A BAA is not a BAAnd-Aid

Alternative Contracting & Health Data Use Agreements

Speakers

MOHAMMAD AMER

Director and Assistant General Counsel,
Global Data Privacy Legal
3M

mamer2@mmm.com

TRINITY CAR

Managing Counsel, Privacy
Syneos Health

trinity.car@syneoshealth.com

JOANNE CHARLES

Senior Corporate Counsel
Microsoft

jocharle@microsoft.com

ELLIOT GOLDING

Partner
McDermott Will & Emery

egolding@mwe.com

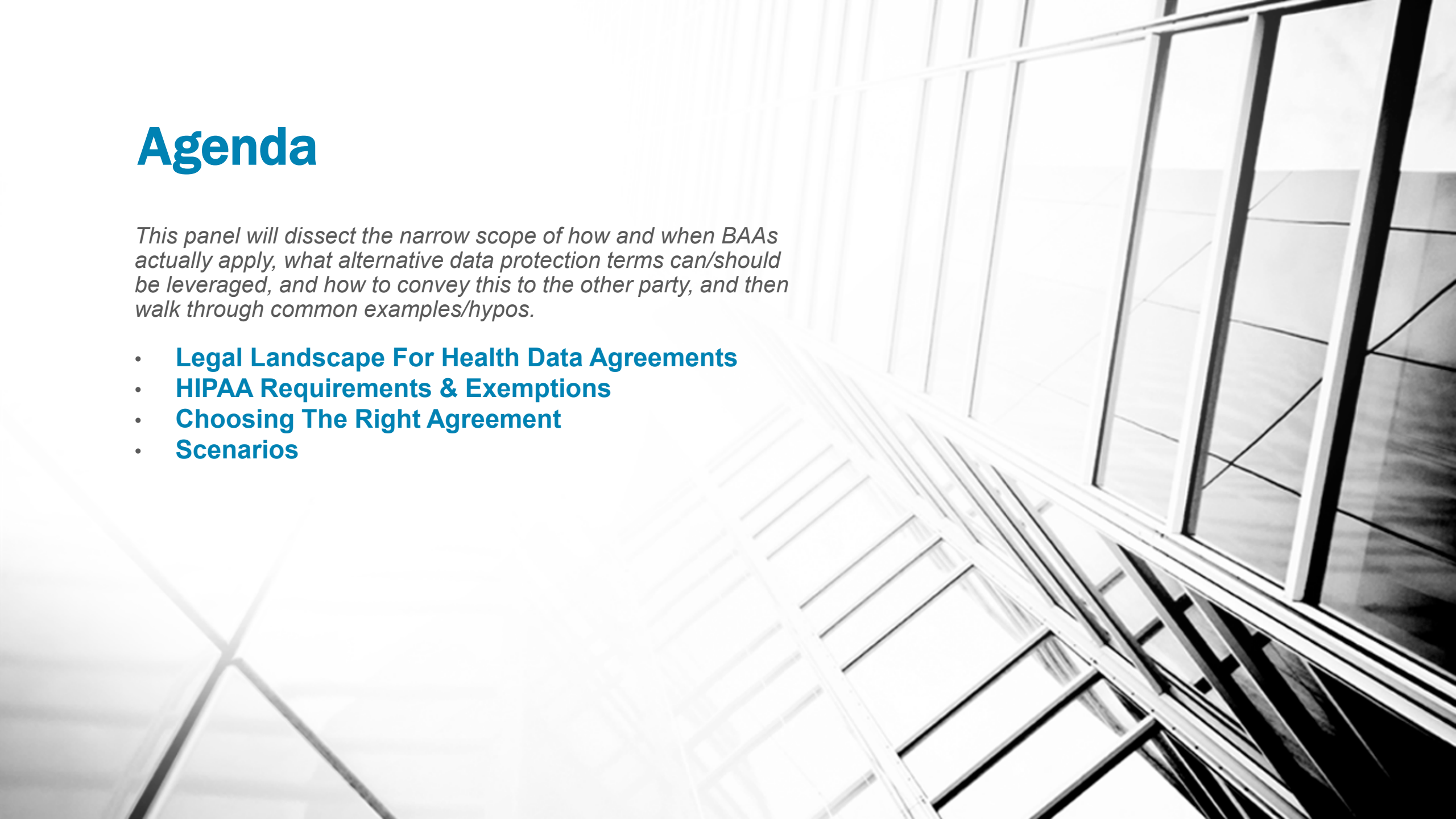
Legal Disclaimer

The information contained in this presentation and delivered as part of this presentation is for educational and informational purposes only. The views, opinions and positions expressed by the panelists are theirs alone and do not necessarily reflect the views, opinions or positions of their employers, affiliated organizations or the Privacy + Security Forum.

