# TWC: Small: Analysis and Tools for Auditing Insider Accesses

Challenge:

- Attacks to patient medical records are increasing

- Millions of accesses per day must be analyzed

- Standard anomaly detection performs poorly due to healthcare's dynamic work environment

Solution:

- Machine learning for EMR auditing

- Large graph search to find connections between patients and employees

- Enhance results by filling in missing data (hospital social network)
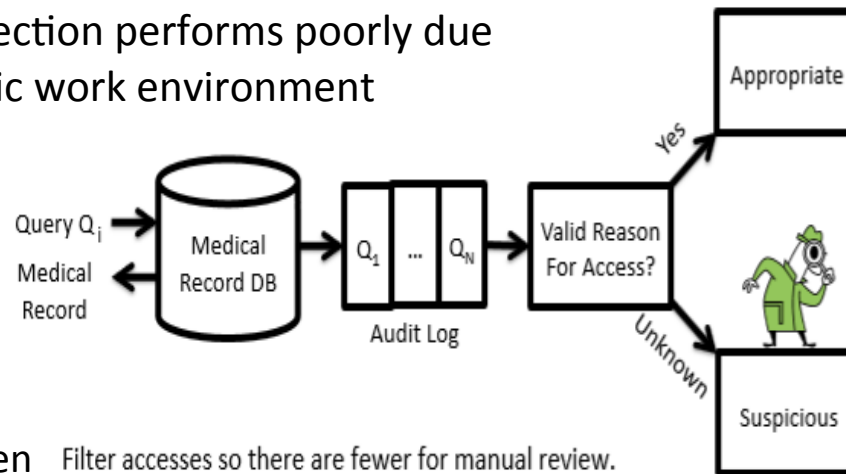
Filter accesses so there are fewer for manual review.
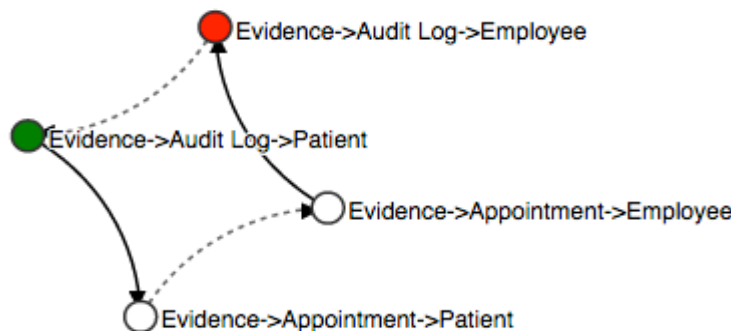
The system learns reasons for access, modeled as connections from patients to employees between EMR metadata (e.g., appointments, diagnosis data).

Scientific Impact:

- Develop methods to differentiate appropriate vs. inappropriate access

- Construct models to fill-in missing data needed for security and privacy analyses

Broader Impact:

- Tools to protect patient medical records and deter future inappropriate use

- Graduate student currently analyzing high-risk alerts statistics