



The Royal Marsden **NHS**  
NHS Foundation Trust

## IronKey Stands Shoulder to Shoulder with The Royal Marsden to Secure Data

“ We chose the IronKey solution as it is AES standard hardware encryption which can't be circumvented. The central policy management was another key criteria combined with the managed service ...that we could disable a device if missing in action, and that it would self-destruct following a set number of failed login attempts was another strong selling point. ”

**Jon Reed**, IT Director  
*The Royal Marsden*



**Healthcare  
Success Story**

Jon Reed chose the IronKey as the best solution for The Royal Marsden which would not cause a problem amongst other trusts accepting it.

The Royal Marsden is a National Health Service (NHS) Foundation Trust in England that specialises in cancer. Situated primarily over two main sites, one in Chelsea and one in Sutton, it also has a number of satellite locations—an area of the business that is being developed. Today, it has a staff of approximately 2,500 all of whom, in one form or another, are responsible for protecting the data they access.

The Royal Marsden is committed to promoting excellence in cancer research, treatment and education. Alongside its academic partner, the Institute of Cancer Research, it is considered one of the leaders, and at the forefront of many major cancer breakthroughs.

The NHS Trust is involved in tackling and taking data breaches very seriously. At the helm is Jon Reed, IT Director for The Royal Marsden, who is responsible for its entire IT infrastructure and the development of all in house clinical applications.

### **The Story So Far...**

According to Jon, "The Trust takes the handling of information very seriously, which is what you would expect of an organisation of our standing, and my defence strategy to protect data in transit began many years ago, back in 2006, long before publicised breaches by public bodies."

Following the high-profile cases, a central policy was introduced by David Nicholson, CBE, NHS Chief Executive stating that every organisation within the NHS must fully implement the policy that all removable data must be encrypted, and also follow the recommendations of the report of the Cabinet Office Data Handling Review, which contains mandatory security standards for the public sector. As The Royal Marsden had already begun researching various solutions it was ahead of the game.

The Royal Marsden encourages its staff to not carry data unless it is absolutely necessary. It recognises that on occasion, patient identifiable records, staff information and commercially sensitive information such as research projects and data, amongst other documents, will be transported and shared and this must be done in a secure manner.

### **And the Solution of Choice Is...**

The Royal Marsden quickly honed in on about six offerings, and it looked to see what other NHS Trusts were doing. One of The Royal Marsden's key concerns had been that organisations would lock down their infrastructure and would only allow certain models of USB devices to be used. This was Jon's thinking, too—the Trust didn't want to run into a compatibility problems. Jon made a decision ahead of the game, and chose the IronKey as the best solution for The Royal Marsden which would not cause a problem amongst other trusts accepting it.

As knowledge of the security programme and policy on the use of USB devices filtered through the organisation, users proactively requested devices, driving their demand and adoption.

Jon clarifies his reasoning, “We chose the IronKey solution as it is AES standard hardware encryption which can’t be circumvented, which then puts the onus on the user to make the decision. The central policy management combined with the managed service was another key criteria, so we don’t have to worry about deploying server infrastructure on our network and applications to manage the devices. The fact that we could disable a device if missing in action, and that it would self-destruct following a set number of failed login attempts was another strong selling point. IronKey’s onboard digital certification for RSA to consolidate encrypted mobile storage—and strong two-factor authentication in a single device—fitted with what we wanted to do around making it easier to connect to our infrastructure securely from remote locations.

Finally, the aesthetics of the device played a part, as it looks credible and from an infection control point of view, it is a waterproof device with a rubberised cap so it can be disinfected—essential for a healthcare institution that prides itself on the standards it sets across the NHS.”

Once the decision had been made and the devices purchased, The Royal Marsden had a two-fold challenge: getting staff to think differently about security and getting staff to remember to use the devices.

Jon explains, “Planning is important with the implementation of any system. Don’t think of IronKey as a straight replacement to your existing insecure USB devices that you buy off the shelf like blank CDs. It’s a key part of your security infrastructure and so you need to think of it as part of your security strategy, and plan how you’re going to deploy it.”

### **We Told Everyone ...**

The Royal Marsden thinks as a whole about information security and has a structured communications campaign to ensure information security across the organisation.

It introduced a policy that specifically covered the transfer of any data to a USB device. To avoid any ambiguity, it decided to not make a distinction between sensitive and indifferent data—it classes all data equally (when being transferred from the Trust’s PCs) —taking the dilemma away from its staff. The Trust’s policy states it must be on an IronKey.

