BakerHostetler

Medical Device Connectivity: HIPAA, FDA and IP Considerations

Hussein Akhavannik
Lee Rosebush

About BakerHostetler

- About 950 attorneys in 14 domestic offices
- About 150 IP attorneys
  - More than 100 registered patent attorneys and agents
    - Including many former examiners, SPEs, and an APJ
  - Majority of about 4,000 applications filed per year for domestic clients
- More than 75 partners in our Life Sciences and FDA groups
  - Multiple attorneys who have worked at or contracted with FDA
- Represent a broad range of companies and institutions, including pharmaceutical, medical device, pharmacy, pharmacy distribution, biologic, cosmetic, nutritional supplements and more.

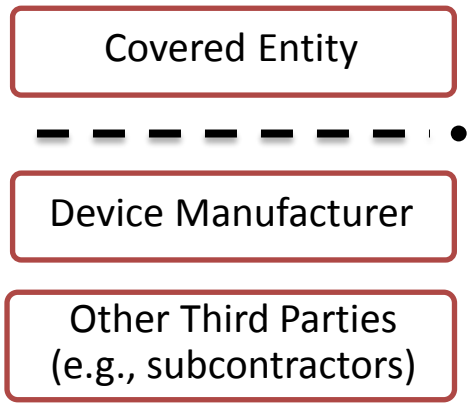
Topics

- HIPAA Compliance
- FDA Cybersecurity
  - Premarket
  - Post market
- Software for Wireless Control & Reception
  - Mobile Applications
  - Stand Alone Software as a Medical Device (SaMD)
- Patent Claiming Strategy + Copyright
- Benchmarking

HIPAA for Connective Medical Devices

HIPAA - Overview

- Who Should be in Compliance?
  - Does the device transmit Protected Health Information?
    - Individually identifiable
    - Consists of data regarding individual's health
  - Is entity subject to compliance with HIPAA?
    - Covered entities – health plans, health care clearinghouses, health care providers
    - Business associates – third party that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity



HIPAA – Business Associates

- Evaluation is very fact dependent
- Business associate activities and services include:
  - data analysis, processing or administration;
  - utilization review;
  - data aggregation
- Typical cases include:
  - When medical device generates protected health information and medical device company transmits PHI to covered entity
  - When a covered entity shares PHI with the medical device company

HIPAA – Compliance Requirements

- Covered entity and business associate required to execute a business associate contract
  - Describe the permitted and required uses of PHI by the business associate;
  - Provide that the business associate will not use or disclose the PHI other than as permitted or required by the contract; and
  - Require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI
- Key issues:
  - Privacy
  - Security (also ties in FDA)

General Considerations - Security

HIPAA and FDA regulated

- Connected medical devices incorporate software that is vulnerable to threats
- When medical device vulnerabilities are not addressed, this can serve as access points for entry into healthcare networks
  - Data confidentiality
  - Data integrity
  - Data availability
- Shared responsibility between healthcare facilities and providers and medical device manufacturers

HIPAA – Privacy Rule

- Basic framework – entities cannot disclose PHI except:
  - As permitted by Privacy Rule
  - When authorized by a patient in writing
- Permitted uses and disclosures include:
  - Treatment, payment, health care operations
  - Research
  - Limited data set

HIPAA – Security Rule

- Basic framework – entities must:
  - Ensure confidentiality, integrity, and availability of PHI;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the PHI;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by workforce
- Rule does not dictate specific measures, but recommends entities to:
  - Perform risk analysis
  - Implement security measures that reduce risk
    - Administrative (security management process, personnel)
    - Physical (facility access and control, workstation security)
    - Technical (access control, audit controls, integrity controls)

FDA Guidance for Connective Medical Devices

FDA – Cybersecurity Guidelines

- Guidance provided in:
  - Premarket Submissions for Management of Cybersecurity (finalized 6/14/2013)
  - Postmarket Management of Cybersecurity (finalized 12/28/2016)
- General considerations:

