Strafford

Presenting a live 90-minute webinar with interactive Q&A

Ensuring HIPAA Compliance When Transmitting PHI Via Patient Portals, Email, and Texting

Protecting Patient Privacy, Complying With State and Federal Regulations, Meeting Meaningful Use Standards

WEDNESDAY, JUNE 10, 2020

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Ryan P. Blaney, Partner, **Proskauer Rose**, Washington, D.C.

Adam H. Greene, Partner, **Davis Wright Tremaine**, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Overview of Presentation

1. Introduction
2. Privacy and Security of Patient Portals
3. Emailing
4. Texting
5. Don’t Forget About TCPA

Patient Interaction & Partnership

I. 99% - think social networks are useful in healthcare delivery. (2018 NEJM Catalyst Insights Council Patient Engagement Survey).

II. 84% of US consumers with smart phones/home computers – want access to electronic medical records

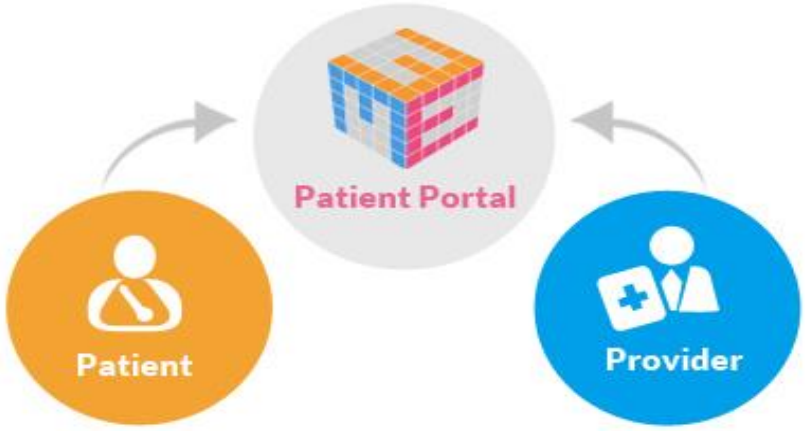
III. 41% willing to switch doctors over issue

IV. 70% of consumers believe it's important to be able to consult their providers via email.

    a. *See* Kaveh Safavi, M.D., J.D., *Accenture Consumer Survey on Patient Engagement*, Sept. 2013.

What is a Patient Portal?

I. A secure online website that gives you 24-hour access to your personal health information and medical records



Federal Regulatory Responsibilities

Health Insurance Portability and Accountability Act (HIPAA) Privacy - *April 14, 2003*

Health Insurance Portability and Accountability Act – (HIPAA) Security – *April 21, 2005*

Health Information Technology for Economic and Clinical Health Interim Act (HITECH) – *February 17, 2009*

Omnibus Final Rule – *March 26, 2013*

General Data Protection Regulations (GDPR) *May 25, 2018*

What is a Business Associate ("BA")?

I. Definition:

A. A person who (i) performs for or on behalf of a covered entity, or assists a covered entity, in performing an activity or function involving use or disclosure of health information **(e.g., claims processing, utilization review, billing)**, or (ii) provides legal, actuarial, accounting, management, administrative, accreditation or financial services where the provision of such services involves the disclosure of health information from the entity or another business associate of the entity

II. Includes anyone with health information from your health plans, providers and covered entities (could include attorneys, consultants, third party administrators, auditors, computer software service companies)

What did HITECH do for Portals?

In 2009, the HITECH Act – accelerates the changing healthcare landscape.

A. To qualify for payments from Medicare & Medicaid EHR Incentive Program, health care providers have accelerated the implementation of EHR.

Meaningful Use Measures

Patient portals are a way to meet the meaningful use requirements ("measures")

1. Core measures – i.e., providing patients with an electronic copy of their health information; providing clinical summaries for each office visit
2. Menu measures – i.e., providing patients with timely electronic access to their health information; patient-specific education resources

Patient Portal Risk Areas

I. Security

II. "User error"

   A. By patients

   B. By staff

Appropriate Topics for E-mail	Inappropriate Topics for E-mail
• Appointment reminders. • Requests for prescription refills. • Data used for chronic disease management such as vital signs. • Short questions that may be answered briefly. • Short, patient-initiated updates about non-urgent clinical treatment matters (e.g., “started the medication; no side effects).	• Urgent or time-sensitive information. • Sensitive and highly confidential subjects (e.g., HIV, psychiatric symptoms, etc.). • Complex concerns or matters requiring extended exchange.

