DRAFT
FDASIA Committee Report

David W. Bates MD, MSc, Chair

Committee Membership

- **David W. Bates, Chair**, Brigham and Women's Hospital
- **Patricia Brennan**, University of Wisconsin-Madison
- **Geoff Clapp**, Better
- **Todd Cooper**, Breakthrough Solutions Foundry, Inc.
- **Meghan Dierks**, Harvard Medical Faculty, Division of Clinical Informatics
- **Esther Dyson**, EDventure Holdings
- **Richard Eaton**, Medical Imaging & Technology Alliance
- **Anura Fernando**, Underwriters Laboratories
- **Lauren Fifield**, Practice Fusion, Inc.
- **Michael Flis**, Roche Diagnostics
- **Elisabeth George**, Philips Healthcare
- **Julian Goldman**, Massachusetts General Hospital/ Partners Healthcare
- **T. Drew Hickerson**, Happtique, Inc.
- **Jeffrey Jacques**, Aetna
- **Keith Larsen**, Intermountain Health
- **Robert Jarrin**, Qualcomm Incorporated
- **Mo Kaushal**, Aberdare Ventures/National Venture Capital Association
- **Mary Anne Leach**, Children's Hospital Colorado
- **Meg Marshall**, Cerner Corporation
- **Mary Mastenbrook**, Consumer
- **Jackie McCarthy**, CTIA - The Wireless Association
- **Anna McCollister-Slipp**, Galileo Analytics
- **Jonathan Potter**, Application Developers Alliance
- **Jared Quoyeser**, Intel Corporation
- **Martin Sepulveda**, IBM
- **Joseph Smith**, West Health
- **Paul Tang**, Palo Alto Medical Foundation
- **Bradley Thompson**, Epstein Becker Green, P.C
- **Michael Swiernik**, MobileHealthRx, Inc.
- **Jodi Daniel**, ONC
- **Bakul Patel**, FDA
- **Matthew Quinn**, FCC

Subgroups

- Taxonomy Subgroup
  - Patti Brennan, RN, PhD, Co-chair
  - Meghan Dierks, MD, Co-chair
- Risk/Innovation Subgroup
  - Keith Larsen, RPh, Co-chair
  - Paul Tang, MD, MS, Co-chair
- Regulation Subgroup
  - Julian Goldman,MD, Co-chair
  - Brad Thompson, JD, MBA, Co-chair

Charge

The Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012 calls for the HHS Secretary to "post a report—within 18 months (or by January 2014)—that contains a proposed strategy and recommendations on a risk-based regulatory framework pertaining to health IT, including mobile applications, that promotes innovation, protects patient safety, and avoids regulatory duplication".

FDASIA Committee did not have to develop the framework itself—that will be done by FDA, ONC, and FCC—but has been asked to make recommendations which will guide the development of the framework

Committee Process

- 3 months deliberation
- 1 in-person meeting
- 3 sub-groups
- Dozens of conference calls both in subgroups and larger group, and substantial processing through on-line approaches
- Considered much of the prior work done in this area including IOM committee recommendations
- Substantial input from all three involved agencies
- Public commentary on FDASIA process

Backdrop

- Literature suggests that HIT clearly appears to improve safety overall
  - Many studies which strongly support the benefits
  - However, literature also provides multiple anecdotes that health IT creates new safety risks
- Magnitude of harm and impact of health IT on patient safety is uncertain:
  - Heterogeneous nature of health IT
  - Diverse clinical environments, workflow
  - Limited evidence in the literature
- FDA has authority to regulate HIT but has not done so except in limited ways

Examples of Problems Associated with HIT

- Mortality rate increased from 2.8% to 6.3% (OR=3.3) in children transferred in for special care after introduction of a commercial CPOE application [1]
- "Flight simulator" of CPOE across 63 hospital EHRs detected only 53% of medication orders which would have been fatal [2]
- Clear problem of providers writing electronic orders on the wrong patient because they don't realize what record they are in [3]
- When even serious safety-related issues with software occur, no central place to report them to, and they do not generally get aggregated at a national level [4]

Example of Adverse Effect of Regulation

In closed loop systems, one application may drive another process, for example oxygen monitoring might tell an intravenous device to stop delivering narcotics if hypoxemia is detected. Traditionally there has been a very high regulatory bar for any closed loop approaches at the FDA, which may be preventing some beneficial closed loop approaches from being implemented.

- Reference: Standard *ASTM F2761-09, Annex B example B2.1*
- *References a death related to this intravenous narcotic use case, and a potentially safer system as described above that could be enabled by integrating sensors (e.g. pulse oximetry, respiratory CO2 monitoring) and infusion technology with decision support to close the loop.* The limitations of the current state and potential safety benefits of the proposed state are represented in animations at this site: http://www.mdpnp.org/MD_PnP_Program___Clinical_S.html

Taxonomy: Assigns HIT to One of Two Categories:

"Requires risk-based regulation" or "Risk-based regulation not needed"

- Guiding principles:
  - All entities addressed by the risk based regulatory framework can be described by a set of defining characteristics
  - Framework must be sufficiently robust to be able to meet future undefined needs
  - Avoid creating an inclusive inventory for determining what is regulated
  - A decision tree approach that emphasizes **functionality** as a primary scoping criterion
  - Functionality will help distinguish between two similar innovations, one requiring risk-based regulation and one not.