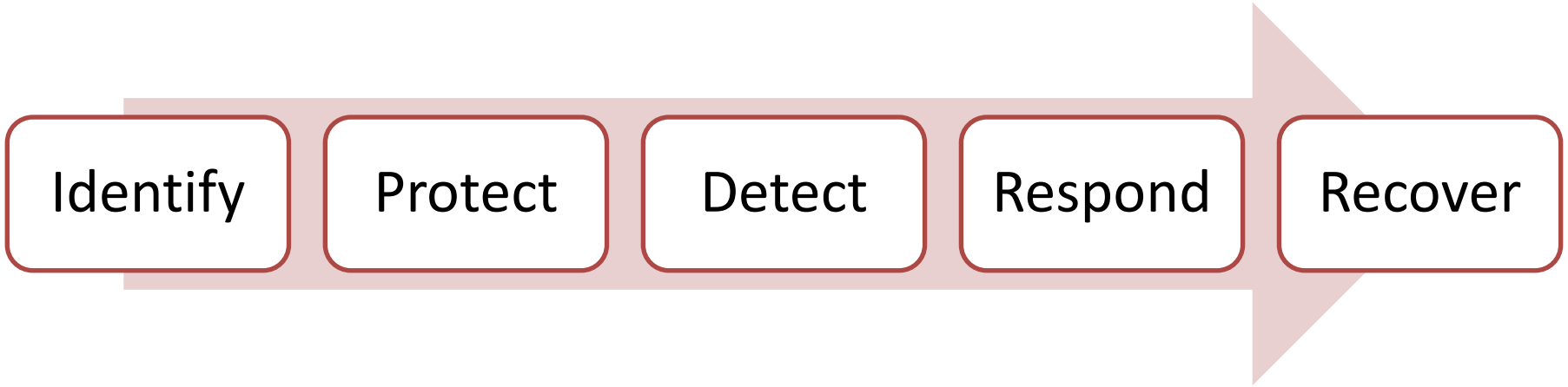
  Expands upon HIPAA considerations
  - Device manufacturers should incorporate specific controls into design of products
  - Device manufacturers should consider risk to patients as well as environment in which device is used

Recommendations for Premarket Submission

- Description of device
- Risk-based approach for verification and validation
- Test data summaries
- Labeling related to wireless medical devices

FDA – Premarket Management

- Core functions:



FDA – Premarket Management

- Identify and protect
  - Limit access to trusted users
  - Employ technical and physical access controls
- Detect, respond, and recover
  - Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon
  - Provide information on appropriate actions to take once device has been compromised
  - Implement device features that protect critical functionality
  - Provide methods for retention and recovery of device

FDA – Premarket Management

- Cybersecurity documentation
  - Hazard or risk analysis:
    - Provide information on risks that were considered
    - Provide justification for controls used to address risks
  - Traceability matrix that links cybersecurity controls to the cybersecurity risks that were considered
  - Summary documentation on:
    - Plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device
    - Controls that are in place to assure that the medical device software will maintain its integrity
  - Device instructions for use and product specifications related to cybersecurity controls

Selection and Performance of Wireless Technology

BakerHostetler

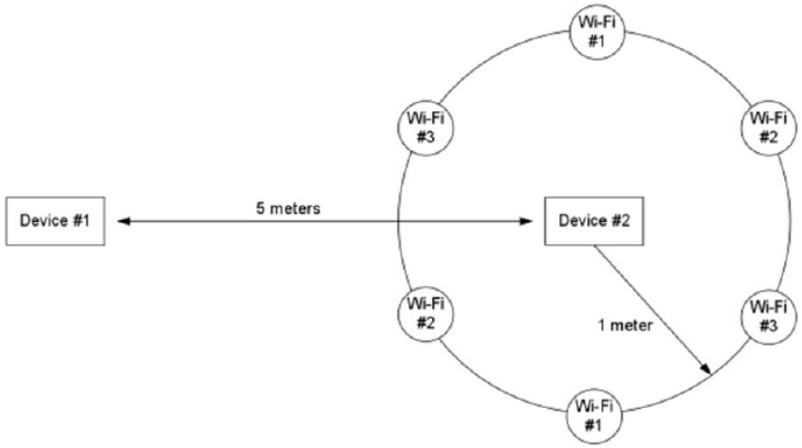
1) Quality of Service - Integrity of data transmitted wirelessly
2) Wireless Coexistence
   - Operating on unlicensed bandwidth?
   - Licensed bandwidth - Incumbent users of selected and adjacent bands
3) Electromagnetic compatibility - tissue propagation and absorption rate
4) Security
5) Maintenance