Agenda

This panel will dissect the narrow scope of how and when BAAs actually apply, what alternative data protection terms can/should be leveraged, and how to convey this to the other party, and then walk through common examples/hypos.

- **Legal Landscape For Health Data Agreements**
- **HIPAA Requirements & Exemptions**
- **Choosing The Right Agreement**
- **Scenarios**



Legal Landscape for Health Data

Federal & State Statutes / Rules

- HIPAA/HITECH
- 42 CFR Part 2 (substance use disorder)
- ONC Information Blocking and CMS Interoperability Regs
- Federal Trade Commission (FTC) Act Section 5 Authority
- Common Rule / FDA Human Subjects Research Regulations
- Other federal laws (COPPA, FCRA, GLBA)
- Federal health program rules (Medicare, Medicaid)
- State health information privacy laws (mental health, HIV/AIDS, genetic information, HIEs, etc.)
- State data breach laws
- State consumer privacy laws (CCPA, VCDPA, etc.)

Laws requiring data protection agreements

- HIPAA/HITECH
  - Business Associate Agreements
  - Data Use Agreements
- GDPR (General Data Protection Regulation)
  - Data Processing Agreements for EU personal data
- CCPA (California Consumer Privacy Act)
  - Service Provider Agreements for California consumer data
- State-specific data protection laws
  - Various agreements depending on state requirements
- Industry-specific regulations
  - Financial (e.g., GLBA), education (e.g., FERPA), etc.

HIPAA & HITECH: The Rules

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Among other things, required the creation of national standards to protect the privacy and security of protected health information (PHI)
- Predates most modern online and mobile services and excludes health information created or managed by patients themselves

The Health Information Technology for Economic and Clinical Health Act (HITECH)

- Enacted in 2009 to cover the proposed increase in the use of electronic PHI 9or ePHI) through electronic health records (EHRs)

Privacy, Security, and Breach Notification Rules

- Promulgated by HHS Office for Civil Rights
- Regulate uses and disclosures of PHI (Privacy Rule), administrative, physical, and technical safeguards to protect ePHI (Security Rule), and notification requirements in the event of a breach of unsecured PHI (Breach Notification Rule)

Covered Entities and Business Associates

- A “Covered Entity” (CE) is a health plan, health care clearinghouse, or a health care provider that engages in HIPAA standard transactions (e.g., electronic claim submission for reimbursement, verification of insurance, etc.)

- A “Business Associate” (BA) is a person or entity that performs certain functions or activities for a CE (or an upstream BA) that require the BA to create, receive, maintain, or transmit PHI when providing services to the CE or upstream BA. Examples:
  - A third party administrator that assists a health plan with claims processing
  - A revenue cycle management company that processes claims for a hospital or other health care provider
  - A cloud service provider that stores PHI on behalf of a health plan or healthcare provider
  - An independent medical transcriptionist that provides transcription services to a physician
  - An attorney whose legal services to a Covered Entity involve access to PHI

- However, certain service providers are not considered BAs even if a CE discloses PHI to them to perform a function on behalf of the CE:
  - “Conduits” transmitting PHI (e.g., postal service, courier service, ISPs)
  - Financial institutions, but only if processing payments on behalf of CEs and nothing more

What does HIPAA *actually* require?