Defining Characteristics of What Should be Included as HIT

1. User type
2. Phases of product lifecycle
3. Developer/ 'Manufacturer' Type
4. Distribution model
5. Conditions of use
6. Intended use
7. Product categories
8. Miscellaneous

**More specifics regarding what group believed should be included as HIT are provided in additional slides*

DRAFT

Products Types - Categories

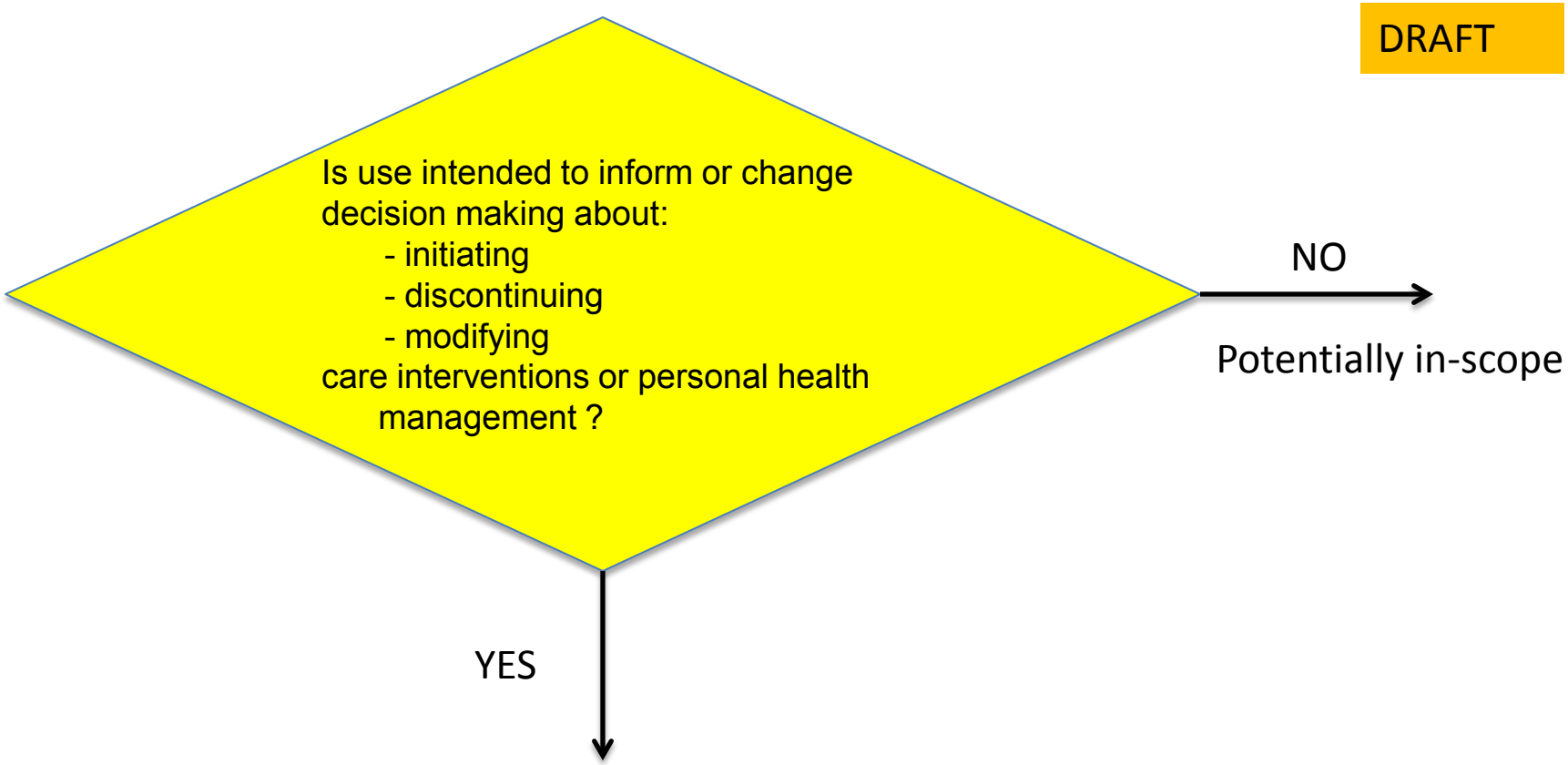
In Scope

- EHRs (installed, SaaS)
- Hospital information systems-of-systems
- Decision support algorithms
- Visualization tools for anatomic, tissue images, medical imaging and waveforms
- Health information exchange
- Electronic/robotic patient care assistants

Out of Scope

- Claims processing
- Health benefit eligibility
- Practice management / Scheduling / Inventory management
- General purpose communication applications (e.g., email, paging) used by health professionals
- Population management tools
- Software using historical claims data to predict future utilization/cost of care
- Cost effectiveness analytic software
- Electronic guideline distribution
- Disease registries

DRAFT



Out-of-scope …
defer to existing regulatory framework

Risk Framework

The patient-risk framework enumerates various important factors influencing the risk of software systems. It does not weight or "calculate" any specific risk score for a given software product. Rather, it serves as a framework to assess the factors to consider when evaluating the potential risk of patient harm arising out of the use of the software system. While the matrix characterizes the relative risk (i.e. "lower risk", "higher risk") of certain conditions of each risk factor, these serve as directional guidance only. Exceptions for each relative risk condition exist.