Wireless Quality of Service

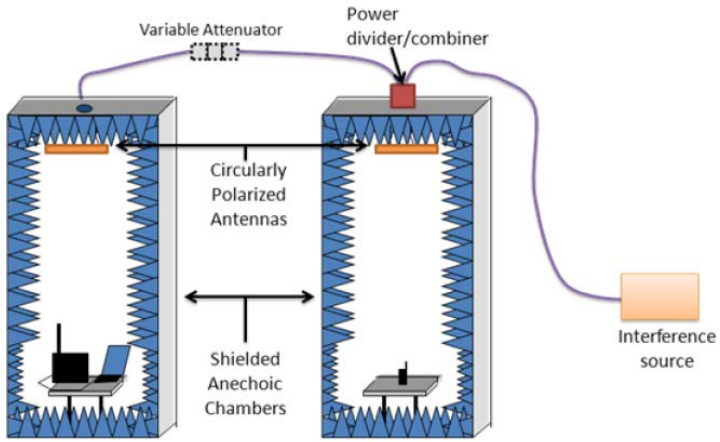
- Necessary level of service and performance needed for wireless functions of the medical device (e.g., latency and throughput, corruption control and prevention, signal to noise ratio)
- Potential Risks:
  - Connections lost without warning
  - Failure to establish connections
  - Degradation of service
- Justification of acceptable risk or demonstration of risk mitigation
  - Study fail modes
  - Regularly update patches
  - Ensure patient education

Wireless Coexistence Testing

- Appropriate testing required to demonstrate appropriate risk mitigation



Environmental Testing
Unlicensed Spectrum



Controlled Testing
Licensed Spectrum

[“An FDA Perspective on Medical Device EMC and Wireless”]

Electromagnetic Compatibility (EMC) of Wireless Technology

BakerHostetler

1. Considerations for interference to/from other equipment (e.g., overlapping frequency bands)
2. Risk analysis of potential interference (EMI) from environmental sources
   - Most EMI reports occur in defibulators (ICDs), pacemakers, neurostimulators, and infusion pumps
   - Case studies show probable EMI from common devices, such as electric razors and metal detectors
3. Biocompatibility - Comply with IEC 60601 (e.g., radiation, leak current, protective grounding, etc.)

Security of Wireless Signal and Data

- Access Control - Protection against unauthorized wireless access to device control
  - Prevent automatic detection of other devices (e.g., discovery mode of Bluetooth)
- Encryption - Software protection of wireless data transmission against unauthorized access
  - Latest wireless encryption encouraged – examples provided in October 2, 2014 guidelines

Labeling

- Specification (standard) and performance (e.g., power, range, bandwidth…) of wireless data transmission
- Information on limitations (e.g., max power or proximity to other in-band devices)
- Recommended security and encryption measures
- Information on issues that might arise and what to do
- Information on international limitations
- Appropriate FCC labeling

Common Bandwidths

- **Inductive Implants** (e.g., control or monitor cardio activity): Bands below 200 kHz at distances less than one foot
- **Medical Device Radiocommunication Service (formerly "MICS")**: Licensed bandwidth of 401-406MHz at distances up to about 10 feet.
- **Wi-Fi, Bluetooth and Zigbee**: Unlicensed bandwidth commonly used with cell phones, handheld devices and personal computers, operate in 902-928, 2400-2483.5 and 5725-5850 MHz bands at distances up to a few hundred feet.
- **Ultra-Wideband**: New uses of unlicensed ultra-wideband technologies are starting to emerge for medical telemetry and imaging applications.
- **Medical Micropower Networks**: New licensed spectrum to accommodate operation of implanted microstimulator devices in the 413-457MHz band at distances up to a few feet.
- **Medical Body Area Networks**: Licensed spectrum to allow a wireless personal area network ("PAN") of multiple body sensors to monitor or control patient functions. Operate in the 2360-2400 MHz band at distances up to a few feet.