- Before a CE discloses PHI to a BA, the Privacy Rule requires that (1) the CE enter into a written agreement (BAA) with the BA, and (2) the disclosure is otherwise permitted by the Privacy Rule.
- If a BA engages a downstream service provider to perform services that require the use or disclosure of PHI, the BA must enter into a downstream BAA with the service provider that contains the same conditions and restrictions that apply to the BA.
- The Privacy Rule sets forth specific content requirements for BAAs, including provisions requiring the BA to:
  - With limited exception, use PHI only for the purposes for which it was engaged (the CE may not authorize the BA to use PHI in a way that violates the Privacy Rule)
  - Establish safeguards to protect the PHI from unauthorized use or disclosure and comply with the Security Rule
  - Assist the CE in complying with its obligations under the Privacy Rule

HIPAA vs. Non-HIPAA

	Types of Entities	Types of Data	Types of Agreements
HIPAA	• CEs • BAs	• PHI	• BAAs • Data Use Agreement
Non-HIPAA	• Self-Pay Health / Telehealth Providers • Consumer Digital Health Companies • Life sciences companies and other research organizations (typically) • Non-US institutions • Adtech	• Health data collected by healthcare providers not regulated by HIPAA • Consumer health data • Data collected for research sponsored by federal agencies or private industry • De-identified data	• Data Processing Addendum/Service Provider Agreement & SCCs • Non-Disclosure Agreements (NDA) • Other

Research

- Authorization and/or IRB waiver
- Activities Preparatory to Research (ARP)
- Research on PHI of Decedents
- Limited Data Set
- Researchers must provide representations that the use or disclosure of PHI is solely for research purposes and necessary for the research
- A Data Use Agreement (DUA) can be used to permit disclosure of a limited data set to the researcher for research, public health, or health care operations
- Documentation of death may be required for research on decedents' PHI

Research — Common Use Cases

- **Authorization and/or IRB waiver.** *No BAA needed!*
- **Activities Preparatory to Research (ARP)**. *No BAA needed!*
  - Instead, the Privacy Rule requires representations from the researcher that the use or disclosure of the PHI is solely to prepare a research protocol or similar purposes preparatory to research, that the researcher will not remove any PHI from the CE, and that the PHI for which access sought is necessary for the research purpose. See 45 C.F.R. 164.512(i)(1)(ii)
- **Research on PHI of Decedents**. *No BAA needed!*
  - Researcher must represent that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research, and, at the request of the CE, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii)
- **Limited Data Set**. *No BAA needed!*
  - You can leverage a Data Use Agreement (DUA) entered into by the researcher and the CE, permitting the covered entity to disclose a limited data set to the researcher for the purpose of research, public health, or health care operations. See 45 C.F.R. 164.514(e)

Research — Data Use Agreements

- What goes in a DUA/How is it different than a BAA?
- A DUA must do the following:
  - Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purpose of the research, and which may not include any use or disclosure that would violate Privacy Rule if done by the CE;
  - Limit who can use or receive the data; AND
  - Require the recipient to do the following:
    - Not use or disclose the information other than as permitted by the DUA or as otherwise required by law;
    - Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the DUA;
    - Report to the CE any use or disclosure of the information not provided for by the DUA;
    - Ensure that any agents, including subcontractors, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; AND
    - Not to identify the information or contact the individual.

  See 45 C.F.R. 164.215(e)

International-Specific Considerations

- Some countries prohibit exporting personal data
- The GDPR requires certain data protection measures when transferring data outside the EU
- Different countries have different standards for data security and breach notification
- BAA may not be recognized or enforceable in some countries
- The contract language in BAAs may need to be adapted to comply with local laws
- Some countries require additional contractual obligations or documentation beyond what is typically included in a BAA

AdTech – Recent Trends/Issues

- OCR issued bulletin regarding online tracking technologies in Dec. 2022
  - OCR clarified that such trackers may collect and disclose PHI
    - Authenticated vs. Unauthenticated Webpages
    - Mobile Apps
  - Privacy Rule Requirements (if applicable)
    - Permissible purpose
    - Authorization for marketing
    - **Business Associate Agreement**
  - OCR also undertaking proactive “compliance reviews”
- Federal Trade Commission
  - Two big settlements focusing on collection and tracking of sensitive health data using data collection technologies
- State laws – now require more explicit C2P (or C2C) agreements with adtech providers

Assessing Agreement Options

Analysis & Factual Considerations

Analysis Basics:
Data Flow Decision Points

- Where to start?
- What privacy laws might apply?

