TRUSTWORTHY HEALTH AND WELLNESS (THAW)

Dartmouth College

Johns Hopkins University

University of Illinois

University of Michigan

Vanderbilt University

David Kotz – February 2014

Trustworthy Health and Wellness

- Funded by a Frontiers award from the NSF Secure and Trustworthy Cyberspace (SaTC) program, starting September 1, 2013.
- Follow us at **thaw.org**

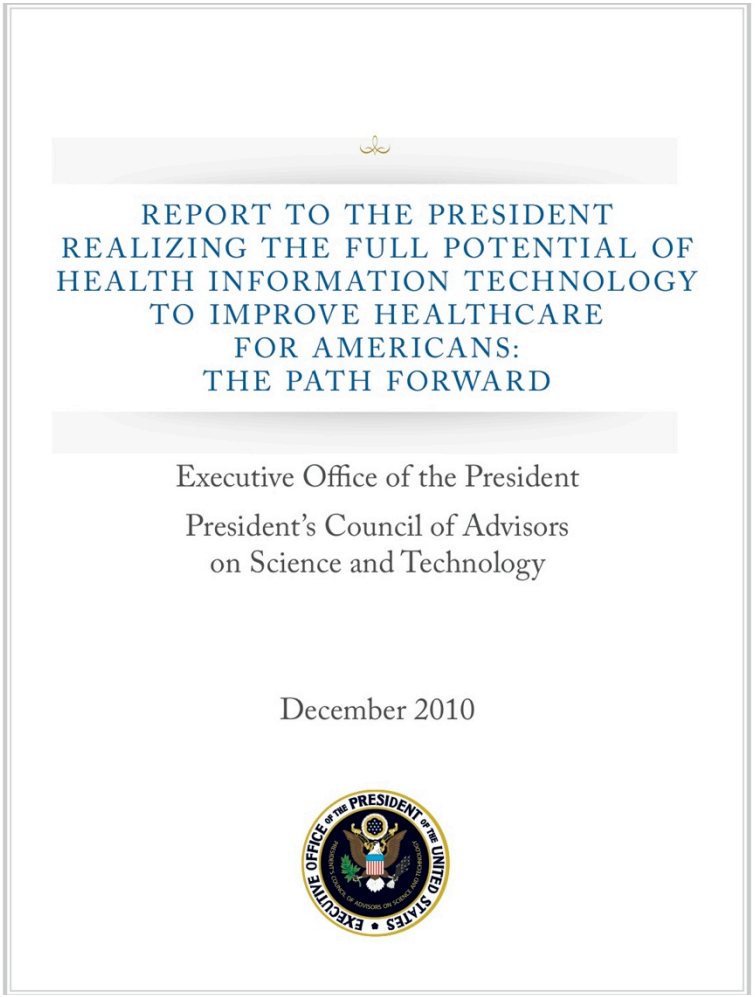
TH&W

Interdisciplinary research team

- Principal Investigators
  - **Kevin Fu** (UM) – medical device security
  - **Carl Gunter** (UIUC) – computer security in healthcare
  - **David Kotz** (Dartmouth) – mHealth security and privacy
  - **Avi Rubin** (JHU) – cybersecurity, cryptography, e-voting, healthcare
- Computer Science
  - **Michael Bailey** (UM) – availability and security of complex distributed systems
  - **Roy Campbell** (UIUC) – security, cloud computing, and ubiquitous computing
  - **Steve Checkoway** (JHU) – embedded systems security
  - **Peter Honeyman** (UM) – storage, security, and distributed systems
  - **Carl Landwehr** (GWU) – cybersecurity
  - **Klara Nahrstedt** (UIUC) – security, cloud computing, and multimedia
- Economics of healthcare IT
  - **Eric Johnson** (Vanderbilt) – economics of financial and medical identity theft
- Healthcare IT
  - **Darren Lacey** (JHU) – Chief Information Security Officer at JHU Medicine
- Behavioral health
  - **Lisa Marsch** (Dartmouth) – Director of the Center for Technology and Behavioral Health
- Health policy and population health
  - **Jonathan Weiner** (JHU) – Director of the Center for Population Health IT

Healthcare IT essential to the U.S.

