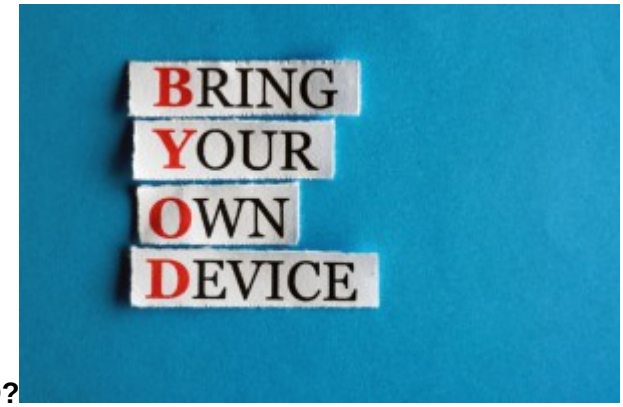
HIPAA “BYOD” Rule Changes: What You Need to Know

What is BYOD? 

BYOD (Bring Your Own Device) appears to be a win-win for companies andemployees: employers save money on smart phone, tablet and laptop costs and employees enjoy the freedom of choosing their own device while enhancing communications and mobile care collaboration. **BYOD in the Medical Industry** However, in the medical industry, BYOD raises HITECH and HIPAA concerns such as:

- Accessing and storing hospital and patient information
- Regulatory compliance
- Employee privacy concerns
- Encrypting data where necessary
- Social media policy issues
- Multi-platform integration of key software applications
- How to manage usage charges

3 Challenges You’ll Face with the HIPAA Security Rule The myriad of complex risks can be simplified into 3 challenges:

1. **Control**. BYOD forces health care organizations to give up the control they’re used to having with company-issued devices. BYOD leads to numerous devices, operating systems and levels of? configuration which all lead to security complexities. To further complicate matters, employees using their own device expect the option of BYOA (apps) and BYOC (cloud).
2. **Compliance**. BYOD complicates and opens your ecosystem and makes it much harder to stay in compliance with the guidelines regulated by HITECH and HIPAA.
3. **Privacy**. Privacy is a human issue. Employees bringing their own devices feel like they should be able to control the information on those devices, but this can cause issues should litigation arise or if the employee loses the device and the company policy requires a remote wiping of all data.

What You Can Do About It: Create a BYOD Policy (and Enforce It) It’s obvious the benefits and myriad of risks that come from a BYOD workforce, so here’s what you can do to make the most of it and stay compliant.

1. **Define who can participate**. It might make sense to only allow certain employees to BYOD,

depending on the level of access to secure data.

2. **Limit the devices that qualify**. Consider designating certain products as part of your BYOD program to cut down on the number of devices and operating systems your IT team needs to learn to manage and regulate.
3. **Get consent from employees**. This is a relevant and complex issue as the company doesn't own the device or the account, but access may still be necessary during discovery processes.
4. **Outline security requirements**. Consider implementing an MDM (mobile device management) tool to handle encryption keys, increase strength of user passwords and enable remote wiping for misplaced devices.
5. **Outline steps when employees leave the company**. Your exit process must include ways to remove company data from departing employee's devices. Make sure you consider how contacts will be handled as the line between personal and professional contacts can blur.
6. **Clearly outline reimbursement policies**. Check into local employment and data protection laws to ensure your device compensation guidelines are compliant.

Consult with the Experts Setting policies that mitigate non-compliance risk include IT restrictions, technical safeguards and more. After outlining your BYOD policy, it's recommended to have your legal team review the process to ensure it's compliant with both HITECH and HIPAA. The health care attorneys at Seigfreid Bingham are experienced and up-to-date and can guide you through the process. Image: Thinkstock/ivosar *This article is very general in nature and does not constitute legal advice. Readers with legal questions should consult with an attorney prior to making any legal decisions.