FDA – Postmarket Management

- Implement cybersecurity risk management programs:
  - Identify hazards associated with the cybersecurity of a medical device
  - Estimating and evaluating the associated risks
  - Threat modeling to define how to maintain safety and essential performance of device
  - Controlling the associated risks
  - Monitoring the effectiveness of the controls
- Programs should focus on assessing <u>risk of patient harm</u> by assessing:
  - Exploitability of cybersecurity vulnerability
  - Severity of patient harm if exploited

FDA – Postmarket Management

FDA – Postmarket Management

- Controlled vs. uncontrolled risk
  - Controlled (acceptable) risk:
    - Implement routine updates and patches, device enhancements, etc. in timely fashion
    - Premarket review for software change is not typically required
  - Uncontrolled (unacceptable) risk:
    - Implement risk remediation measures as quickly as possible
    - Provide information on controls and residual risks to customers
    - Report vulnerability to FDA under Part 806 except when:
      - No adverse events
      - Remediate within timeline (60 days)
      - Active participant in an Information Sharing and Analysis Organization

Maintenance for Manufacturer

- Continue to manage risks associated with wireless technology
  - Implement routine updates and patches, maintain up-to-date encryption protocols
- Mandatory Reporting
  - Death
  - Serious Injury
  - Malfunctions that caused or could have caused death or serious injury
- Must investigate known failures

FDA Guidance and Legislation on Software for Medical Devices

Legislative Exclusions of Software (21st Century Cures Act)

BakerHostetler

- Streamlines FDA procedures to prioritize Breakthrough Devices
- Reduces or eliminates review of medical devices deemed to be low risk
- Requires the FDA to finalize guidance on software by November 7, 2017
- Removes five categories of software from FDA review with some categories capable of being brought back under FDA review

Software Excluded from FDA Review

- Category A: Software for administrative support of healthcare facilities
  - e.g., processing and maintaining financial records, claims and billing information, appointment schedules
- Category B: "Healthy lifestyle" software that provides no diagnostic, prevention or treatment function
- Category C: Electronic patients records, but not interpret or analyze patient records
- Category D: Software for transferring, storing, converting formats, or displaying test data lab tests or med device data, but not interpret or analyze patient records
- Category E: Clinical Decision Support Software (CDSS)
  - Software that provides recommendations based on medical information (e.g., peer-review)
  - Must enable independent review of the basis of the recommendations
  - Category E does not include medical imaging or *in vitro* testing

Recapture of FDA Jurisdiction by Congress

- FDA may bring Categories C, D, and E back under regulation with a showing of:
  - Likelihood and severity of patient harm
  - Extent to which software is intended to support clinical judgement
  - Reasonable opportunity for a health care professional to review the basis of the information
  - Intended user and use environment
- Requires Notice and Comment Rule Making

Mobile Applications (Apps) – 2015 Guidance

BakerHostetler

- Is the software a medical device under FDA regulations?
- FDA defines 3 broad categories that are regulated:
  - App controls a medical device – FDA considers it an accessory.
    - Example: Software that controls an insulin pump.
  - App that transforms the mobile device into a regulated device. May include attachment for standard mobile device. App may be labeled for medical specific uses.
    - Example: App that allows for control of attached transducer that converts a smartphone into a glucose meter.
  - App that performs patient-specific analysis and provides patient-specific diagnosis or treatment recommendations
    - Example: App that calculates dosage or creates a dosage plan for radiation therapy.
    - Potential overlap with Category E of the Cures Act

Stand Alone Software as a Medical Device (SaMD) – 2016 Guidance

BakerHostetler

- SaMD = software used for one or more medical purposes without being part of a hardware medical device
- Medical device not necessary to achieve function (peripheral)
- Examples of SaMD
  - Software that allows commercially available devices to view and process images for diagnostic purposes
  - Treatment planning software that supplies information used in a linear accelerometer
- SaMD does not include:
  - Software that drives or controls a medical device
  - Embedded software - Firmware
  - Non-medical software that just encrypts data (medical records)
  - Enables clinical communication and workflow such as patient registration, scheduling visits, voice calls, and video calling

