CASE STUDY - UNIVERSITY HEALTH CARE SYSTEM

Background: The Mission of University Health Care is to improve the health of those they serve. University Health Care System employees, management and medical staff share a deep commitment to the health of the citizens of our communities.

Characterized by a strong commitment to quality and safety, the University Health Care System helps ensure their patients receive the highest level of care, delivered with dignity and compassion, for every patient and family member, every time.

Challenge: University Health officials consistently research new technologies and methods to help protect safety and streamline registration to improve the patient experience. Protecting patient medical identities from the danger of medical ID theft and fraud was another important initiative at University Health to ensure safety throughout the care continuum and sustain patient data integrity.

Emergency Departments (ED) can be subjected to healthcare fraud from individuals without insurance seeking care, especially those with manageable chronic conditions. University Health's ED was no exception, experiencing a number of cases where individuals attempted to defraud the healthcare system by providing different names, dates of birth, or other demographic information during registration.

University Health's Hospital patient access staff on alert for healthcare fraud often must strike a tricky balance of ensuring a patient receives timely care with the need to identify and prevent these individuals from illegally obtaining medical services that could raise liability and possibly harm the patient.

Location: Augusta, GA
Number of beds: 581
Biometric Modality: Photo Biometrics (Iris)
Electronic Medical Record (EHR) System: Epic

Patients who may be trying to defraud the system can raise the cost of care for everyone with most of the cost to treat these individuals passed on to insurance providers that raise premiums to subsidize care provided to the uninsured. It's a persistent problem at University and throughout healthcare that jeopardizes patient safety.

University Health's challenge was to identify a patient identity management technology that would create a unique identifier linked to a patient's medical record to eliminate duplicate medical records, overlays, medical ID theft, and patient fraud. The solution had to be:

- User-friendly
- Hygienic, requiring no contact from patients
- Non-invasive for patient acceptance
- Require minimal internal resources to implement
- Seamlessly interface with their Epic electronic health record (EHR) system
- Provide fast and accurate results
- Easily be scaled to use across a health information exchange (HIE) or integrated delivery network (IDN) ensuring a clean MPI
- Able to instantly identify unconscious patients or trauma patients

CASE STUDY - UNIVERSITY HEALTH CARE SYSTEM

Solution: When University Health System staff sat down to address the problem of healthcare fraud and began to assess patient authentication technology options that had the potential to prevent it, they decided to deploy the RightPatient® biometric patient identification as part of an overall strategy to increase patient safety, eliminate duplicate medical records, and prevent medical identity theft and fraud throughout their network.

University launched the RightPatient® patient identification system in August of 2015 at both hospitals in their network and began registering patients and linking their unique biometric credentials to a single electronic health record (EHR).

University Health diligently evaluated several different biometric patient identification technologies before deciding to deploy Photo Biometrics with RightPatient®, the most accurate, hygienic, and versatile solution available. University Health was pleased with the seamless integration of RightPatient® into their Epic workflows and the unique ability to minimize potential patient registration errors.

Using RightPatient®, patients simply take their picture and the platform identifies them, retrieves the correct medical record within Epic, and displays the patient photo for two-factor authentication. Seamless integration of RightPatient® into Epic's registration system along with an extremely user-friendly interface and a comprehensive analytics platform sealed University's decision to implement RightPatient® with Photo Biometrics.

Benefits: University Health implemented RightPatient® because photo biometrics is more accurate than fingerprinting or palm vein mapping and they liked the fact that patients did not have to touch a device to be identified, ensuring a safe, hygienic environment that supports hospital infection control.

RightPatient® added an important layer of protection over University Health's Epic EHR data integrity and patients feel very confident that University is taking the right steps to protect their medical identities and ensure a safe care environment.

Since implementing RightPatient®, University Health has seen a nearly 30% decline in chart corrections among other benefits. The platform is also eliminating write-offs associated with patient fraud.

The deployment has been a resounding success, with over 99% of patients opting in to ensure the safety and privacy of their PHI. So far, nearly 50,000 patients have enrolled in the system. Considering the fact that true return on investment (ROI) of biometric patient identification solutions are realized when an enrolled patient returns and is identified, University adopted a clear, transparent and thorough approach to explaining the technology to patients that quickly built their enrollment database. University placed a great deal of emphasis to ensure their staff understood why the RightPatient® solution was implemented and meticulously trained patient access personnel on how to properly use the system prior to launch.

The persistent and dangerous problem of medical identity theft and healthcare fraud is a direct threat to patient safety but also has repercussions that impact many other facets of care delivery.

Implementing modern patient identification technologies that have the unique ability to prevent healthcare fraud should be a key goal for any medical facility set on improving safety, lowering liability, and raising the quality of care.

CASE STUDY - UNIVERSITY HEALTH CARE SYSTEM

In one case, a patient was registered through the ED in the RightPatient® system, and then returned to the same ED days later claiming a different date of birth and a different last name. Following hospital registration protocol, the University patient access representative took the patient's photo with an iris camera and the RightPatient® system immediately flagged the patient's medical record and instantly notified staff that the patient had previously enrolled with their biometric credentials already linked to another unique EHR. University staff then realized that the patient was attempting to assume another identity and took action to prevent it.

Even if this patient had enrolled in the RightPatient® biometric patient identification system at another location within University's network, they still would have been flagged as a potential fraud case if they returned to a different facility due to the fact that RightPatient® seamlessly integrated with University's Epic EHR system and can be used at any point along the care continuum, regardless of the patient's physical location within the network (RightPatient® can even be used to authenticate an identity on patient portals and mHealth applications!). The University Health System case study clearly demonstrates that RightPatient® deters medical identity theft and healthcare fraud throughout the care continuum by linking a patient's unique biometric credentials to one medical record.