Basic definitions (International Electrotechnical Commission, modified)

- Harm – physical [or mental] injury or both to the health of people
- Hazard – potential source of harm
- Risk – combination of the probability of occurrence of harm and the severity of that harm
- Transparency – clear declaration of purpose, intended users, sources of data, sources of content knowledge, application logic applied to data, commercial sponsors of content knowledge

- Definitions which follow are to

Definitions (I)

- **Purpose of software** – the intended purpose for the software, as declared by the developer
- Developer provides transparent purpose and "scope of intended use"
  - For limited scope systems (e.g., radiation planning for use by radiation oncologist), would reduce the burden of complying with any regulation
  - For limited applications (e.g., information only for patients/consumers), it may effectively waive consideration for regulation
  - Regulatory language could control "off-label" use
  - By transparently declaring intended purpose, FTC may be able to hold developer accountable to stated purposes
- **Intended users** – the intended users of the software, as declared by the developer
  - The usability, ability to understand and act on the software output by the intended user is considered in the risk of the software's use in contributing to patient harm
  - The risk assessment would be applied to each class of intended user
- **Severity of injury**– the seriousness of patient harm that might arise from appropriate use of the software
  - Patient harm is an adverse event resulting from use of the software, which could vary in severity from a life-threatening event to a non-life-threatening adverse event
  - Risk could arise from anticipated, appropriate use or from foreseeable inappropriate use

Definitions (II)

- **Likelihood of the risky situation arising** – likelihood of the risky situation arising when the system is used in the care of a patient with the possible condition (e.g., cancer, hospital admission, subject of a procedure)
- **Transparency of software operation, data, and knowledge content sources** – visibility of the data, algorithms, and knowledge sources being used in the generation of the system's output
- **Hazardous situation**--circumstance in which people, property, or the environment are exposed to one or more hazard(s)
- The consumer of the system output could be a human user directly, or could be another system
  - On one end of the spectrum, the recipient of the system output can view all the data, algorithms, and knowledge content used to generate system output
  - At other end of the spectrum, the system could be operating as a black box
- **Ability to mitigate harmful condition** – ability for a human to detect and take action to mitigate any potential for harm
- Human intermediary could be mandatory (i.e., system output goes directly to a human), optional, or excluded (closed-loop operation)

Definitions (III)

- **Complexity of software and its maintenance** – complexity of the system software and the process for updating/maintaining it
  - Software may be complex, but can be tested comprehensively and can be operated reliably; complexity is considered in the risk assessment, but does not determine the level of risk alone
- **Complexity of implementation and upgrades** – complexity of human effort required to implement the software and its upgrade
  - Having a lot of "build" flexibility can allow helpful customization of the usability and effectiveness of the software, but it can provide many avenues for introducing risky situations not present in the "vanilla" system\
  - Methods and reliability of timely upgrades can affect patient-safety risk
- **Complexity of training and use** – complexity of learning to use the software effectively
  - Proxy for this is number of hours required for training
- **Use as part of more comprehensive software/hardware system** – the anticipated use as a part of a broader software system
  - Likely considerations could include:
    - Typical number of interfaces
    - Whether interfaces use mature, broadly adopted content and messaging standards
    - Level of redundancy to avoid single point of failure
- **Network connectivity** - standards, security, and regulated spectrum compliance
  - Include consideration of enforced standards and compliance

DISCUSSION DRAFT v2.3 for FDASIA Subgroup on Framework for Risk and Innovation DIMENSIONS of ASSESSING RISK of PATIENT HARM

Item	Lower risk	Medium Risk	Higher Risk/More Attention
Purpose of software product	Information-only; purpose is transparent and clear	Makes recommendations to user	Automated decision making (e.g., intelligent IV pump, AED)
Intended user(s)	Targeted user(s) are knowledgeable and can safely use product	Makes recommendations to knowledgeable user	Provides diagnosis or treatment advice directly to knowledgeable user
Severity of injury	Very low probability of harm	Potential for non-life threatening adverse event	Life-threatening potential
Likelihood of hazardous situation arising	Rare (<1 per 10,000 patient-years)	Unpredictable, but hazardous situation arises > 1:10K pt-yrs and < once a year	Common (arises once per -year)
Transparency of software operations and data and included content providers	Software output is easy to understand and its "calculation" (data and algorithm) transparent	Software operates transparently and output is understandable by software expert	"Black box"
Ability to mitigate harmful condition	Human intermediary knowledgeable and empowered to intervene to prevent harm	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	Application of mature, widely adopted technologies with information output that is easy to understand by the user	Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.	Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.	The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.	The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."
Complexity of training and use	The software system output is clear and easy to interpret. Minimal training needed.	Moderate complexity. Less than 2 hr of training required.	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.
Use as part of more comprehensive software/hardware system	Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure	Software interacts with 1-3 other systems with mature, well described interfaces	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].
Network connectivity, standards, security	Wired or tightly controlled wireless spectrum compliant with standards	Unregulated spectrum, but low risk of interference	Wireless using unregulated spectrum; proprietary interfaces

USE CASE: mHealth Nutrition app using DRAFT v2.3 Patient-Safety Risk Framework

USE CASE: mHealth Nutrition app. All of the Items listed in column 1 are highlighted as **Lower Risk** (defined in column 2).

Items	Lower risk	Medium Risk	Higher Risk / Greater Attention
Purpose of software product	***Information-only; purpose is transparent and clear***	Makes recommendations to user	Automated decision making (e.g., intelligent IV pump, AED)
Intended user(s)	***Targeted user(s) are knowledgeable and can safely use product***	Makes recommendations to patients	Provides diagnosis or treatment advice directly to patient
Severity of injury	***Very low probability of harm***	Potential for non-life threatening adverse event	Life-threatening potential
Likelihood of hazardous situation arising	***Rare (<1 per 10,000 patient-years)***	Unpredictable, but risky situation arises > 1:10K pt-yrs and < once a year	Common (arises once per year)
Transparency of software operations and data and included content providers	***Software output is easy to understand and its "calculation" (data and algorithm) transparent***	Software operates transparently and output is understandable by software expert	"Black box"
Ability to mitigate harmful conditions	***Human intermediary knowledgeable and empowered to intervene to prevent harm***	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	***Application of mature, widely adopted technologies with information output that is easy to understand by the user***	Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.	Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	***The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.***	The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.	The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."
Complexity of training and use	***The software system output is clear and easy to interpret. Minimal training needed.***	Moderate complexity. Less than 1 hr of training required.	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.
Use as part of more comprehensive software/hardware system	***Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure***	Software interacts with 1-3 other systems with mature, well described interfaces	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].
Network connectivity, standards, security	***Wired or tightly controlled wireless spectrum compliant with standards***	Unregulated spectrum, but low risk of interference	Wireless using unregulated spectrum; proprietary interfaces

USE CASE: mHealth BP display app using DRAFT v2.3 Patient-Safety Risk Framework

USE CASE: mHealth BP display app. All of the Items listed in column 1 are highlighted as Lower Risk (defined in column 2).