What personal data is involved?	What is my client's role in this data processing?	Who is the data subject? (*e.g.*, patient, research participant, consumer)
Is the data identifiable? (consider if De-identified Data vs. Limited Data Set)	What is the data source? (*e.g.*, data broker, research study, government, CE/BA)	What is the use case / purpose (primary and secondary) of this data processing? (*e.g.*, is it research)
Is the data "sensitive"? (*e.g.*, Part 2 data, state sensitive health information laws)	Who is the data recipient, and how will recipient use the data? (*e.g.*, is it a "sale"?)	What jurisdictions apply? (Domestic vs. international; state-specific considerations)

Analysis Basics:
Additional Considerations

What authorizations are required? (*e.g.*, HIPAA, Part 2)	What kind of agreements are required? (*e.g.*, Data Use Agreement, BAA, Non-Disclosure/Data Sharing Agreement, HIE Participant Agreement)	Does this health-related data require heightened security?
What privacy notice (external representations about data practices) applies and does this data processing align with the privacy notice?	What data retention requirements apply?	What other stakeholders should be involved?
How is your notice structured and delivered/to whom?	Operational/logistical issues? (*e.g.*, Application Programming Interface ("API"), integration of multiple data sources, possibility/feasibility of connecting to Health Information Exchange ("HIE"))	If working with another party, have you conducted privacy and security due diligence?

Choosing the wrong agreement

- What are the consequences of choosing the wrong agreement?
  - Business risk
  - Administrative action?
  - Civil liability?
  - Scenarios in the news…
  - Reputation
  - Data use limitations
  - Creates bad precedent

Do you need a BAAnd-Aid?

(Use Case Discussion)

Scenario 1 – Digital Health App

- LifeCo is an established German life sciences company that wants to develop a patient-facing app to facilitate the creation of patient-generated health data, including information about drug adherence, vital signs, etc.
- HubCo is a technology company with a robust health data platform that performs a variety of functions – e.g., backend hosting of mobile apps, data aggregation, analytics, technology integrations, deidentification, etc.
  - As a condition of using HubCo's services, HubCo requires data contributors to: (a) allow HubCo to use data to "improve the services"; (b) allow HubCo to create and share deidentified data (and retain such data post-termination of any contractual relationship); and (c) represent that the data contributor has obtained all necessary consents and authorizations for HubCo to perform such functions.
- LifeCo plans to use HubCo to: (a) host the app and patient data; and (b) analyze the data to inform development of clinical guidelines; and (c) push app data to provider EHRs.
- LifeCo is considering two business models: (a) partnering with HCPs in the US and EU (in which case app would also push data back to the HCP EHR); or (b) direct to consumers in the US and EU (consumers opt in to having data pushed to provider EHR)

Scenario 2 - Research

- MJET is a contract research organization (CRO) providing investigator (researcher) staffing and support to its contracted pharmaceutical client, Les Drogues.
- Les Drogues has started a clinical trial at DC University Hospital, and MJET provides several researchers and a site coordinator at its client's request. It quickly becomes apparent that more study subjects are needed to make this study successful.
- DC University Hospital, wanting to keep Les Drogues happy, sends MJET a BAA, stating that if MJET signs the BAA, DC University Hospital will send a file of potential study candidates it has "pre-pre screened" for MJET's further review and to contact these study candidates.
- MJET learns of a third-party app that collects information from individuals who are interested in becoming study subjects. This information goes beyond demographic and contact information and includes health-related information. That app either offers access to individuals in its own data pool or will execute a recruitment campaign at the direction of a client/controller.

Scenario 3A – Use of tracking technologies

- DC University Hospital (DCUH), a CE, maintains a website available to the general public.
- The website includes webpages that (a) provide general information about DCUH (e.g., information regarding DCUH's history and current leadership), (b) provide information regarding specific symptoms and health conditions and permit the visitor to search for available appointments with providers who treat those conditions, and (c) allow visitors to enter login credentials and access their medical record.
- In order to improve the user experience for certain website visitors, DCUH's web developers add a third-party session replay script to the general information webpages to track visitor activity.
- The session replay script sends individually identifying information directly to the third-party developer, who also want to use the information to track the visitor even after the visitor navigates away from the DCUH website.

Scenario 3B – Use of tracking technologies

- Same facts as 3A, but now, in order to increase brand visibility and advertise the opening of a new cancer center and oncology service line, DCUH's marketing department insists that the web developers add a tracking pixel provided by a third-party social media site, Glitter, to track and collect information across the entirety of DCUH's website.
- The marketing department intends to use the information collected by the tracking pixel to target advertisements to users on Glitter.
- The web developers are not comfortable with the request and invite you to a meeting with the marketing department.

Q&A

Thank You