Secure
point of care.

**Challenge**
- There are too many touch points that create risk when it comes to sharing PHI inside and outside of the hospital
- Hospitals today need a solution that automatically provides security and control both at the smart MFD where patient information is shared and distributed and in the use of mobile computing technologies

**Solution**
- Nuance—securing health information at the point of care

**Results**
- Helps hospitals protect patient health information as part of achieving HIPAA-compliant use of PHI at the point of care
- Minimizes the manual work and decisions that invite human error
- Mitigates the risk of non-compliance and helps hospitals avoid fines, reputation damage and other costs of HIPAA violations and privacy breaches

**Challenge.**
By allowing patients’ electronic health records (EHR) to be shared at the point of care, hospitals can improve clinical decision-making, reduce errors, increase efficiency, lower costs and produce better outcomes. Unfortunately, the technologies—including smart multifunction devices (MFDs), smartphones, tablets and laptops—which increase access to EHR are also some of the biggest security vulnerabilities in EHR. Smart MFDs and mobile devices are often used for sending or receiving unencrypted protected health information (PHI).

The growing use of smart devices at the point of care exacerbates the dual, yet contradictory, challenges confronting hospital IT directors and compliance officers today: Making patients’ health information easier to access and share, while at the same time, increasing security. Smart MFDs, smartphones, tablets and notebook computers are especially attractive to thieves. The Office of Civil Rights reported that theft or loss of portable and unencrypted devices is the leading source of reported HIPAA data breaches and fines.
“According to a study by the data security and privacy research organization The Ponemon Institute, 81% of healthcare organizations said they already use smart devices to collect, store or transmit some form of Protected Health Information (PHI), although 49% do nothing to protect them.”
Electronically completed forms can be printed securely on networked MFDs, with the mobile device used to activate “touch free” release of the document. This reduces the risk of exposing PHI in a document left unattended at the printer.

Physicians can also receive electronic requests for orders or referrals that they can review and sign on their mobile devices, wherever they are. For example, a physician receives a document as a secure email attachment. After opening it with the Nuance software, the physician simply chooses “MD Electronic Signature”—or whatever label the hospital might apply to the activity—to sign the document with a user-authenticated signature, now burned onto the form permanently, creating a complete audit trail.

Photos taken with the device’s camera can be added to documents, but they don’t remain on the camera roll. Instead, these images are deleted automatically, so that a lost or stolen device provides no access to patient information.

Nuance software enforces security policies automatically to prevent confidential data loss. The solution filters outbound communications for PHI content, controls all attempts to send information, and intercepts documents that should not leave the hospital network. Fax transmission from smart MFDs can be restricted to approved numbers, eliminating mis-delivery. Nuance software can redact confidential information automatically before sending the fax, or it can prevent the fax from being sent.

The security of smart technologies and devices is a significant and unresolved challenge for hospitals that want to use and share patient information effectively at the point of care. The smart MFDs, smartphones, tablets and laptops that can deliver the full benefits of EHR deployments are also among the biggest security vulnerabilities.

With Nuance document workflow and security solutions, hospitals no longer have to worry about the security and control of their patients’ protected health information at the point of care.

To learn more about Nuance please call 1-855-367-4445 or visit nuance.com
About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.