Item	Lower risk	Medium Risk	Higher Risk / Greater Attention
Purpose of software product	***Information-only; purpose is transparent and clear***	Makes recommendations to user	Automated decision making (e.g., intelligent IV pump, AED)
Intended user(s)	***Targeted user(s) are knowledgeable and can safely use product***	Makes recommendations to patients	Provides diagnosis or treatment advice directly to patient
Severity of injury	***Very low probability of harm***	Potential for non-life threatening adverse event	Life-threatening potential
Likelihood of hazardous situation arising	***Rare (<1 per 10,000 patient-years)***	Unpredictable, but risky situation arises > 1:10K pt-yrs and < once a year	Common (arises once per year)
Transparency of software operations and data and included content providers	***Software output is easy to understand and its "calculation" (data and algorithm) transparent***	Software operates transparently and output is understandable by software expert	"Black box"
Ability to mitigate harmful conditions	***Human intermediary knowledgeable and empowered to intervene to prevent harm***	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	***Application of mature, widely adopted technologies with information output that is easy to understand by the user***	Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.	Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	***The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.***	The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.	The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."
Complexity of training and use	***The software system output is clear and easy to interpret. Minimal training needed.***	Moderate complexity. Less than 1 hr of training required.	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.
Use as part of more comprehensive software/hardware system	***Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure***	Software interacts with 1-3 other systems with mature, well described interfaces	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].
Network connectivity, standards, security	***Wired or tightly controlled wireless spectrum compliant with standards***	Unregulated spectrum, but low risk of interference	Wireless using unregulated spectrum; proprietary interfaces

USE CASE: Insulin Pump using DRAFT v2.3 Patient-Safety Risk Framework

M

USE CASE: Insulin Pump: Four items are highlighted as **Higher Risk** (column 4) and the remainder are **Medium Risk** (column 3**)**. Purpose of Software Product (row 2); Intended User (row 3), Severity of injury (row 4) and Transparency of software operations (row 6) are highlighted as being **Higher Risk/More Attention.** The remainder of items in column 1: Likelihood of risky situation arising (row 5), Ability to mitigate harmful conditions (7), Complexity of software and its maintenance (8), Complexity of implementation and upgrades (9), Complexity of training and use (10); Use as part of more comprehensive software/hardware system (11); and Network connectivity, standards, security (row 12) are highlighted as being **Medium Risk.**

Item	Lower risk	Medium Risk	Higher Risk / More Attention
Purpose of software product	Information-only; purpose is transparent and clear	Makes recommendations to user	***Automated decision making (e.g., intelligent IV pump, AED)***
Intended user(s)	Targeted user(s) are knowledgeable and can safely use product	Makes recommendations to knowledgeable user	***Provides diagnosis or treatment advice directly to knowledgeable user***
Severity of injury	Very low probability of harm	Potential for non-life threatening adverse event	***Life-threatening potential***
Likelihood of hazardous situation arising	Rare (<1 per 10,000 patient-years)	***Unpredictable, but risky situation arises > 1:10K pt-yrs and < once a year***	Common (arises once per year)
Transparency of software operations and data and included content providers	Software output is easy to understand and its "calculation" (data and algorithm) transparent	Software operates transparently and output is understandable by software expert	***"Black box"***
Ability to mitigate harmful conditions	Human intermediary knowledgeable and empowered to intervene to prevent harm	***Human intermediary may be (but not routinely) involved***	Closed loop (no human intervention)
Complexity of software and its maintenance	Application of mature, widely adopted technologies with information output that is easy to understand by the user	***Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.***	Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.	***The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.***	The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."
Complexity of training and use	The software system output is clear and easy to interpret. Minimal training needed.	***Moderate complexity. Less than 2 hr of training required.***	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.
Use as part of more comprehensive software/hardware system	Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure	***Software interacts with 1-3 other systems with mature, well described interfaces***	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].
Network connectivity, standards, security	Wired or tightly controlled wireless spectrum compliant with standards	***Unregulated spectrum, but low risk of interference***	Wireless using unregulated spectrum; proprietary interfaces

USE CASE: EHR using DRAFT v2.3 Patient-Safety Risk Framework

USE CASE: EHR. More than half the column 1 Items are highlighted as **Higher Risk**. Two Items are highlighted as **Lower Risk**: Ability to mitigate harmful conditions (row 7) and Network connectivity, standards, security (row 12). Two items are **Medium Risk**: Purpose of Software product (row 2) and Transparency of software operations and data (row 6). The remaining items: Intended user(s) (row 3); Severity of injury (row4); Likelihood of risky situation arising (row 5); Complexity of software and its maintenance (row 8); Complexity of implementation and upgrades (row 9); Complexity of training and use (row 10); and Use as part of more comprehensive software/hardware system (row 11) are highlighted as **Higher Risk/More Attention.)**