- Healthcare is a major part of our economy (18% GDP)
- I.T. has the potential to improve quality and reduce cost of healthcare
- Mobile & cloud technology is being deployed for health and wellness
- Security and privacy are essential to attain the quality and trust of patients and clinicians alike
- Fundamental research challenges remain!



REPORT TO THE PRESIDENT
REALIZING THE FULL POTENTIAL OF
HEALTH INFORMATION TECHNOLOGY
TO IMPROVE HEALTHCARE
FOR AMERICANS:
THE PATH FORWARD

Executive Office of the President

President's Council of Advisors
on Science and Technology

December 2010

Five trends in Healthcare IT

– and their implications for security and privacy

- Shifting locus of care
  - Healthcare delivered through small clinics, elder-care centers, or home
  - Patients and clinical staff move among hospital, clinic, and residence
  - Distributed and remote monitoring, supported by cloud services

Five trends in Healthcare IT

– and their implications for security and privacy

- Shifting locus of care
- Accountable care and patient engagement
  - Accountable Care Organizations (ACOs)
  - ACOs need to collect metrics about health of their patient population
  - ACOs motivate patients to engage and remain healthy

Five trends in Healthcare IT

– and their implications for security and privacy

- Shifting locus of care
- Accountable care and patient engagement
- Continuous patient monitoring outside the clinical setting
  - For post-discharge monitoring of patients returning home
  - For monitoring and managing chronic conditions
  - For encouraging healthy behavior and assisting with behavioral health

Five trends in Healthcare IT

– and their implications for security and privacy

- Shifting locus of care
- Accountable care and patient engagement
- Continuous patient monitoring outside the clinical setting
- Advent of mobile devices and cloud services in health-related applications
  - Smartphones and wearables measure physiology, activity, and environment
  - Cloud services support small and distributed healthcare organizations

