Reconnecting to networks:

A number of organisations have taken the precaution to disconnect their infrastructure from internet gateways, including the Transition Network (formerly N3). There is no evidence to suggest that this will help limit the propagation of any infection, and can cut off access to clinical systems. Since the propagation of the malware has reduced dramatically in recent hours, here is some guidance for organisations to reconnect network connectivity in the safest possible way:

- Block SMB related ports (UDP 137, 138 and TCP 139, 445) across the network https://support.microsoft.com/en-us/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic-from-leaving-the-corporate-environment

- Ensure all affected platforms are updated in line with the Microsoft security bulletin MS17-010 https://technet.microsoft.com/en-us/library/security/ms17-010.aspx (internet facing systems should be prioritised). It should be noted that Microsoft have released patches against this particular vulnerability for unsupported platforms such as Windows XP and Server 2003.

- Confirm with your Anti Virus (AV) provider that they have rolled out virus definition to protect you from the spread of this malware and the MS17-010 vulnerability.

- Update all AV software with the latest definitions that include this patch.

- Unblock SMB related ports (UDP 137, 138 and TCP 139, 445) across the network on fully patched systems only.