Item	Lower risk	Medium Risk	Higher Risk / More Attention
Purpose of software product	Information-only; purpose is transparent and clear	***Makes recommendations to user***	Automated decision making (e.g., intelligent IV pump, AED)
Intended user(s)	Targeted user(s) are knowledgeable and can safely use product	Makes recommendations to knowledgeable user	***Provides diagnosis or treatment advice directly to knowledgeable user***
Severity of injury	Very low probability of harm	Potential for non-life threatening adverse event	***Life-threatening potential***
Likelihood of hazardous situation arising	Rare (<1 per 10,000 patient-years)	Unpredictable, but risky situation arises > 1:10K pt-yrs and < once a year	***Common (arises once per year)***
Transparency of software operations and data and included content providers	Software output is easy to understand and its "calculation" (data and algorithm) transparent	***Software operates transparently and output is understandable by software expert***	"Black box"
Ability to mitigate harmful conditions	***Human intermediary knowledgeable and empowered to intervene to prevent harm***	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	Application of mature, widely adopted technologies with information output that is easy to understand by the user	Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.	***Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks***
Complexity of implementation and upgrades	The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.	The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.	***The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."***
Complexity of training and use	The software system output is clear and easy to interpret. Minimal training needed.	Moderate complexity. Less than 2 hr of training required.	***The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.***
Use as part of more comprehensive software/hardware system	Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure	Software interacts with 1-3 other systems with mature, well described interfaces	***Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].***
Network connectivity, standards, security	***Wired or tightly controlled wireless spectrum compliant with standards***	Unregulated spectrum, but low risk of interference	Wireless using unregulated spectrum; proprietary interfaces

USE CASE: CDS using DRAFT v2.3 Patient-Safety Risk Framework

USE CASE: CDS. One item, Severity of injury (row 4), is highlighted as **Higher Risk/More Attention**, Four column 1 items are highlighted as **Lower Risk:** Intended user(s) (row 3); Ability to mitigate harmful conditions (row 7); Complexity of training and use (row 10) and Network connectivity, standards, security (row 12). Six items are highlighted as **Medium Risk:** Purpose of software product (row 2); Likelihood of risky situation arising (row 5); Transparency of software operations and data and included content providers (row 6); Complexity of software and its maintenance(row 8); Complexity of implementation and upgrades (row 9); and Use as part of more comprehensive software/hardware system (row 11);.

Item	Lower risk	Medium Risk	Higher Risk / More Attention
Purpose of software product	Information-only; purpose is transparent and clear	***Makes recommendations to user***	Automated decision making (e.g., intelligent IV pump, AED)
Intended user(s)	***Targeted user(s) are knowledgeable and can safely use product***	Makes recommendations to knowledgeable user	Provides diagnosis or treatment advice directly to knowledgeable user
Severity of injury	Very low probability of harm	Potential for non-life threatening adverse event	***Life-threatening potential***
Likelihood of hazardous situation arising	Rare (<1 per 10,000 patient-years)	***Unpredictable, but risky situation arises > 1:10K pt-yrs and < once a year***	Common (arises once per year)
Transparency of software operations and data and included content providers	Software output is easy to understand and its "calculation" (data and algorithm) transparent	***Software operates transparently and output is understandable by software expert***	"Black box"
Ability to mitigate harmful conditions	***Human intermediary knowledgeable and empowered to intervene to prevent harm***	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	Application of mature, widely adopted technologies with information output that is easy to understand by the user	***Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.***	Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.	***The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.***	The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."
Complexity of training and use	***The software system output is clear and easy to interpret. Minimal training needed.***	Moderate complexity. Less than 2 hr of training required.	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.
Use as part of more comprehensive software/hardware system	Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure	***Software interacts with 1-3 other systems with mature, well described interfaces***	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].
Network connectivity, standards, security	***Wired or tightly controlled wireless spectrum compliant with standards***	Unregulated spectrum, but low risk of interference	Wireless using unregulated spectrum; proprietary interfaces

USE CASE: PHR using DRAFT v2.3 Patient-Safety Risk Framework

USE CASE: PHR. No items are highlighted as **Higher Risk.** Two items are highlighted as **Medium Risk**: Use as part of more comprehensive software/hardware system (row 11) and Network connectivity, standards, security (row 12). The remainder of items (rows 2 through 10) are highlighted as **Lower Risk**.

Item	Lower risk	Medium Risk	Higher Risk / More Attention
Purpose of software product	***Information-only; purpose is transparent and clear***	Makes recommendations to user	Automated decision making (e.g., intelligent IV pump, AED)
Intended user(s)	***Targeted user(s) are knowledgeable and can safely use product***	Makes recommendations to knowledgeable user	Provides diagnosis or treatment advice directly to knowledgeable user
Severity of injury	***Very low probability of harm***	Potential for non-life threatening adverse event	Life-threatening potential
Likelihood of hazardous situation arising	***Rare (<1 per 10,000 patient-years)***	Unpredictable, but risky situation arises > 1:10K pt-yrs and < once a year	Common (arises once per year)
Transparency of software operations and data and included content providers	***Software output is easy to understand and its "calculation" (data and algorithm) transparent***	Software operates transparently and output is understandable by software expert	"Black box"
Ability to mitigate harmful conditions	***Human intermediary knowledgeable and empowered to intervene to prevent harm***	Human intermediary may be (but not routinely) involved	Closed loop (no human intervention)
Complexity of software and its maintenance	***Application of mature, widely adopted technologies with information output that is easy to understand by the user***	Medium complexity. Testing procedures exist that reliably assess patient-safety risk profile of product.	Complexity of data collection and "transformation" involved in producing output is significant. Difficult to test reliably for all safety risks
Complexity of implementation and upgrades	***The "build" and configuration of the software is straight-forward and does not materially affect the integrity of the output. Safety upgrades can be accomplished easily.***	The "build" and configuration of the software is moderately complex, but "guard rails" significantly limit types of changes that might induce life-threatening risk.	The "build" and configuration of the software is complex and can introduce substantial changes that can induce serious risk. Limited or no "guard rails."
Complexity of training and use	***The software system output is clear and easy to interpret. Minimal training needed.***	Moderate complexity. Less than 2 hr of training required.	The complexity of the user interface and density of data presented can cause important errors or oversights that can lead to serious risk. Formal training necessary.
Use as part of more comprehensive software/hardware system	Used as a standalone product, or output is unambiguously used as part of larger integrated system. Certified to specific hardware. Redundancy reduces single points of failure	***Software interacts with 1-3 other systems with mature, well described interfaces***	Almost always used as part of a larger software system AND output is subject to interpretation or can be configured in multiple ways whose mis-interpretation may induce harm. [e.g., DDI thresholds].
Network connectivity, standards, security	Wired or tightly controlled wireless spectrum compliant with standards	***Unregulated spectrum, but low risk of interference***	Wireless using unregulated spectrum; proprietary interfaces

