



Resources for Human Development (RHD)

Supporting personally owned devices brings flexible, hassle-free compliance



Resources for Human Development (RHD) is a Philadelphia-based not-for-profit social services organization that serves tens of thousands of people with intellectual and developmental disabilities, behavioral health and addiction problems. Many of their 4,600 employees spend their time in the field helping clients or scattered among multiple RHD offices and across 14 states.

The BlackBerry solution in place at RHD was great for IT, but users now wanted to switch to iOS, Android and Windows devices. Employees in greater and greater numbers wanted to use their personally owned devices to access corporate email, calendar, contacts and more.

RHD's Chief Technology Officer Endre Walls knew how important it was to the employees to have access to email at all times and in all places. RHD had rarely used laptops for mobile employees. Smartphones (and now tablets) served them better, and they wanted to use their own devices, ones they knew and were comfortable with.

Endre had already created a compliance initiative for computers, requiring employees to meet corporate standards for data security. He considered smartphones and tablets to be the same

CUSTOMER:

Resources for Human Development (RHD)

INDUSTRY:

Healthcare

LOCATION:

Philadelphia, PA

CHALLENGE:

Protecting sensitive patient data on tablets and smartphones which are employee-owned in addition to corporate owned devices while ensuring compliance with HIPAA regulations.

SOLUTION:

MaaS360 by Fiberlink provides centralized policy management and control for iOS, Android, BlackBerry, and other next generation devices in a rapidly deployable cloud-based model.

RESULTS:

RHD currently manages over 140 devices; most of them are employee-owned. RHD has received immediate ROI and peace of mind with MaaS360 in utilizing the remote device wipe capabilities twice within the first two months of deployment.

Resources for Human Development (RHD)

“*This ability to take immediate action and avert data breaches is an invaluable asset to our organization.*

- Endre Walls, Chief Technology
Office, Resources for Human Development

as computers, and he wanted IT to create a safe infrastructure for them, too.

IT staff sought a solution that would provide the tools they needed to protect the organization and its data from potential risks.

The Challenge: Support Personally-Owned Devices

Some of the key considerations were that the solution had to be flexible, allowing IT to support over 160 RHD programs. It needed to be able to enforce RHD’s corporate acceptable-use policies on employees’ personal mobile devices as well as any corporately owned devices. They needed a solution that wouldn’t increase spend—i.e., require hiring additional staff and building infrastructure. It also had to protect sensitive medical and personal information on mobile devices in compliance with HIPAA regulations.

The Solution: Enabling BYOD with MaaS360

RHD implemented a “Bring Your Own Device” (BYOD) strategy using the MaaS360 Platform. It provides the compliance management and control that RHD wanted while enabling the employees to make their own device choices.

This mobile device management solution enforces RHD’s acceptable-use policies and helps secure corporate and client data. Any employee who wants to access RHD’s corporate network or email from his or her personal mobile device must enroll in the “Bring Your Own Device” initiative. When employee devices become enrolled, IT automatically implements a security policy on the device that forces the employee to create a passcode or PIN. Then it will automatically supply access to the correct corporate Wi-Fi network.

In addition, IT staff can easily identify personal devices that try to access the corporate network but aren’t enrolled under management. They then reach out to those device owners with information on how to enroll in the Bring Your Own Device initiative. This information can also be triggered automatically from the MaaS360 Platform.

RHD has received zero pushback from users who need to enroll in the MDM solution and are thrilled about the policy and the level of support RHD is able to provide them.

The Benefit: Flexible, Hassle-Free Compliance

With MaaS360, RHD has a robust reporting environment to show which devices are out of compliance, along with details as to why the device is considered out of compliance. Reasons often include not having a PIN or passcode on the device, or using unsupported data sharing software. Devices that don’t comply can be immediately and automatically blocked from accessing corporate resources using MaaS360 compliance engine rules.

All brands and their products, featured or referred to within this document, are trademarks or registered trademarks of their respective holders and should be noted as such.

For More Information

To learn more about our technology and services visit www.maaS360.com.
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
Phone 215.664.1600 | Fax 215.664.1601 | sales@fiberlink.com