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **Security Rule:**
  - *Risk Analysis*. Include patient portal in enterprise-wide risk analysis
    - Risks from public-facing portal
    - Risks of data at rest
  - *Risk Management*. Include in risk management plan
  - *Encryption at Rest*. Data at rest should be encrypted where reasonable

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **Security Rule:**
  - *Encryption in Transit*. Data in transit (*e.g.*, to patient) should be encrypted where reasonable
  - *Authentication*. Reasonably balancing security and usability.
    - The "X" factor – would an X spouse be able to log in as the patient? If yes, is this a reasonable risk in exchange for usability?

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **Security Rule:**
  - *System Activity Review.* Are log-in attempts reasonably monitored for potential inappropriate access?
  - *Business Associate Agreement*. Is a BAA in place with any subcontractor.
  - *Evaluation*. To what extent has the security of the software been assessed for vulnerabilities?
  - *Automatic Login*. Does automatic logoff need to be enabled?

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **Privacy Rule:**
  - *Disclosure to the Individual*. Privacy Rule permits disclosures to the individual who is the subject of the PHI.
  - *Right of Access*. Individual can choose to access designated record set information through patient portal.
    - Right to access additional designated record set PHI outside of portal.
    - Right to access same PHI through other means *(e.g.*, email or paper).

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **The Trouble with Kids …**
  - Personal representative has right to receive access to most PHI of minor.
    - Right to receive access in preferred form and format, including patient portal
  - Personal representative does not have right to access PHI if minor consents to health care him- or herself

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **The Trouble with Kids …** (cont'd)
  - State laws vary on:
    - To what health care may minor consent (e.g., reproductive health, substance use disorder treatment, mental health services, etc.)
    - At what age minor may consent (which will vary by type of health care)

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **The Trouble with Kids …** (cont'd)
  - Option #1 – Obtain minor's HIPAA-compliant authorization to provide access to all PHI to personal representative.
    - Is minor's consent voluntary?
    - Can you limit access when minor does not consent?

Privacy and Security of Patient Portals

- **The Trouble with Kids …** (cont'd)
  - Option #2 – Obtain minor's agreement that parent is involved in care, otherwise exclude.
    - Is minor's consent voluntary?
    - Can you provide parent with only PHI relevant to their involvement?

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **The Trouble with Kids …** (cont'd)
  - Option #3 – Exclude certain type of PHI from patient portal.
    - Can you sufficiently segregate the data?
    - What if portal is minor's preferred form of access? (Seems unlikely)

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Privacy and Security of Patient Portals

- **The Trouble with Kids …** (cont'd)
  - Option #4 – Exclude all PHI of minors within age of consent.
    - Obstacle to care (parents want continued access to portal information).
    - What if portal is parent's preferred form of access (for normal PHI)?

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Emailing (Between Workforce)

Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?

Answer:

The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

https://www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html

Emailing (Between Workforce)

- **Security Rule**
  - Encryption of PHI in transit is addressable.
    - Default is that all transmissions of PHI must be encrypted.
    - Encryption is not required if not reasonable and appropriate.
    - Must document if it is not reasonable and appropriate.
    - Must implement an equivalent alternative measure if reasonable and appropriate. (Not clear what that might be).

Emailing (Between Workforce)

- **Security Rule**
  - Is unencrypted email reasonable?
    - What is the burden?
    - What is the risk?
      - What is the likelihood of interception?
      - What is the impact?
  - Risk can be reduced by limiting the amount of PHI so that minimal impact if intercepted.

Emailing (Between Workforce)

- **Security Rule**
  1. Limit scope of PHI that may be emailed.
  2. Determine reasonableness (burden vs. risk).
  3. Document determination that encryption is not reasonable.
  4. Document that no equivalent alternative measures.
  5. Don’t forget other safeguards, such as confirming correct address.

Emailing (Between Workforce)

- **Privacy Rule**
  - Reasonable safeguards (see Security Rule discussion).
  - Must be for a permissible purpose.

