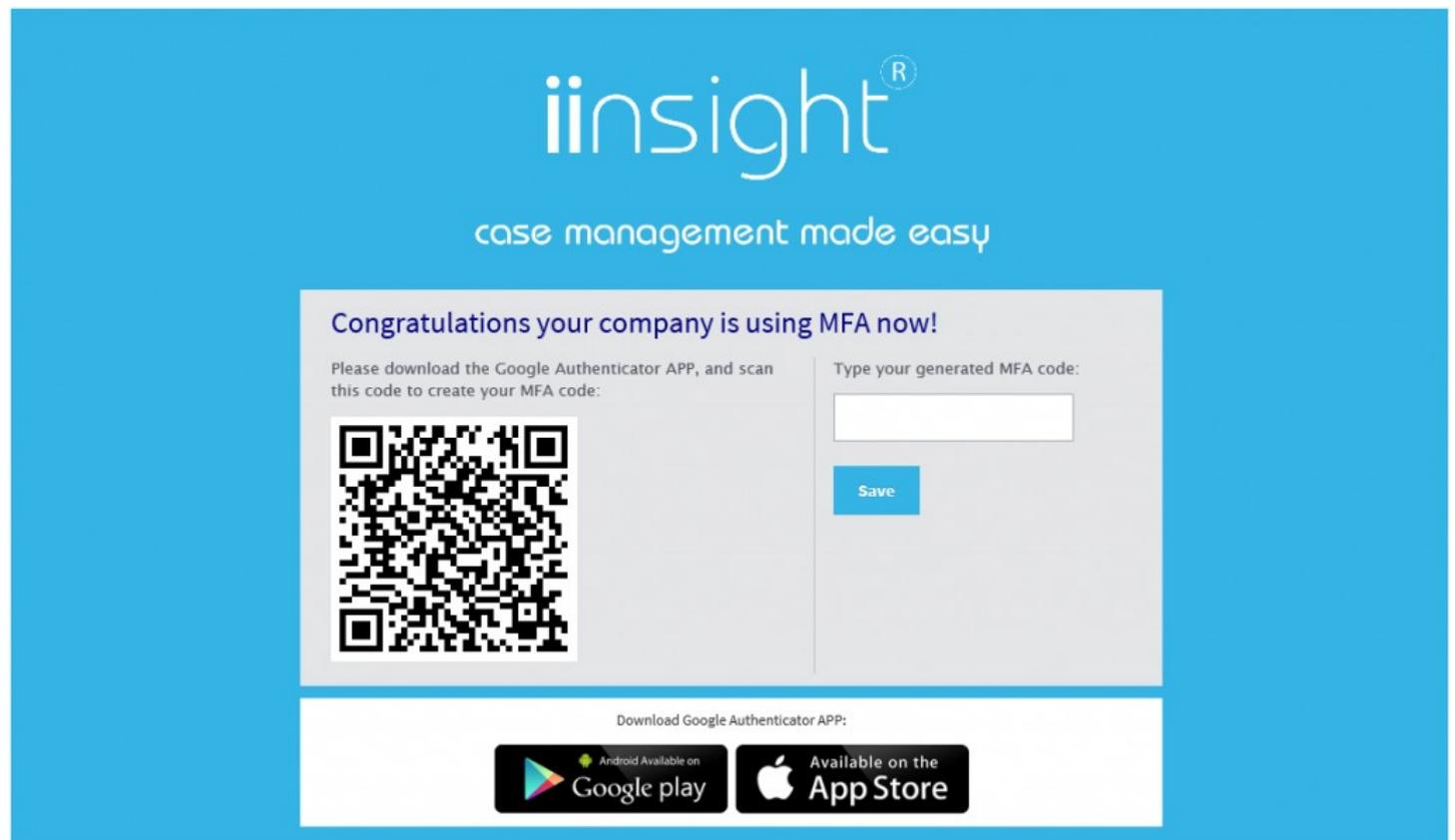


## Be Software Releases Version 6.2.9 of IINSIGHT

Be Software added a new feature Multi-Factor Authentication (MFA) in their latest Version 6.2.9 of IINSIGHT the leading injury case management software.



**Sydney, Mar 4, 2019** ([Issuewire.com](http://Issuewire.com)) - Before they advise more details of this amazing iinsight solution (further below) it is reassuring to know how iinsight is already helping their client to comply with GDPR (EU) and Privacy Amendment Act 2017 (AUS) and prevention of data breaches will be further enforced when using Multi-Factor Authentication (MFA):

Data breach – How iinsight® helps comply with GDPR (EU) and Privacy Amendment Act 2017 (AUS)

There are a global reinforcement and accountability on organizations data protection obligations which have included European Union and Australia updating their legislations respectively, GDPR and Privacy Amendment Act 2017, is to include an obligation on companies to notify individuals and governing authorities when personal information involved in a data breach is likely to result in serious harm.

Prevention is the Key

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Today, simple use of passwords, tokens, or biometrics is not enough to prevent unauthorized access. Instead, Multi-Factor Authentication (MFA) is one of the most effective controls an organization can implement to prevent an adversary from gaining access to a device or network and accessing sensitive

information, therefore its implementation is recommended by ACSC (the Australian Cyber Security Centre) and ENISA (the European Union Agency for Network and Information Security).

To help organizations comply with the new legislation, focus on strong privacy governance and encourage good practice, iinsight® (<http://www.iinsight.biz/>) will now be supporting Multi-Factor Authentication (MFA). This will help your organization prevent issues, such as health records been stolen or compromised, due to users sharing passwords, having predictable passwords etc.

The transition from a single password to MFA will be done in 2 steps to enable organizations to update their Access Control Policies and Procedures accordingly.

iinsight® Solution: MFA – via Google Authenticator App

This multi-factor authentication method uses a time-limited one-time 6-digit PIN provided via the Google Authenticator mobile app as a second authentication factor. When the users enrol, they scan a QR code so that a one-time PIN can be provided to them after registering their mobile phone with the iinsight application.

During the logon process, the google authenticator app provides the users with a one-time 6-digit PIN in order to complete the authentication process. The users then provide this information to the iinsight login service, which verifies the credentials of that user and grants or denies access to the iinsight resources. The expiry time of the one-time PIN generated via the google authenticator app is set to renew every 60 seconds.

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) - For more information, see [www.oaic.gov.au/ndb](http://www.oaic.gov.au/ndb)

GDPR Art 33 Data Breaches - For more information, see <https://gdpr-info.eu/art-33-gdpr/>

They would like their clients to jump on board and take advantage of this higher level of security and start using MFA. This will also help them to be familiar with this method before at some point (yet to be announced) this authentication method will be mandatory.

Read IINSIGHT 6.2.9 Release Notes to enable MFA for your organization - <https://injurymanagementsoftware.wordpress.com/2019/02/25/iinsight-6-2-9-release-notes/>

## Media Contact

Cathy Zhang

[info@iinsight.biz](mailto:info@iinsight.biz)

Source : Be Software International Pty Ltd

See on IssueWire : <https://www.issuewire.com/be-software-releases-version-629-of-iinsight-1627146414878870>