Observations

Application of Use Cases to Risk Framework

- Easier to classify lower risk applications (attributes)
  - Standalone
  - Narrowly defined functions
  - Less variability in context of use
- Harder to classify more complex software precisely (“it depends”)
  - More dependent on context of use
  - More complex software to develop and QA
  - Greater effort and expertise required to implement
  - More interfaces to other systems
  - Greater reliance on QMS process and risk controls for known failure rates

Policy Implications

- Define clearer criteria for software functions that are not regulated, but may have transparency labeling requirements
- Define clearer criteria for software functions that warrant regulation, or at least greater attention
- Create a robust surveillance mechanism to track adverse events and near misses for the majority of software functions that lie in between

Current FDA Medical Device Regulation

Class	Risk	FDA Requirements
Enforcement Discretion A/K/A Class 0	Negligible	None applied.
Class I	Low	• Two levels—class I, quality system requirement; class II, no quality system requirement • Quality system requirements change manufacturing operations in ways beyond normal ISO quality standards • Also paperwork requirements (e.g. adverse event reporting, facility registration and listing)
Class II	Medium	• Two levels—class I, no premarket clearance; class II, premarket clearance • The software cannot go on the market typically until the manufacturer proves to FDA is "substantially equivalent" to other software already on the market. Review cycle is 90-180 days usually.
Class III	High	Same as class I, but also premarket approval • Must develop clinical evidence, and a longer FDA review cycle (may take 2-5 years).

DRAFT

Medical Device Regulation

Innovation Impact Review

Pros

- Process control, not product definition:
  - Consistent manufacturing process that can be applied to software
  - Supports innovation in new products
- Good manufacturing Process has increased the confidence in resulting products
- Contains a post-marketing surveillance program

Cons

- Clarity
  - Who is subject to regulation?
  - Implementation barriers – knowledge & overly prescriptive
- Geared especially but not exclusively to physical devices
  - Turnaround time
  - Configuration and extension
  - "Class Up" effect on software working with device
  - But, can be applied to software with some modifications recognizing differences between physical devices and software
- Blood Bank use case
  - Commonly presented as a negative use case
  - Requires more in-depth review for lessons learned
- Entry impedance:
  - Need way lower burden of applying these regulations to new development and to products that started small without regulation, but then have regulation applied after the development and initial use

ONC Certification Regulation

Innovation Impact Review

- Motivation: defined product
  - Government is funding a capital improvement to healthcare practice (link to *Meaningful Use*)
  - Therefore, obligation to promote good products
  - Therefore, certification of the products
- Effect on innovation:
  - Specification of specific software behaviors and certifying specific test behaviors limits innovation
  - Narrows solutions to problems to a prescribed solution
  - Working to the test – “Compliance Innovation”

ONC Certification Regulation

Specific Recommendations to Promote Innovation

- Increase the flexibility of compliance
  - Define the desired features
  - Avoid specific implementations in the description
  - Increase flexibility of compliance certification
- Avoid requirements dependent on effectively a single source (e.g. current regulations which relate to SureScripts)
- Increase predictability
  - Staging the definition of the requirements versus having a defined roadmap of features
  - Re-certification criteria

DRAFT

Comparison of Approaches

Innovation Impact Review

Medical Device Regulation

- Process control – e.g., current good manufacturing process
- Pre-marketing approval – in some cases
- Impact
  - Can be positive when combining software from different sources – increased trust
  - Lack of clarity (flipside of regulatory discretion) yields policy uncertainty
  - Entry impedance
    - Clarity on requirements & process – purpose of AAMI report
    - Late entry into process with existing product
  - Continued overhead: heavy process versus agile development – need for scaling of process
  - If fully applied to HIT and local implementation, devastating to market – Blood Bank example

Certification Regulation

- Product definition
- "Best Practice" feature definitions
- Pre-use approval
- Impact
  - Reduced flexibility (specific detailed requirements), reduced innovation
  - Empowered added private regulation
  - Non-productive work to test – "Compliance Innovation"
  - Less market neutral – favors existing software with defined features

Regulations—Questions Addressed

1. Are the three regulatory systems – ONC, FCC and FDA – deficient in any way with regard to how HIT is regulated?
2. Are there ambiguities in the three regulatory systems that need to be clarified so that HIT vendors and others can proceed more easily to innovate?
3. Do any of the three regulatory systems duplicate one another, or any other legal, regulatory or industry requirement?
4. Setting aside existing approaches, is there a better way to assure that innovation is permitted to bloom, while safety is assured?

