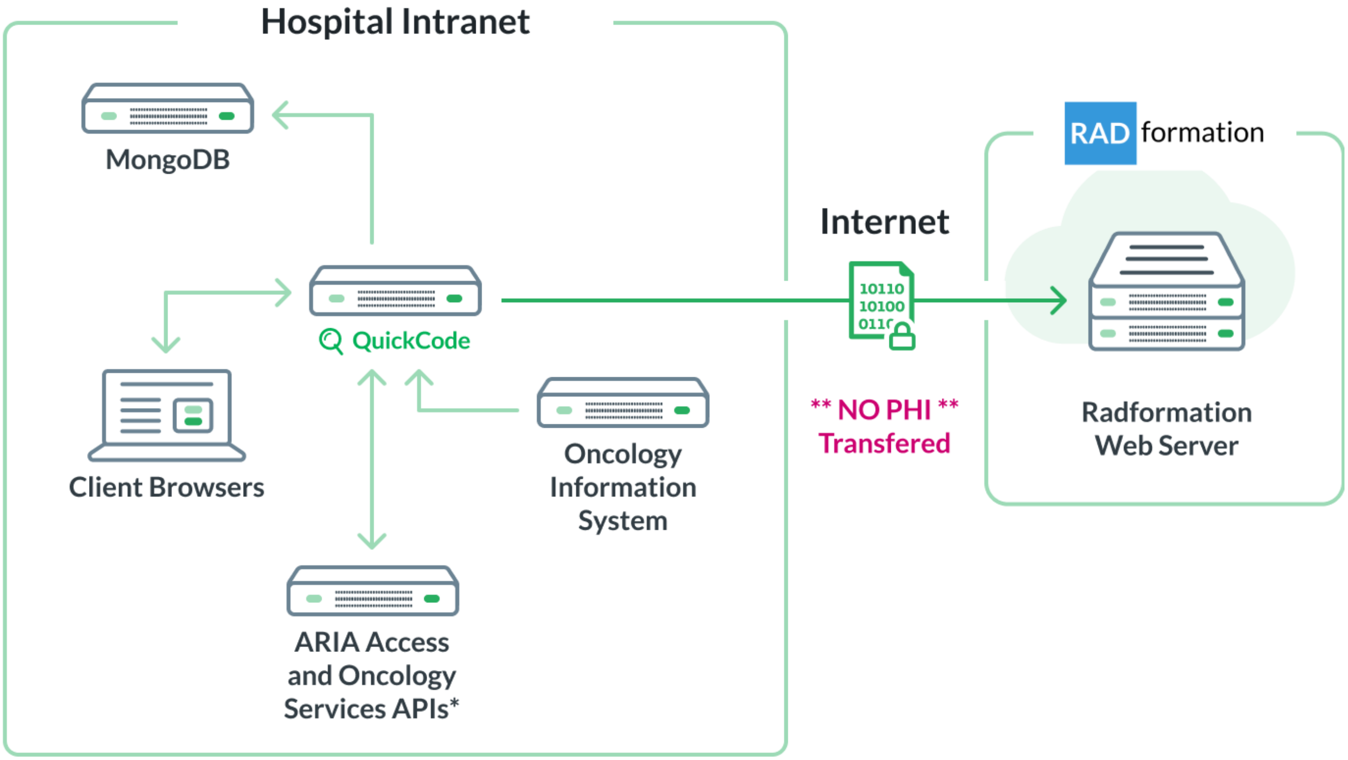
- Operating Systems Supported: Windows 10 (32- or 64-bit), Windows 11 (32- or 64-bit), Windows Server 2016, 2019 and 2022
- CPU: 2.4+ GHz, Multi-core processor (2+ cores, 4+ threads)
- Hard drive space:
  - Software components fully installed require ~3GB, but storage requirements for patient data are much larger and vary from clinic-to-clinic. A minimum of 100 GB hard drive is suggested for larger patient sets.
- Memory (RAM): 16+ GB
- Display Resolution: A minimum of 1280 x 1024, 24- or 32- bit color depth
- Citrix Receiver 4.12 is highly recommended
- .NET 4.5.2 or higher
- Microsoft Visual C++ Redistributable 2015 (or higher)
- MongoDB 6.0 installation is required:
  - MongoDB functionality requires the MongoDB service to be installed and set up on a computer or server that is accessible over the network
  - MongoDB may be installed on an existing, non-vendor computer or server that is accessible widely over the network (a computer or server hosting software from other vendors, except servers hosting SunCHECK®, would also suffice)

## Radformation Software PHI Overview

- No PHI data is transmitted outside of the local hospital network.
- No PHI is stored in any of the Radformation software's encrypted files.
- MRN is used to save folders and file names on the local Network Storage Drive.
- No planning, treatment data, or patient dose constraint related data is sent to the Radformation Web Server.
- Each user has a unique login within the QuickCode application.
- QuickCode has the option to authenticate user login with Active Directory windows credentials. Within QuickCode, admin users are able to create additional users and manage user rights.