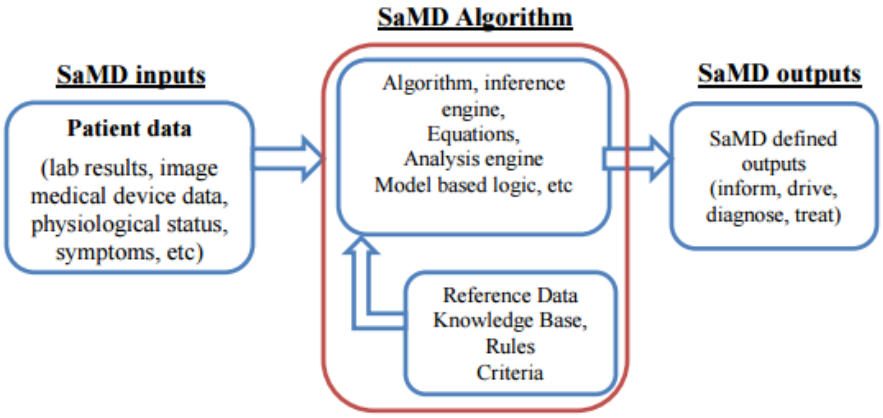


Figure 2: High Level SaMD Components

SaMD Categories

- SaMD grouped by four categories (I-IV) and three types (i-iii):
  - Category breakdown - Significance of the information provided by the SaMD
    - Inform clinical management
    - Drive clinical management
    - Treat or diagnose
  - Type breakdown - State of the healthcare situation or condition
    - Non-serious
    - Serious
    - Critical
  - Treat or diagnose for Critical type is fourth category

