

Integrated Research
9/100 Pacific Highway
North Sydney
NSW 2060

18th May 2018

To Whom It May Concern,

NCC Group were engaged by Integrated Research to perform a data protection impact assessment of its Prognosis on premises application, to seek assurance that its components meet the requirements of the EU General Data Protection Regulation (GDPR), which takes effect on 25 May 2018. The engagement ran from 18th April to present.

Integrated Research see that ensuring the privacy and security of its customer and employee's personal data is a priority and to enhance its existing arrangements have commenced a programme of work using both internal and external resources.

As part of its GDPR programme, a data protection impact assessment was carried out by its partner, NCC Group, a company that specialises in privacy and cyber security. NCC Group assessed how the Integrated Research Prognosis on premises application is currently configured to meet the requirements of the GDPR and specifically to identify any privacy-related risks and their solutions to reduce those risks to an acceptable level so that the personal data of clients and employee data is appropriately protected.

The data protection impact assessment found that whilst the Prognosis application is "out of the box" configured to meet the requirements of the GDPR, Integrated Research customers will need to ensure that their configuration is reviewed if different. In particular the following recommended standard configuration settings and relevant features include:

- **Data purging and retention:**

Storage Area	Duration
Prognosis database	14 days
SfB (PostgreSQL)	14 days
Reporting SQL Database	180 days
CRA (PostgreSQL)	7 years

- **Access control:**

- No Security – Allow all access.
- Low Security – Domain users cannot alter security settings.
- Medium Security – Domain users cannot alter configurations or start analysis.
- High Security – Domain users cannot start or stop thresholds, databases, etc.
- Maximum Security – Only the user that installed Prognosis can manage it.

- **Encryption of data** in transit is available, using AES256-CFB-HMAC or for legacy systems, AES256-CTR-SHA256 encryption algorithms, where operations are compliant to FIPS 140-2.

- **Default communication components are configured** to operate in accordance with FIPS140-2.

NCC Group +61(0)295524451
Level 13, 92 Pitt Street apac@nccgroup.trust
Sydney NSW 2000 www.nccgroup.trust
Australia



CONFIDENTIAL


- **Windows Client** – irgui.exe. The Prognosis Windows Client will always attempt to communicate with the Prognosis Server using the FIPS certified encryption algorithm AES256-CFB-HMAC). If FIP's has not been enabled, the connection will not be successful, and the window client will lower the encryption to the non-FIP's encryption algorithm (AES256-CTR-SHA256).
- **Password Configuration** – Passwords will always be encrypted with FIP's compliant encryption algorithm.
- **PACE XML** – Pace XML files will always be encrypted with FIP's compliant encryption algorithm.

The findings of NCC Group do not guarantee that other vulnerabilities may not be present given the specific scope and time investment. Further, NCC Group carried out the testing for Integrated Research and its customers and accepts no liability to any other party that relies on the above findings.

About NCC Group

NCC Group is an ISO9001 and ISO27001-certified organisation with over 2,000 employees and 35 offices globally. We are specialists in the provision of end-to-end professional and managed cyber security and privacy services.

Yours sincerely,



Julian Davies
Head of Asia Pacific

NCC Group
Level 13, 92 Pitt Street
Sydney NSW 2000
Australia

+61(0)295524451
apac@nccgroup.trust
www.nccgroup.trust