## Data Interfaces

QuickCode interfaces directly with the locally-hosted or cloud-hosted Oncology Information System database to read charge, treatment, and medical data.



*For ARIA users only

QuickCode requires one installation per Oncology Information System database. QuickCode is installed on any Network Storage Device (NAS) or file share, with a single NAS supporting one or more QuickCode installations. For any QuickCode installation, the network must be configured such that the environment or machine executing QuickCode can perform a network request to the relevant Oncology Information System database.

User credentials to access the Oncology Information System database can be either a SQL user or an Active Directory user. The database must be accessible either locally or via the network.

When utilizing QuickCode:

- No data is ever written to the OIS database.
- All data retrieved from the OIS databases is encrypted using industry standard algorithms (see **Cyber Security** for details).
- Any data transmitted to Radformation via the Send Patient Data feature is anonymized and encrypted prior to transmission and is used for debugging purposes only.

## Communication Ports

QuickCode communicates over the following ports, including those required for cloud-hosted solutions:

| Purpose | Port | Direction |
|---|---|---|
| Read-only queries to OIS DB | TCP 1433 | QuickCode server to OIS DB server |
| Access to MongoDB | Port 27017 | QuickCode to installation location *(if on a different server)* |
| Access to https://api.radformation.com | Port 443 | QuickCode installation location to Radformation website |
| ARIA Users | | |
| ARIA Access and Oncology Services API | TCP 55051 (ARIA 15+)<br>TCP 56001 (ARIA 13 and prior) | QuickCode server to ARIA Varian Service Portal server |

## Anonymization

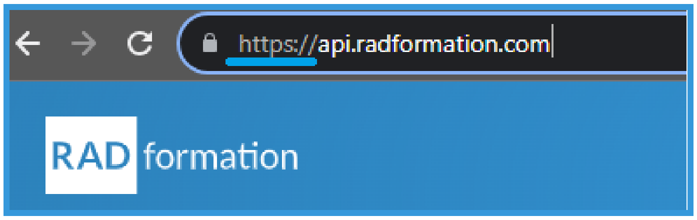
Radformation may occasionally request anonymized data from users to investigate software behavior(s). When providing this data via QuickCode, the transmitted file is fully anonymized and encrypted for use by Radformation Support. The anonymized data is transmitted to the Radformation Web Server. In this manner, no PHI is shared with Radformation as this data is considered to be de-identified per the “Safe Harbor Method” as defined by HHS:

- https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
- Description of included data:
  - Plans
  - Treatments
  - Sessions
  - Charges captured
  - Prescription

**No patient information (PHI) is ever transferred to the Radformation Web Server.**

# Web Server API Communication

The Radformation Web Server uses an API at api.radformation.com. The server Security Patterns follow the Open Web Application Security Project (OWASP) guidelines. The API only connects over SSL/TLS so there is a direct connection between client and server with no opportunity for a Man in the Middle Attack (MITM). Additionally, all webpages only connect over SSL/TLS 1.2+ to ensure that the QuickCode Client connection to the Radformation Web Server is secured.



The **API takes in an authentication key and token ID** that is passed in with the request from the QuickCode client. **Every institution has their own authentication key for QuickCode and these are typically on the order of 45+ characters.**

The steps to access API are as follows:

1. Radformation software first makes a token request to the web server and passes an authentication key to the Radformation Web Server.
2. Radformation Web Server responds with either a “valid” or “invalid” response. If the response is valid, it also passes back a **time-sensitive (60 second) token id to use with the request** (this token is stored on the Radformation Web Server).
3. Radformation software makes the actual request to the Web Server with the authentication key and token id. If more than 60 seconds has passed since it received the token, the request is invalid. If both authentication key and token are valid, then the request is validated.
4. The Radformation Web Server responds with the data that has been requested for validated requests from Radformation software.

All data that is transmitted between Radformation software and the Radformation Web Server is transferred over SSL and is also encrypted inside the request and response body. Encryption uses the Rijndael cypher, also known as Advanced Encryption Standard (AES) which is a NIST standard for encryption. Radformation uses AES-256 bit for encrypting the data. **All data that is stored locally is encrypted with AES-256 bit and all API requests and responses have the body encrypted with AES-256 bit along with the connection being SSL/TLS.**

Authentication for forgotten user passwords, crash reports, metrics reporting, licensing information, and new updates for the Radformation software are done through the API. The license information file is encrypted and sent over the API as *productData.db*, which stores information about:

- Synchronization Date
- Institution Name
- Product Name
- Major Product Version

- Is Product in Trial Mode
- Is Product Active
- Product Active End Date
- Number of Concurrent Users
- License Release Delay
- License Key

**No patient information (PHI) is ever transferred to the Radformation Web Server.**

# Cyber Security

The product was tested for software and cyber security.