Clinical Evidence and Expectations of SaMD

BakerHostetler

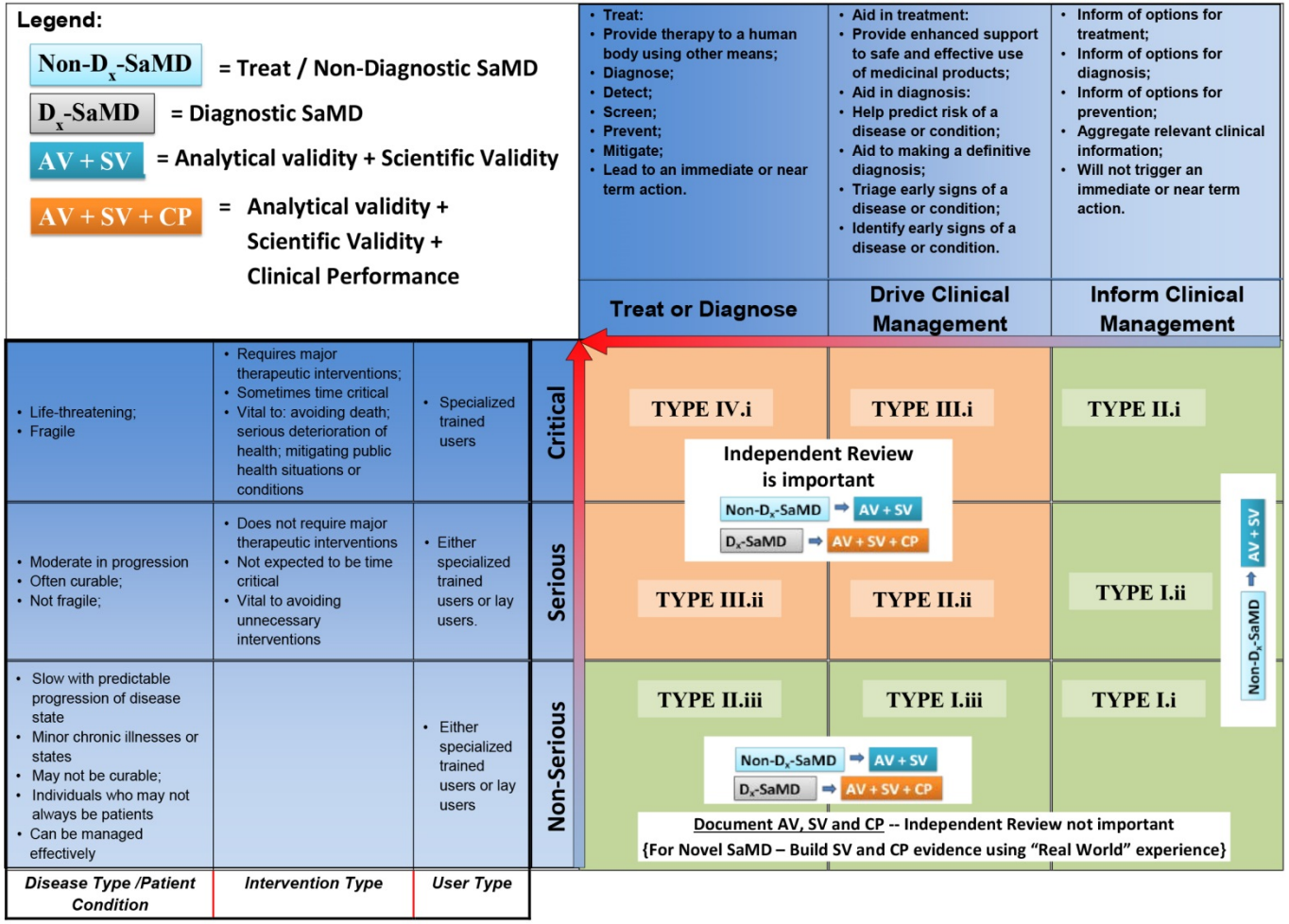


Figure 8 – Summary of Clinical Evidence and Expectations by SaMD Category

Patent Claim Strategy and Benchmarking

Strategies for Claim Drafting

- Focus claims on a single actor
  - Devices are connected - ecosystem is inherently a multi-actor
  - Ensures coverage for your system
  - Higher likelihood of infringement by direct competitors
- What can be protected?
  - Hardware
    - Combination of device/system-on-chip
      - Currently common with implantable devices
    - Position on device, in-vitro protection, material, etc.
  - Software
    - Processing and data collected by:
      - Device
      - Gateway (bedside receiver, router, mobile phone, etc.)
      - Server (hospital, manufacturer, or other covered entity)
  - Data structures
  - Graphical User Interface (GUI)
  - Trade secret for software details

Claiming Software

- Communication protocol (process) between actors
- Software for data collection
- Software for data analytics
  - Account for and analyze bad or unreliable data
  - Determine and transmit insight from data
    - Data visualization to deliver insight from data for hospitals and similarly situated patients
- Utility patent for GUI
  - Federal Circuit recently found claims to a GUI to be eligible. *See Trading Technologies International, Inc. v. CQG, Inc.* (2017).

Overcoming Alice

- Alice not as rigorously applied in the medical device art units as the business method art units
  - Understanding that there is some specialty hardware (device) associated with the process
  - The concept of connected medical devices and big data processing is **inherently new**
    - Not an old "fundamental concept"
- Recommend including details of the device collecting the data, the type of data collected, the algorithms used to process the data
- Explain changes that may result from processing – e.g., activating an alarm, cause update of firmware, change sensitivity or modality, etc.
- Discuss **practical benefits provided by the** invention

