Quokka

WHITEPAPER

Mobile App Security

And Privacy Transformational Assessment and Validation

Mobile App Security and Privacy Transformational Assessment and Validation

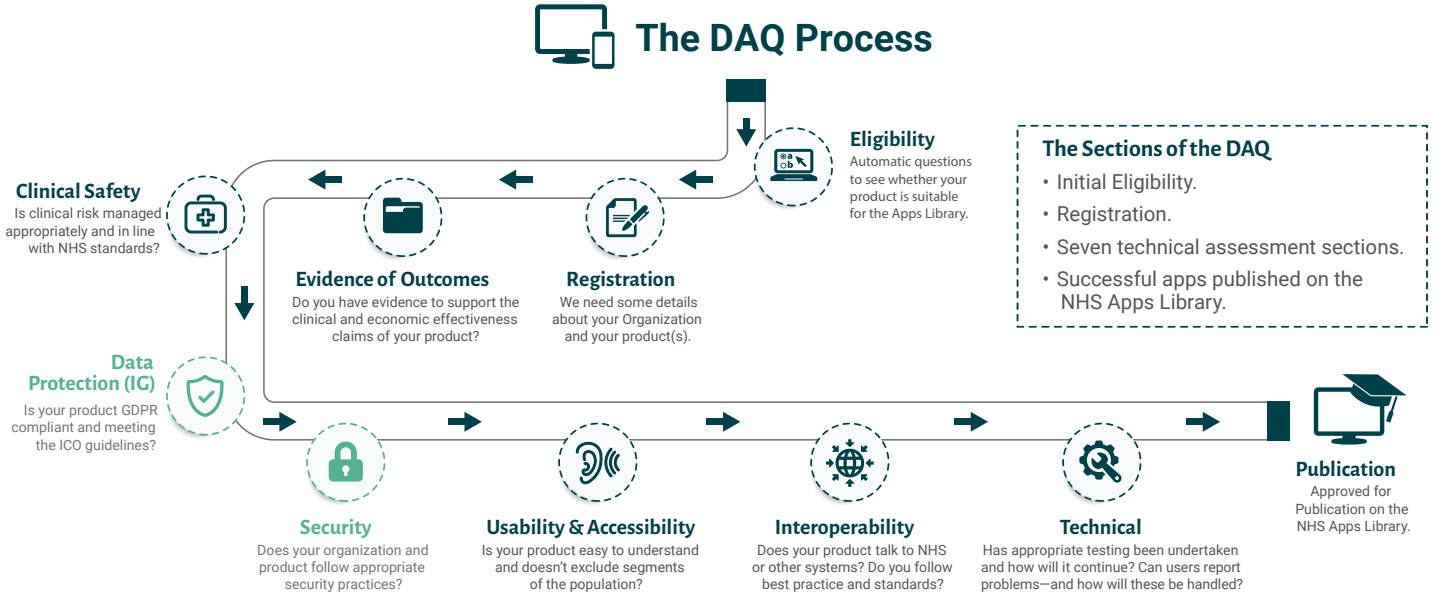
NHS Apps Library: An Overview

There are well over 300,000 mhealth apps available to download from a myriad of sources. The quality of these apps varies considerably. NHS Apps Libraries deliver a valuable service to citizens, patients, and health and social care professionals. The NHS Digital (NHSD) Apps Library (The Library) provides access to trusted digital tools, improving health and well-being outcomes by supporting people who take an active role in managing their own mental and physical health.

Assessing the Security and Privacy of Mobile Applications

The products on The Library were assessed to be clinically safe and secure to use, with products having met standards sourced by the NHS, including evidence of clinical safety, security, and technical stability.

The Library developed the Digital Assessment Process (DAP), which included the Digital Assessment Questionnaire (DAQ). The DAQ required Developers to answer questions relating to their apps' clinical, security and technical stability elements. The more complex the app, the more complex the question set. The completed DAQs were then assessed by The Library team and associated personnel, including a clinical panel to assess the clinical merits of an app, complemented by security and technical stability personnel dependent on resource availability, app complexity and findings; the length of the process varied considerably.



The Library looked to continually improve the DAP whilst maintaining its quality and integrity and reducing the time and cost of getting apps published into the Library and available to the public, clinicians and staff. An area of significant concern was App Security and Privacy.

The Library team considered procuring the services of several companies that could provide app security and privacy assessment services. However, the approach would have required significant management, with the variability of results being problematic. Furthermore, the time and costs associated with the approach were considerable.

The Library team was open to considering innovations to improve the situation.

Quokka: Automated Mobile Application Security

Testing

Quokka, formerly Kryptowire, was jump-started in 2011 by the US Defense Advanced Research Projects Agency (DARPA), the US Department for Homeland Security, Science and Technology (DHS S&T) and the US National Institute for Standards and Technology (NIST) and has become a leader in the field of automated Mobile Application Security Testing (MAST).

Quokka has developed a proven, cloud-based solution which has automated the assessment of mobile apps by comparing them against stringent standards, including NIAP, OWASP and GDPR, providing an auditable baseline and delivering actionable results in less than 2 hours.

Standards-Based, Automated, Validated

Quokka became a key component of the DAP. The Library Team downloaded candidate iOS or Android apps for analysis from the relevant app store or submitted the app code directly into the portal. Quokka compared the code against the standards, utilizing Static Analysis, Dynamic Analysis, Behavioral Analysis, Forced Path Execution, and other proprietary functions. This combination delivers comprehensive, auditable, and repeatable results.