It ran a number of specific communication campaigns to encourage awareness of new policies, and the introduction of IronKeys, which included: top-down management briefings; it sent out leaflets with payslips; and targeted emails for key individuals.

### **We Led from the Front ...**

The next approach employed by The Royal Marsden to reduce potential negativity was the tactical deployment of a few initial devices to selected key users. This secured general acceptance within the organisation, prior to critical mass roll out, which it believes has removed resistance to the devices. As knowledge of the security programme and policy on the use of USB devices filtered through the organisation, users proactively requested devices, driving their demand and adoption.

“The technology has been made quite simple to use.”

The Royal Marsden found the deployment to be quite straight forward with only a few minor difficulties—as it familiarised itself with the technology—which were from an operational standpoint rather than the end users experience. Jon explains, “There have been no real problems with the product itself. The technology has been made quite simple to use, but having a strong password protection on USB devices was alien to our users—which they initially struggled with—and which have been down to our zero tolerance policy rather than caused by IronKey.”

Prior to IronKey's deployment, The Royal Marsden had another solution for remote access and found the integration seamless, creating a more flexible easy to use solution for its staff. As the RSA token facilitates secure access to the infrastructure, users have just one device—which is also their security device—making it easier for them to use it.

When asked for any other advice Jon could offer, he said, “Tackle any areas of weakness on a risk priority basis. You need to think of your whole infrastructure and the way that users handle information right through from careless conversations in the canteen that might be overheard through to moving personal information around on USB devices to confidential faxes being left lying around. Introducing technology to combat a problem is just one part of a programme on information security.”

“You have the peace of mind that if one drive should end up in the wrong hands, after a few attempts at access it will be permanently inaccessible, which is a strong feature.”

### **The Future with IronKey ...**

Since introducing IronKey some devices have gone missing in action but The Royal Marsden has simply disabled them centrally. Tongue in cheek, Jon says “It doesn't quite self-destruct but very close to it! You have the peace of mind that if one drive should end up in the wrong hands after a few attempts at access it will be permanently inaccessible, which is a strong feature. In terms of what central policy requires us to do—it has certainly met that, and I would go as far to say that it's better than what some others are using.”

Going forward The Royal Marsden is quite excited by the opportunities IronKey offers in terms of taking remote access a step further. It has a vision of giving employees a virtual machine that's run from their IronKey. This will enable staff to work from anywhere securely, thereby controlling how the Trust's infrastructure is accessed and where data is stored—either on the network or an IronKey—with obvious saving implications. It has just started to examine this, and has taken some soundings from its key users, with the possibility of rolling it out early in early 2010, if everything goes to plan.

Jon sums it up when he concludes, “If the unthinkable happened, and our data was breached, personally I would be devastated, by both the reputational damage and the shattered trust of the individuals involved. As I have got the responsibility of sourcing and purchasing a solution, I'm not going to settle to meet the bare minimum Government standards; I'm going to invest in the strongest solution that I possibly can.”

## About The Royal Marsden

The Royal Marsden Hospital was the first hospital in the world dedicated to cancer treatment and research into the causes of cancer. Today the hospital with its academic partner, The Institute of Cancer Research, forms the largest comprehensive cancer centre in Europe with over 40,000 patients from the UK and abroad seen each year.

The Royal Marsden NHS Foundation Trust is ranked as one of the top NHS trusts in the UK in the NHS national performance rankings. In October 2008, The Healthcare Commission's Annual Health Check showed that The Royal Marsden received the highest score of 'excellent' for both quality of services and use of its resources for the third year in a row.

The Trust provides inpatient, day care and outpatient services for all areas of cancer treatment. The Trust pioneers and innovates in all areas of cancer treatment. It is a leader in its field, striving for excellence. Its unique relationship with The Institute of Cancer Research assists the development of new treatments and brings benefits to patients as quickly as possible.

## About IronKey

IronKey, based in Los Altos, California, was founded in 2005. The security specialist develops solutions around the topics of authentication, encryption, data protection and identity management. IronKey's USB flash drives are used by customers in 23 countries. Amongst these are many Fortune 500 companies. All products are validated in accordance with the US security standard FIPS 140-2, Level 3 and comply therefore with the highest security standards.

THE WORLD'S MOST SECURE MANAGED FLASH DRIVE



www.ironkey.com sales@ironkey.com  
5150 El Camino Real, Suite C31, Los Altos, CA 94022 USA  
Toll-Free 866 645 9847 Federal Hotline 888 351 4698  
T 650 492 4055 F 650 967 4650