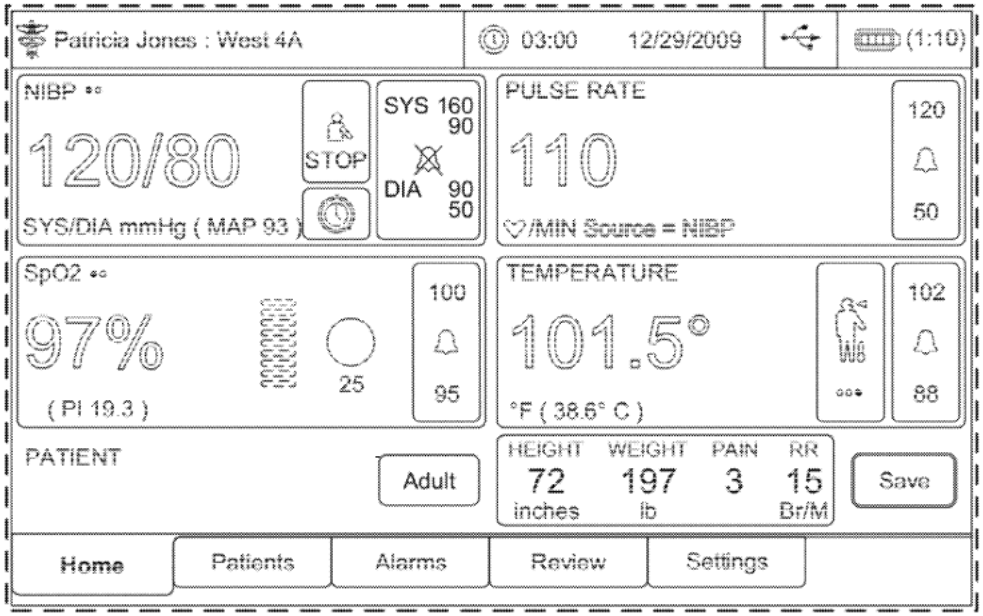
International Filing

- Device claims and method of manufacturing claims (more rare) patent eligible worldwide
- Methods of surgery and medical treatment methods
  - Patentable in the United States and Australia
  - Not in Europe, Japan, South Korea, or Canada
  - Sometimes can covert to “use” claims without mentioning human body
    - Manipulate device in novel way

Design Patent for GUIs

BakerHostetler

- Cover static structure of a GUI
  - Does not include the dynamic data (dashed out)
  - Bedside monitor
  - App for monitoring



Design Patent for GUIs

- Cover dynamic functionality by showing GUI over time or in response to user input
- Example: Apple's Slide to Unlock (D675,639)

