

**Beyond the BAA:**  
Understanding the  
Compliance Requirements  
and Risks of Data Use  
Agreements

Aaron J. Lund, JD, LL.M., CHC, CHRC, CHPC  
Director of Corporate Compliance & Privacy  
Officer

---

---

---

---

---


---

---

---

**Disclaimer:**

The materials and views expressed  
in this presentation are the views of  
the presenter and not necessarily  
the views of Northwell Health.



---

---

---

---

---


---

---

---

**Objectives**

- What is a Data Use Agreement (“DUA”) and where are they commonly used?
- Impact of violating provisions within the DUA
- Establishing controls to minimize the risk to your organization



---

---

---

---

---

---

---

---



### What is a Limited Data Set?

- Health information that excludes certain, listed direct identifiers but may include:
  - City, state, zip code;
  - Elements of data; and
  - Other numbers, characteristics ,or codes not listed as direct identifiers.
- Must be removed to qualify as LDS:
 

<ul style="list-style-type: none"> <li>• Names</li> <li>• Postal address information</li> <li>• Telephone numbers</li> <li>• Fax numbers</li> <li>• Electronic mail addresses</li> <li>• Social Security numbers</li> <li>• Medical record numbers</li> <li>• Health plan beneficiary numbers</li> <li>• Account numbers</li> </ul>	<ul style="list-style-type: none"> <li>• Certificate/license numbers</li> <li>• Vehicle identifiers and serial numbers</li> <li>• Device identifiers and serial numbers</li> <li>• Web universal resources locators</li> <li>• Internet protocol address numbers</li> <li>• Biometric identifiers</li> <li>• Full-face photographic images and any comparable images</li> </ul>
---	---




---

---

---

---

---

---

---

---

---

---

### When is a DUA necessary?

- Anytime your are sharing data that is not de-identified in a matter that was not explicitly covered in the consent form




---

---

---

---

---

---

---

---

---

---

### When should I use a DUA instead of a BAA?

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>• BAA Required</li> <li>- Anytime a CE needs to share/transfer data that contains direct identifiers or PHI with another party.</li> </ul> | <ul style="list-style-type: none"> <li>• DUA Required</li> <li>- When a LDS is to be shared/transferred to another party</li> </ul> |
|---|---|




---

---

---

---

---

---

---

---

---

---

### A closer look at DUAs in action – CMS’s “Super BAA”

- CMS retains all ownership rights to the data files;
- The user may be used for the purposes listed within the DUA;
- The user will not allow access to the patient data except as authorized by CMS;
- The user agrees to any use or disclose of the patient data will be the minimum necessary to achieve its stated purpose;
- The user will not retain the data beyond the terms of the agreement and will provide written assurances to CMS of its destruction;




---

---

---

---

---

---

---

---

### A closer look at DUAs in action – CMS’s “Super BAA” – (continued)

- The user will establish appropriate administrative, technical, and physical safeguards that meet OMB and NIST standards;
- The user is prohibited from using unsecured telecommunications to transmit individually identifiable, bidder identifiable or deducible information derived from the patient files;
- The user agrees not to disclose any information derived from the patient data, even if the information does not include direct identifiers, if the information can, by itself or in combination with other data, be used to deduce an individual’s identity;
- The user agrees that no cell 10 or less may be displayed
- The user agrees to notify CMS of any breach of personally identifiable information from the CMS data files, loss of the data files, or disclosure to an unauthorized person within 1 hour