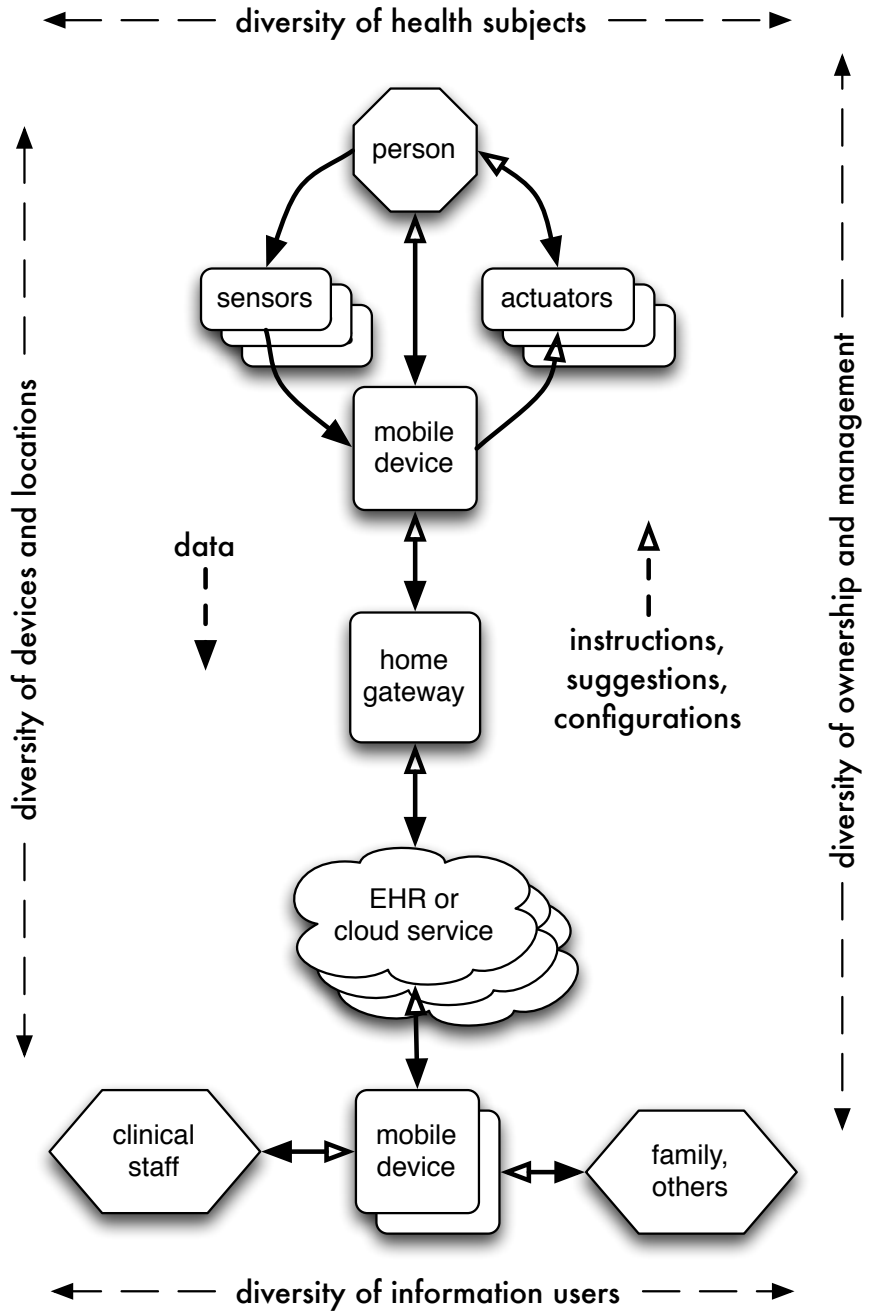
Five trends in Healthcare IT

– and their implications for security and privacy

- Shifting locus of care
- Accountable care and patient engagement
- Continuous patient monitoring outside the clinical setting
- Advent of mobile devices and cloud services in health-related applications
- Emerging threats and changing regulatory environment
  - Expanding use of EHRs increase risk of large-scale privacy breaches
  - Increasing occurrence of Medical identity theft
  - Mobile devices and cloud services increasingly under attack
  - FDA planning to regulate some mHealth devices/apps as medical devices

TH&W

- Focus on the advent of mobile and cloud tech
- Address issues of authentication, privacy, trustworthy control, and accountability
- Issues are critical in healthcare domain
- Solutions applicable to other domains



Nine initial projects on three themes

- Usable authentication and privacy tools
  - Clinician friendly authentication
  - Selective reporting of mHealth telemetry
  - Break-the-glass with segmented records
  - Genomic personal health records
- Trustworthy control of medical devices
  - Securing small health networks
  - Securing remote directives
- Trust through accountability
  - Malware detection using power analysis
  - Trust in mHealth data
  - Audit models and malware detection

Clinician friendly authentication

- Extensive studies* of clinical settings show that passwords are an inconvenient and insecure method for access control.
- Clinical staff come and go frequently, on shared computing devices.
- We propose to explore a method based on continuous monitoring of user's gestures, noting whether they correlate with interactions on screen.

- Staffer wears an identification bracelet, which wirelessly shares accelerometry with nearby devices.
- Scientific challenge: real-time, low-energy determination of which bracelet is using which tablet, computer, or other device.

*Sara Sinclair and Sean W. Smith. *Access control realities as observed in a clinical medical setting.* Technical Report TR2012-714, Dartmouth College, Computer Science, Hanover, NH, January 2012.