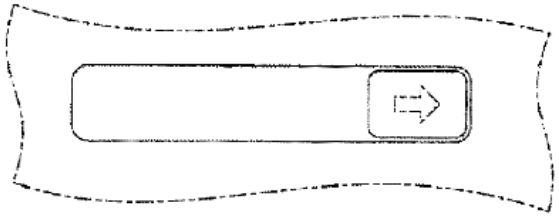


FIG. 4

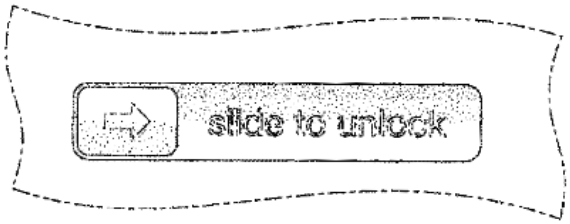


FIG. 5

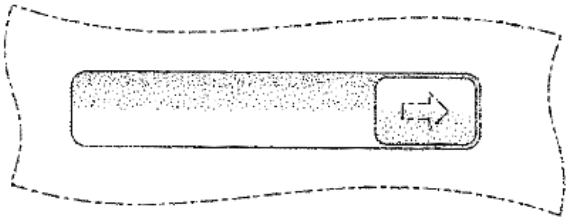


FIG. 6

Protecting Patient Monitoring

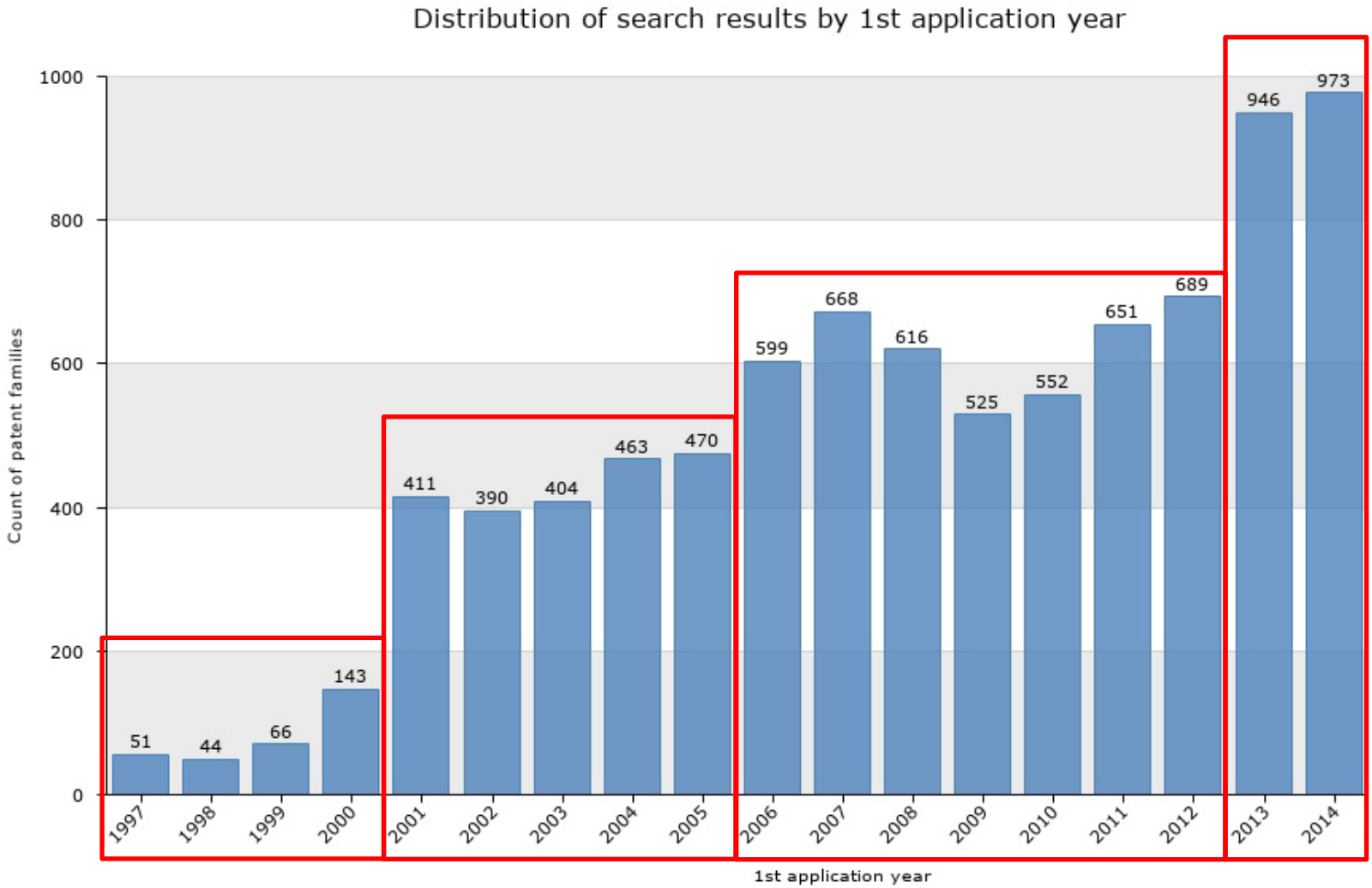
- Multi-tiered approach
  - Process for data collection
  - Process for data processing
    - Data validation/correction
    - Data visualization
    - Alert/alarm processing
  - GUI
    - Utility
    - Design
  - Process for patient input

Protectable Features of Databases

- Databases generally have copyright protection in the US
  - Per the Compendium sec. 1002.6—"[A] database generally consists of two fundamental elements:
    - (i) a data set or multiple data sets, and
    - (ii) an information retrieval program or system that serves as the sole entry point into the underlying data, information, or files.
  - Typically, the party that created the information retrieval program or system is not the same party that created the copyrightable content contained within the database.
  - An application to register a database typically covers the selection, coordination and/or arrangement of data, information or files, but does not cover the data, information or files unless they are specifically claimed in the application.

Increased Filings

BakerHostetler



Where being filed?

BakerHostetler

Atlanta
Chicago
Cincinnati
Cleveland
Columbus
Costa Mesa
Denver
Houston
Los Angeles
New York
Orlando
Philadelphia
Seattle
Washington, DC

www.bakerlaw.com