---

---

---

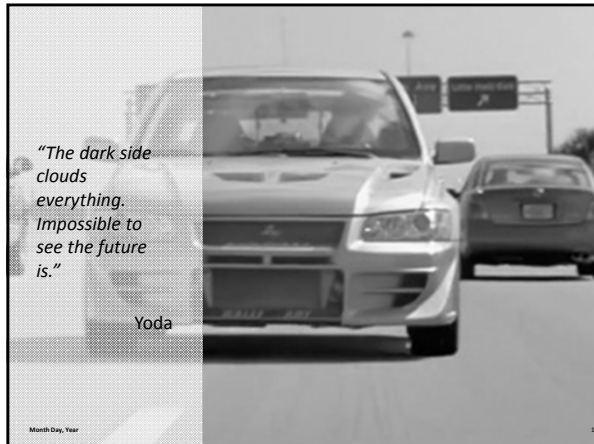
---

---

---

---

---




---

---

---

---

---

---

---

---

### Potential impact of DUA violations

- Breach of contract
- Civil penalties
  - General Penalty for Failure to Comply with Requirements and Standards (42 U.S.C. §1320d-5)
- Criminal penalties
  - Wrongful Disclosure of Individually Identifiable Health Information (42 U.S.C. §1320d-6)
  - §1106(a) of the Social Security Act (42 U.S.C. §1306(a))
  - Privacy Act (5 U.S.C. §552a(i)(3))
  - Protection of Government Property (18 U.S.C. §641)




---

---

---

---

---

---

---

---

### A closer look at civil penalties

- General Penalty for Failure to Comply with Requirements and Standards
  - Amount of penalty depends on knowledge
    - Person did not know (and by exercising reasonable diligence would not have known)
    - Reasonable cause and not willful neglect
    - Willful neglect
  - Minimum \$100 for each violation/Maximum \$50,000 for each violation
  - Not to exceed \$1.5M/calendar year




---

---

---

---

---

---

---

---

### A closer look at criminal penalties

- Wrongful Disclosure of Individually Identifiable Health Information
  - Looks to state of mind – knowingly, false pretenses, intent
  - Civil fine \$50,000 to \$250,000
  - Imprisonment up to 10 years
- Social Security Action, Section 1106, Disclosure of Information in Possession of Agency
  - Enacted to become the statutory basis for maintaining the confidentiality of SSA records
  - Prohibition against disclosures applies to any person who comes into possession of the information
  - Civil fines not to exceed \$10,000
  - Imprisonment up to 5 years




---

---

---

---

---

---

---

---

### A closer look at criminal penalties (continued)

- Privacy Rule
  - Applicable to any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses
  - Guilty of a misdemeanor
  - Fined not more than \$5,000
- Protection of Government Property
  - Applicable where it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to their own use data file(s), or received the file(s) knowing that they were stolen or converted
  - May be fined under Title 18
  - Imprisonment not more than 1 year



---

---

---

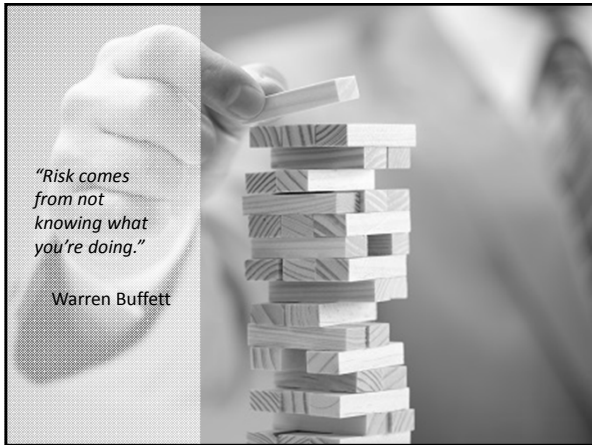
---

---

---

---

---



---

---

---

---

---

---

---

---

### Data custodians and storage

- How is the information received?
- Where is it stored once received?
- Who is the custodian of the raw data?
- Who may request data?



---

---

---

---

---

---

---

---

### Policies and Procedures

- Are policies and procedures consistent with the requirements found within the DUA?
- Confidentiality agreements with employees/handlers
- Training of employees
- Controls to approve/disapprove requests for data
- Tracking of data requests and delivery
- Obligation to report mishandling of data



---

---

---

---

---

---

---

---

### Attestations and Assurances

Through submitting this request, I affirm that the request is solely for purposes that support the ACO's participation in the MSSP, such as for clinical treatment, care management and coordination, quality improvement, and provider incentive design and implementation. I further affirm that this request is for the minimum necessary to accomplish the intended purpose of the use. Finally, I affirm that I will not disseminate the data, with or without identifiers, to anyone other than the ACO Data Team and ACO participants, providers and suppliers.



---

---

---

---

---

---

---

---

### Monitoring

- Who made the request?
- Has the requestor signed a confidentiality agreement?
- Does the request clearly articulate its intended purpose?
- Is the intended purpose within the scope of permissible use?
- Was the request for the minimum necessary?
- Did the request receive the appropriate approval?



---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---