Radformation software security testing included:

- All local storage data is encrypted using AES-256 bit encryption. When encrypted at this level, any editing of the files corrupts them.
- Restricted User Access:
  - QuickCode is  accessed as a Standalone executable which may be accessed with a Username and Password control within the QuickCode Administration Application or by Windows Active Directory.
  - The Radformation software Administration Applications are username and password protected.  Passwords are hashed using the Scrypt hashing algorithm. Scrypt is a memory-hard algorithm that makes it difficult to brute-force crack passwords. More information may be found here: https://www.tarsnap.com/scrypt/scrypt.pdf. The below is Table 1 (page 14) taken from this text.

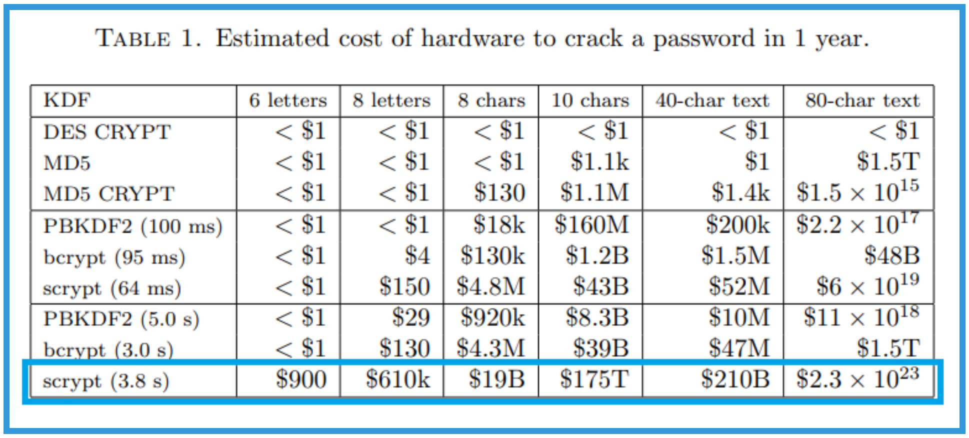


TABLE 1. Estimated cost of hardware to crack a password in 1 year.

| KDF | 6 letters | 8 letters | 8 chars | 10 chars | 40-char text | 80-char text |
|---|---|---|---|---|---|---|
| DES CRYPT | < \$1 | < \$1 | < \$1 | < \$1 | < \$1 | < \$1 |
| MD5 | < \$1 | < \$1 | < \$1 | \$1.1k | \$1 | \$1.5T |
| MD5 CRYPT | < \$1 | < \$1 | \$130 | \$1.1M | \$1.4k | $\$1.5 \times 10^{15}$ |
| PBKDF2 (100 ms) | < \$1 | < \$1 | \$18k | \$160M | \$200k | $\$2.2 \times 10^{17}$ |
| bcrypt (95 ms) | < \$1 | \$4 | \$130k | \$1.2B | \$1.5M | \$48B |
| scrypt (64 ms) | < \$1 | \$150 | \$4.8M | \$43B | \$52M | $\$6 \times 10^{19}$ |
| PBKDF2 (5.0 s) | < \$1 | \$29 | \$920k | \$8.3B | \$10M | $\$11 \times 10^{18}$ |
| bcrypt (3.0 s) | < \$1 | \$130 | \$4.3M | \$39B | \$47M | \$1.5T |
| scrypt (3.8 s) | \$900 | \$610k | \$19B | \$175T | \$210B | $\$2.3 \times 10^{23}$ |

- Radformation software API establishes a direct tunnel between the client and the Radformation web server using SSL. All data is encrypted in transit and requires dual authentication via 40+ character QuickCode private key and a 60 second time sensitive token. Without these, the Radformation web server returns an unauthorized response and will not transmit data.

Beyond the QuickCode application, the Radformation website has been securely built following OWASP guidelines: https://owasp.org/www-project-top-ten/.

- The Radformation website is username and password protected. All passwords are hashed with the Scrypt hashing algorithm, as discussed above.
- All pages are served over SSL/TLS to prevent MITM attacks.
- All Database queries are internal so SQL injection attacks are not possible.
- Auth cookies are set to HTTP and Secure so cookie values are unable to be read or edited.
- Cross Site Request Forgery is prevented by having a specific xsrf token.
- Cross Site Scripting is prevented by sanitizing all input data.

**Questions? Need assistance?**

Contact Radformation Support at support@radformation.com or 1-844-RADFOR5