Securing small health networks

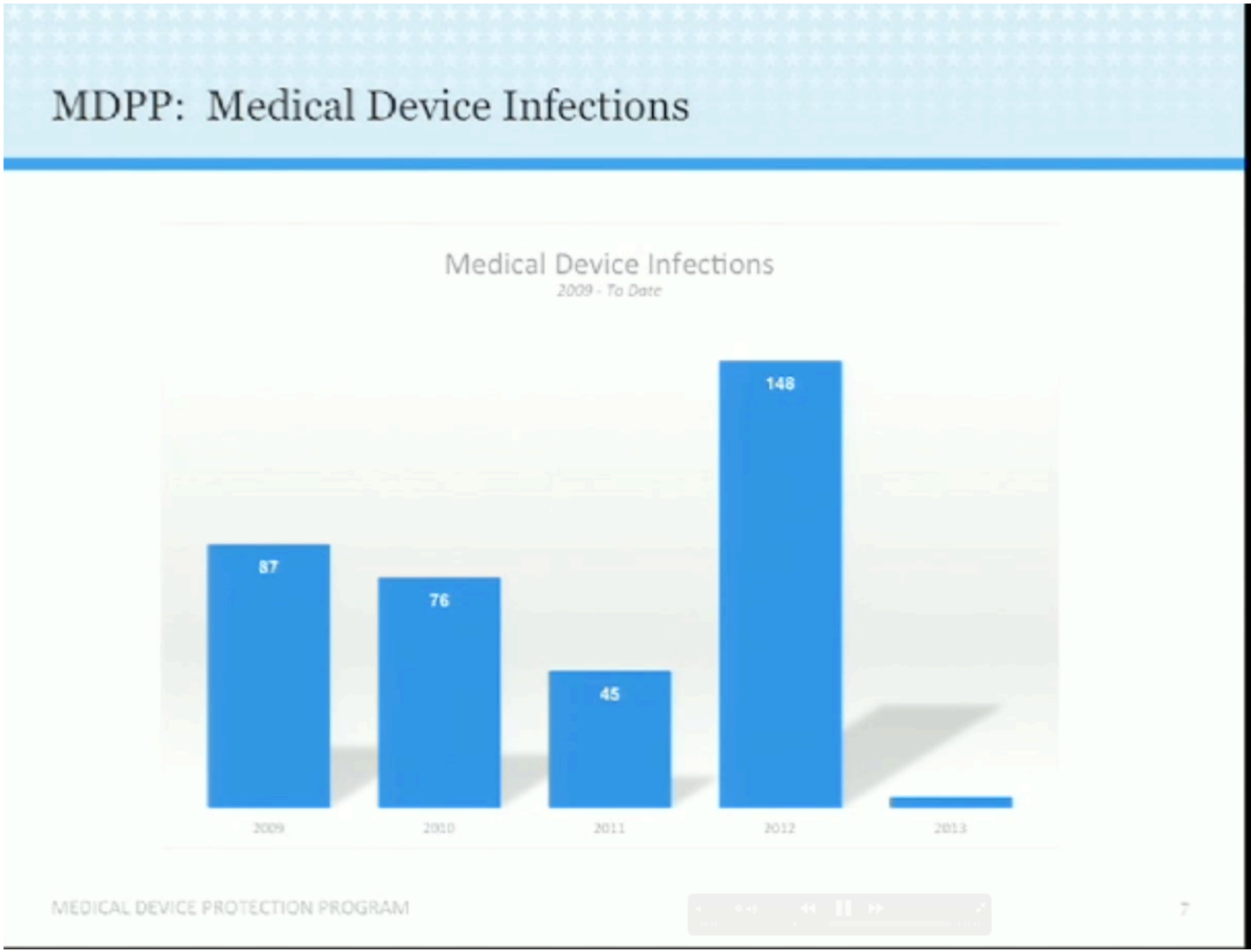
Scenarios:

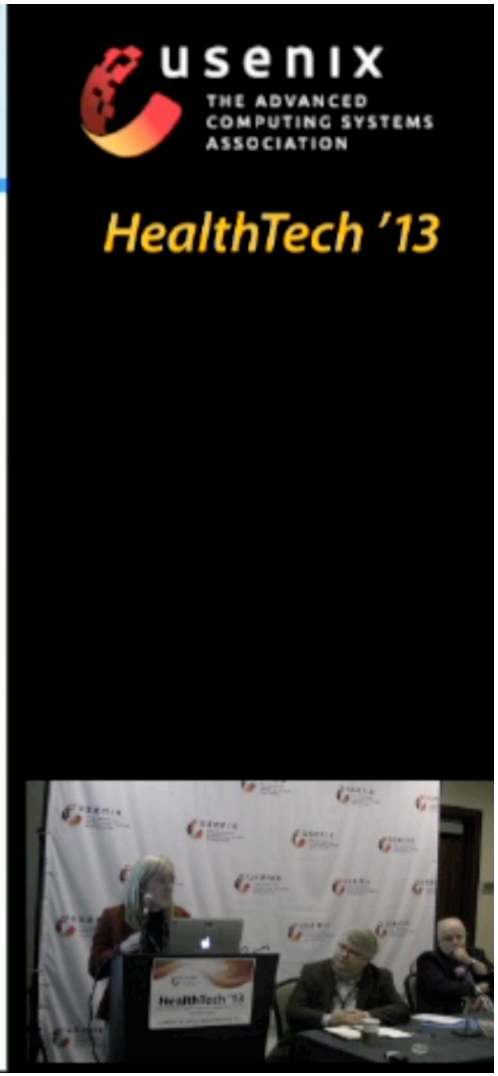
- Small health clinic with no on-site technical staff, needs all computing devices managed remotely by parent hospital or HIT provider
- Household with multiple health-related devices and commodity Internet connection.

Challenges:

- How to automate management tasks in a large network with many distributed components.
- How to design automated unattended key and software update without human interaction.

Medical device malware





Lynette Sherrill, HealthTech'13: https://www.usenix.org/conference/healthtech13/health-data-and-device-perspectives-industry-government-and-health-providers

Malware detection using power analysis

- Goal: Measure actual malware prevalence at hospitals
- Develop scientifically reproducible methods
- The idea:
  - Measure power consumed by the device under normal operation
  - Learn a model of ‘normal’ uninfected power signature(s)
  - Monitor power consumed by the device
  - (no hardware or software changed in the device)
  - Alert sysadmins when the power signal no longer matches normal

Medical De

Summary – THaW mission

To enable the promise of health and wellness technology by innovating mobile- and cloud-computing systems that respect the privacy of individuals and the trustworthiness of medical information.

Follow us at **thaw.org!**

This research program is supported by a collaborative award from the National Science Foundation (NSF award numbers CNS-1329686, 1329737, 1330142, and 1330491).

TH&W

BACKUP SLIDES

Science (projects 1 and 2)

Project 1: Clinician friendly authentication (Kotz)

- Can we build a user-friendly authentication solution based on "what you do" (how you interact with a tablet), in addition to "what you have" (a bracelet)?
- How can we leverage this approach to seamlessly and efficiently maintain continuous verification of the tablet's user?

Project 2: Selective reporting of mHealth telemetry (Kotz)

- How can we present trust policies to non-technical individuals in a way that facilitates informed decisions about the risks and benefits of data sharing, and provide usable controls for personal customization of those policies?
- How can this system 'learn' which inferences about an individual may be considered 'sensitive', and use those learned facts to better inform the individual about the risks of sharing certain kinds of medical or behavioral data?

Science (projects 3 and 4)

Project 3: Break-the-glass with segmented records (Checkoway)

- How to build time- and location-aware role-based access control mechanisms for a heterogeneous collection of devices.
- How to detect anomalous access from noisy audit log data minimizing false positives and false negatives.

Project 4: Genomic personal health records (Gunter)

- Genomics is often mentioned as a key “big data” problem. We will address security and privacy dimensions for this area that will also clarify requirements and yield technologies for other areas.
- Understanding the limits of discretionary control as a foundation for privacy.

Science (projects 5 and 6)

Project 5: Securing small health networks (Rubin)

- How to automate management tasks in a large network with many distributed components.
- How to design automated unattended key and software update without human interaction.

Project 6: Securing remote directives (Rubin)

- How to deal with insider threat.
- Designing protocols between two parties where one party demonstrates to the other that it is not cheating.

Science (projects 7 and 8)

Project 7: Malware detection using power analysis (Fu)

- How to advance measurement science of information security threats in highly constrained computing environments.
- How to infer device state with high precision and accuracy via coarse-grained power side channels.

Project 8: Trust in mHealth data (Kotz)

- How can one express the 'provenance' of health-related data collected by mobile devices, in support of data consumers' need to assess the authenticity and accuracy of that data?
- What structure makes it possible (and easy) for application developers and system designers, not to mention data consumers, to specify the kinds of contextual metadata to be included with sensor data?