36 Minutes: Average Time Taken to Deliver the Results to NHS App Library

A dashboard provides high-risk results to help triage activity. Detailed results provide evidence, including issue location, impact, links to relevant standards, and remediation advice. Depending on the results, the Library Team marked the app as ready for publishing (subject to the clinical and technical stability assessments) or engaged with the developer to discuss any findings and, if appropriate, have issues rectified. The app was then reassessed.

On a daily basis, Quokka's watchlist facility automatically scanned the app stores to look for updates to the published apps. The results were provided in the portal in case the update materially altered the assessment.

2-25 Per App: Range of Updates Over 6-Month Period

Quokka was also used by NHS Digital and interested parties to obtain an indication of potential issues relating to Covid 19 apps. Quokka informed the relevant NHS Track and Trace app development processes.

High-level observations regarding the security and privacy of considered apps included:

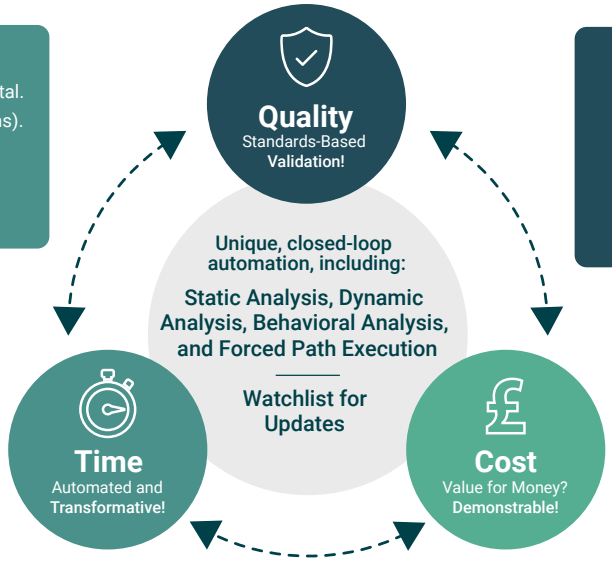
- There were some well-designed apps.
- DAQ needs refining (e.g., iOS and Android apps needed validating separately as results differed).
- App validation is essential. Many of the DAQ submissions were inaccurate, possibly through oversight or lack of secure design knowledge. Only reviewing DAQ submissions could be argued as inadequate and a potential risk to the users of the apps, the NHS Library brand, and trust in The Library's apps.

Quokka Benefits

In addition to improving the quality of the security and privacy of The Library's apps, Quokka's standards-based, automation, auditability, repeatability, watchlist function, and comprehensive output, saved the NHS considerable cost in both time and money. Meeting this need through manual means would have taken much longer, lengthening the process considerably with extensive, knock-on resource costs.

Transformational Process

- Analyst uploads into web-based portal.
- Results in < 2 hours (average 40 mins).
- Reviewed against company risk appetite/policy.
- App published or pushed back for rectification.



Regulatory Quality

- Compared to stringent standards.
  - NIAP, HIPAA, OWASP, GDPR
- Comprehensive reporting, portal interaction auditable, repeatable.
- Improves analyst decision making.

Considerable
Time and Cost reduction!

Standards-Based, Auditable, Repeatable, Rapid Results

- **DAQ Submission Validation:** Demonstrated to be essential.
- **App Confidence:** Baselined against standards, with less variability of output.
- **Developer Engagement:** More effective.
- **Focus:** Validation speed enables the team to focus on things, such as clinical aspects.

Sustainable Confidence and Rapid Re-assessment

- **Dealing with Updates:** In a 6-month period, one app had 25 reassessments due to app changes; many apps had 10+ reassessments.
  - Using Kryptowire demonstrated that continuous review is essential and that only reviewing apps upfront is ineffective.
- **Watchlist:** More time and cost-effective monitoring and reassessment than by other means.
  - We demonstrated that the watchlist is essential.
  - Can be utilised as an alert for changes to other elements of the app (e.g., clinical/technical).

Capability Enhancement

- **NHS:** Library team's Kryptowire utilisation, developer engagement, plus reach back to Kryptowire experts was very informative and beneficial.
- **Developers:** Improved app and developer knowledge from going through the process with wider than NHS benefits for the company.
- **Secure by Design:** Developers get to know what "good" looks like.

Key Points Summary

The Library team and Quokka's collaboration on the security and privacy of mobile apps demonstrated:

App Validation: Essential. Relying on documentation review alone does not provide sufficient confidence.

Standards-Based Reporting: Improves quality. Enables a sound baseline to develop and assess against.

Continuous Review of Updates: Essential.

Quokka Automation: Transformational.

- Speed and quality of results. Enables increased app throughput.
- Drive Efficiencies. Enables Doing More with Less.
- Facilitates Considerable Resource and Cost Reductions.
- Puts focus on assessment of an app's clinical and technical stability merits.

The collaboration not only proved the concept of automating the vast majority of the DAP security and privacy activities, but it has additionally proved exceptional value and delivered demonstrable benefits.

> The NHS Digital Apps Library team and Quokka, formerly Kryptowire, enhanced and transformed the security and privacy aspects of the NHS Digital Apps Library processes. The collaboration demonstrated the need for validation and the automation improved the time and cost effectiveness of the processes, resulting in better quality and increased trust in the Library's mHealth apps.
>
> ***Wayne Shirt, Operational Lead, NHS Apps & Wearable Programme***

Quokka