FDA Issues

A = Ambiguous, B = Broken at the written law level,
C = Existing mechanism for immediate relief

Item	Issue: A, B or C	Description of challenge
Wellness/disease borderline	A, B, C	FDA needs to explain how to discern disease related claims from wellness, and needs to deregulate low risk disease related claims
Accessory issues	A, B, C	FDA needs to explain its position on which basic IT elements are regulated when connected to a medical device, and deregulate or down-regulate those that are low risk
CDS software	A, C	FDA needs to explain which forms of clinical decision support software it regulates
Software modularization	A, C	FDA needs to specify its rules for deciding the regulatory status of software modules either incorporated into a medical device, or accessed by a medical device

FDA Issues

A = Ambiguous, B = Broken at the written law level,
C = Existing mechanism for immediate relief

Item	Issue: A, B or C	Description of challenge
QS application to standalone software	A, C	FDA needs to explain how the quality system requirements and facility registration apply to manufacturing of standalone software
Premarket requirements for interoperable devices	A	FDA needs to adopt a paradigm for reviewing software that is intended to be part of a larger, but unspecified, network. Could build on the efforts of a working group of companies, academics, and hospitals that developed and submitted a pre-IDE regulatory submission to help refine the FDA clearance process.
Postmarket requirements for networks	A, B	Responsibilities for reporting adverse events and conducting corrective actions can be clarified, but also likely need a new approach that reflects shared responsibility across users, producers, and across regulatory agencies

Current FDA Program Mechanisms that Could Enable Innovation

- FDA should actively establish a policy of "Enforcement Discretion" for **lowest**-risk HIT, where enforcement of regulations is inappropriate
- FDA should assess exemption from GMP for **lower**-risk HIT
- FDA should expedite guidance on HIT software, mobile medical apps and related matters
- FDA lacks internal coordination on HIT software, and mobile medical apps policies and regulatory treatment
- FDA should utilize external facing resources to proactively educate the public about how policies and regulation impact HIT and MMA
- There may exist a need for additional funding to appropriately staff and build FDA expertise in HIT and mobile medical apps

ONC Issues

A = Ambiguous, B = Broken at the written law level, C= Capability that is underused

Item	Issue: A or B	Description of challenge
Mandatory elements	B	ONC program does not include capability in law enforcement, nor its programs framed with mandates where necessary
Assurance of Safe Configuration	A	Safety depends on appropriate post-installation configuration. No means to educate or require compliance with documented and evolving best practices
Certification program	B	ONC should avoid regulatory rules and certification test cases that endorse a specific solution or implementation to a desired feature.
Program review	C	ONC does a good job of periodically reviewing its programs and getting rid of those that are no longer necessary. We would like to see them do more of this.

FCC Issues

A = Ambiguous and B = Broken at the written law level

Item	Issue: A or B	Description of challenge
Pre-Installation Assessment	A	Planning for deployment of wireless technologies is difficult in spectrum-crowded, interference-prone environments (i.e. most hospitals). Pre-clinical test and evaluation tools and environments could help manufacturers and healthcare delivery organizations. (FCC “wireless test bed” initiative)
Post-installation Surveillance	A	Spectrum management and identification, diagnosing, and resolving wireless co-existence/Electromagnetic Compatibility (EMC)problems that affect HIT and medical device performance (in healthcare facilities and mHealth environments)

Cross-Agency Issues

Item	Description of challenge
Coverage of interoperability issues FDA/ONC	Unclear and incomplete responsibility over ensuring needed interoperability. ONC may regulate HIT/medical device interface and FDA regulates med device/med device interface. But same med device (e.g. infusion pump) could be installed in either configuration. Who is responsible for resolving? More generally, who will require interoperability when products need to be interoperable to be used safely?*
FCC/FDA review	FCC and FDA do not coordinate their review processes on converged medical devices that are brought independently before both agencies (FCC's equipment authorization program and FDA's premarket review). Coordination between agencies should be transparent and help ensure consistency thereby eliminating duplicative, time consuming, and costly hurdles.
FCC/FDA conformity assessment	Incomplete/missing clinically focused wireless conformity assessment tools that would facilitate safety and co-existence analysis

*See interoperability FDA Pre-IDE regulatory research project: http://www.mdpnp.org/MD_PnP_Program___MDISWG.html

Issues Error/Adverse Event Reporting

A = Ambiguous and B = Broken at the written law level

Item	Issue: A or B	Description of challenge
Difficult to obtain data for system performance analysis	A	When medical device-HIT "system related" adverse events occur, it is often difficult or impossible to find the root cause of the failure. Data logs may be incomplete, inaccessible, non-existent, not in standardized format.
Root cause of events may span regulated and non-regulated space	B	What is best model for reporting and analyzing issues with systems of devices/equipment that span (multiple agency) regulated and non-regulated space? Group surveyed existing approaches: NHTSA, CPSC, ASRS, FDA MedSun and ASTERD, NTSB, and PSOs. Further analysis needed. Notion of a new construct - Health IT Safety Administration* ("HITSA") was discussed. Broad stakeholder involvement emphasized.
Adverse events should be accessible early and broadly	B	Current reporting pathway often does not facilitate timely resolution. Broader access to safety and performance data to enable timely improvements was emphasized.