Science (project 9)

Project 9: Audit models and malware detection (Gunter)

- Formal representations of the meaning of audit data in a heterogeneous context.
- Making assessments of malware penetration in contexts that include a diverse collection of networked systems and changing connectivity.

STIGMALWARE

Problem and Motivation

- Identify, qualify, and quantify malware in the clinical domain.
- “But wait, I thought safety trumps security for medical devices?!”

Methodology

- Using Darknet and U-M Netflow datasets, analyze connections between hosts in the hospital network to hosts in the external world.

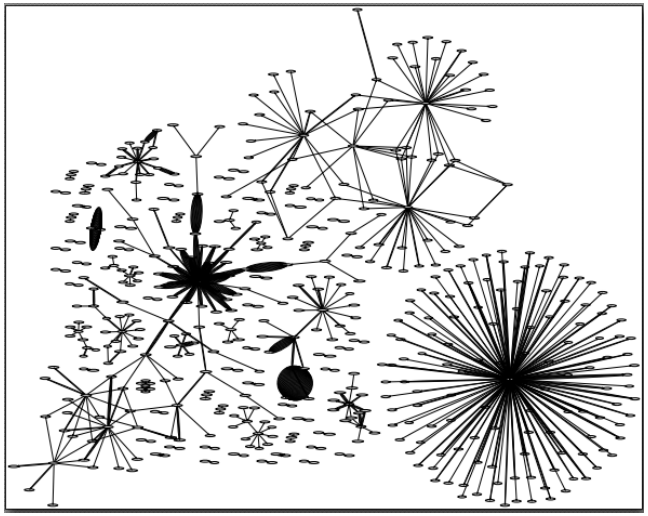
```
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes
2013-09-04 16:24:16.155 84069.531 UDP    179.235.157.234:1230  ->      193.9.0.124:123    .A....   0     4915   373540
2013-09-04 16:24:27.492 84041.945 UDP     114.107.83.123:1230  ->      193.9.0.124:123    .A....   0     4905   372780
2013-09-04 16:23:48.517 84053.166 TCP     141.215.57.221:13802 ->    63.49.242.100:28395  ......   0     6758   333856
2013-09-04 16:23:48.453 84053.491 TCP      63.49.242.100:28395 ->    141.215.57.221:13802 ......   0     7270   433819
2013-09-04 16:24:14.119 84034.928 TCP      31.214.212.10:62915 ->    141.215.57.221:13802 ......   0     5856   330209
2013-09-04 16:24:18.724 83997.809 TCP     141.215.57.221:13802 ->    103.106.155.44:22870 ......   0     5752   286584
2013-09-04 16:23:23.813 84078.195 TCP      178.76.78.242:2596  ->    141.215.57.221:13802 ......   0     3685   177997
2013-09-04 16:24:18.727 84023.217 TCP     103.106.155.44:22870 ->    141.215.57.221:13802 ......   0     5490   307317
2013-09-04 16:24:03.876 84052.911 TCP     141.215.57.221:13802 ->     178.76.78.242:2596  ......   0     5050   256915
2013-09-04 16:24:14.115 84035.122 TCP     141.215.57.221:13802 ->     31.214.212.10:62915 ......   0     5845   291574

IP addresses anonymised
```

Goals

- What are the common pathways that lead to infected medical devices?
- How can we safeguard against these pathways? (at the user, institutional, and perhaps most importantly, manufacturer levels.)

Preliminary results

- Not much activity in Darknet data
  - Supports “hunch” that most malware now of the drive-by download variety.
- Netflow data seems to be infinitely more useful, as we can visualize flows in connection graphs.
  - There are hosts in U-M hospital subnet contacting malicious websites.



Current steps

- Need to perform data drill down on suspicious U-M host machines: are these hosts on the guest network or on the medical network? If on the latter, what type(s) of machines are these?
  - Do some computer “forensics”
- Try to gather netflow data from other hospitals, to supplement work being done with U-M dataset.

TH&W

THANK YOU.