*See http://www.mdpnp.org/uploads/HITSA_draft_Goldman_2011.pdf

Specific Recommendations (I)

- FDA Classification
  - ❑ HIT should not be subject to FDA premarket requirements, except:
    - ✓ Medical device accessories (to be defined clearly by FDA)
    - ✓ Certain forms of high risk clinical decision support, such as Computer Aided Diagnostics (to be defined clearly by FDA)
    - ✓ Higher risk software use cases per the Safety WG report, including those where the intended use elevates aggregate risk
    - ✓ Vendors should be required to list products which are considered to represent at least some risk if a non-burdensome approach can be identified to doing so
  - ❑ To develop better post-market surveillance of HIT, through a collaborative process with stakeholder participation:
  - – Should include spontaneous reporting
  - – Also post-implementation testing to ensure key safety-related decision support is in place[1]
  - – Approaches are needed to allow aggregation of safety issues at the national level, including federal support
  - ❑ This approach would be provisional, to be re-examined periodically

Specific Recommendations (II)

- We recommend the following areas be further developed which may be accomplished through either private and/or public sector efforts:
  - ❑Adoption of existing standards and creation and adoption of needed new standards
  - ❑A public process for customer rating of HIT to enhance transparency

Measurement of Regulatory Impact on Innovation

General Attributes / Requirements

IOM Report, Appendix D

Stringency  **Innovation** 

Flexibility  **Innovation** 

– Defined as the number of implementation paths to meet compliance.

.

Information  **Innovation** 

– Defined as if a regulation promotes more or less complete information in the market.

Lessons Learned

Recommendations for a New Regulatory Framework

- Certification regimens should be used judiciously
  - When specifying specific implementations, they can narrow creativity and innovation to a specific or narrowed list of solutions
    - Some instances where narrowing choice desirable: e.g., interoperability standards
  - Innovation impact
    - Channel energy into working to the test – compliance innovation
    - Channel the discussion to definitional terms rather than meeting the market needs
- Transparency of results to supplement or replace certification
  - Instead of a certification process to differentiate the market, use transparency
  - Transparency in the marketplace is more efficient and richer in content
    - Certification just reveals that the system passed the certification test and all vendors will – at that point, there is no differentiation
- National goals should be encouraged – JCAHO, Meaningful Use
  - They meet the "flexibility" test (Appendix D – IOM Report)
  - Set problem agenda, not product agenda
  - They do change and, if well set, correct the market and create markets
  - Where the market goes, vendors will follow

Innovation Requirements

Sources of Innovation: Full Spectrum of the SocioTechnical System

- Developed software – vendor and local
- Software setup / customization / extensions
  - Integration with medical processes – sociotechnical system
- Combining technologies
  - Communication devices
  - Predictable combinations (e.g., HL7 interfaces)
  - Non-predictable combinations (e.g., end user combination of available technologies – software and hardware)

Summary of Recommendations for a New Framework (I)

- National accountability
  - Outcomes assessment rather than product definitions
  - National and international standards for quality process – measureable and transparent
  - National interoperability standards to lower the entry cost through full participation of affected stakeholders
  - Encourage configuration and extension to support process and solve problems
  - Transparency of product and results
  - Support ability to experiment or iteratively develop
  - Aggregation of safety issues at a national level

Summary of Recommendations for a New Framework (II)

- Local control, local accountability
  - Design, document, and prove a local control system
  - Accreditation of the software implementation process – e.g., through an entity such as JCAHO
  - Scope
    - Local configuration of software
    - Local extensions of software
    - Ability to iteratively develop, implement, and measure changes
    - Integration with medical processes
    - Training of end users
    - Sharing of lessons learned
    - Surveillance by the organization
    - Post-implementation testing

IOM Report

Imaging a different regulatory framework

- To encourage innovation and shared learning environments, the committee adopted the following general principles for government oversight:
  - Focus on shared learning,
  - Maximize transparency,
  - Be non-punitive,
  - Identify appropriate levels of accountability, and
  - Minimize burden

DRAFT

Comparison Between Current Approach and a New Framework

Current Regulation

- Defined solution
- Slow response to innovation and problems
- Opaque results
- Discourages participation

Learning Environment

- Multiple solutions
- Continuous innovation
- Continuous measurement of results
- Encourages participation

Overall Summary

- Have described a taxonomy for considering what the bounds are for what is HIT
- Have proposed recommendations around development of a risk framework which may be useful in considering whether or not regulation is needed
- Have described current regulatory frameworks, potential new approaches, and deficiencies, ambiguities and duplication in current frameworks
- Have described what we believe will be helpful to promote innovation in both the short and long term and maintain patient safety
- Have tried to illustrate with use cases all the above

Overall Recommendations (I)

- Definition of what is included in HIT should be broad but have also described exclusions
- Patient-safety risk framework and examples should be used as building blocks to develop a more robust and transparent framework
- The agencies should address the deficiencies, ambiguities and duplication the FDASIA group has identified
- New frameworks with some of the characteristics aimed at stimulating innovation may be helpful

Overall Recommendations (II)

- Substantial additional regulation of HIT beyond what is currently in place is not needed and would not be helpful (should be Class 0), except for:
  - ✓Medical device data systems (MDDS)
  - ✓Medical device accessories
  - ✓Certain forms of high risk clinical decision support
  - ✓Higher risk software use cases
    - For the regulated software, it will be important for the FDA to improve the regulatory system

Overall Recommendations (III)

- In addition, we believe that as recommended by the IOM Committee:
  - Vendors should be required to list products which are considered to represent at least some risk and a non-burdensome approach should be developed for this
  - Better post-market surveillance of HIT is needed
    - Standard formatting of involved reports
    - Also post-implementation testing
    - Approaches to allow aggregation of safety issues at the national level, including federal support to enable this
  - FDA and other agencies need to take steps to strongly discourage vendors from engaging in practices that discourage or limit the free flow of safety-related information