Emailing Patients

Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C.

Emailing Patients

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual's request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html

Emailing Patients

- Two Step Process:
  1. Determine reasonableness under Security Rule.
  2. Comply with individual's preferences under Privacy Rule.

Emailing Patients

- **Security Rule:**
  - Same process as emails between workforce members:
    1. What is the burden (including on patient)?
    2. What is the risk (such as likelihood and impact of interception)?
    3. Document if encryption is not reasonable.
    4. Document that no alternative equivalent measures.
    5. Use appropriate safeguards (e.g., confirm address)

Emailing Patients

- **Privacy Rule:**
  - Patient has a right to alternative form of communication.
    - If Security Rule default allows for unencrypted emails, patient can opt out of unencrypted email.
    - If Security Rule default requires encryption, patient can opt in to unencrypted email.
      - Warn patient of risk.

Emailing Patients

"If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual."

HIPAA Omnibus Rule, 78 Fed. Reg. 5566, 5634 (Jan. 25, 2013)

Emailing Patients

- **Privacy Rule:**
  - Patient Right of Access
    - Patient is entitled to receive designated record set via unencrypted email if this is preferred form of transmission.
    - Provide patient with warning of risk of interception.
    - Confirm address.

Emailing Patients

A covered entity is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access; whether the individual's requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the covered entity's Security Rule risk analysis. See 45 CFR 164.524(c)(2) and (3), and 164.308(a)(1). However, mail and e-mail are generally considered readily producible by all covered entities. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail (except in the limited case where e-mail cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI while in transit (such as where an individual has requested to receive her PHI by, and accepted the risks associated with, unencrypted e-mail). Thus, a covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests that the copy be mailed or e-mailed.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Texting (Between Workforce)

- **Security Rule**
  - Similar analysis as unencrypted email.
  - Lesser risk of interception?
  - Additional challenge – lack of centralization
    - Limited ability to centrally monitor.
    - Copy remains on device.
  - The problem: Are prohibitions effective?
    - Consider secure alternative solution.

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Texting Patients

- Same Two Step Process:
  1. Determine reasonableness under Security Rule.
  2. Comply with individual's preferences under Privacy Rule.

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Texting Patients

Text messaging and HIPAA

There is currently a lack of clarity about whether patient consent to communicate via (unencrypted) SMS is adequate to protect covered entities from HIPAA concerns. HHS (and medical research) has released data supported use of non-encrypted SMS, given its high accessibility to patients and its efficacy in achieving behavior change (e.g. medication compliance, smoking cessation).

Many covered entitites *[sic]* feel that this use of unencrypted SMS is okay - as long as sensitive information is not communicated, and as long as it is in agreement with patients' preferences, and as long as consent is obtained. Other covered entities disagree.

What is your perspective?

https://hipaaqsportal.hhs.gov/a/dtd/Text-messaging-and-HIPAA/135929-36899#idea-tab-comments

Texting Patients

Text messaging and HIPAA

From OCR: These are important questions, and your comments are helping OCR as we develop guidance on text messaging. We will post guidance on this portal when it is finalized. Meanwhile, please continue to add questions and comments on this topic, so our responses address what you need.

https://hipaaqsportal.hhs.gov/a/dtd/Text-messaging-and-HIPAA/135929-36899#idea-tab-comments

Texting Patients

Is a BAA required with SMS service

If my provider is communicating PHI and non-PHI with patients through a 3rd party SMS service, such as Twilio, would my provider be required to sign a BAA with an SMS service company or such a company be classified as a conduit? We are sending encrypted data to the SMS service which is then sending unencrypted SMSs to patients. Patients can then potentially respond to those SMSs via unencrypted SMS which would be directed to our SMS service and then communicate the message through an encrypted channel back to my provider.

Our SMS service is not storing any information regarding patients or logs, nor is it analyzing the contents of the messages to provide any type of diagnostic feedback. It is not even determining when messages should be sent or scheduling messages. It is simply responding immediately to requests from my provider or from our patients directly.

https://hipaaqsportal.hhs.gov/a/dtd/Is-a-BAA-required-with-SMS-service/149569-36899

Texting Patients

- Is SMS provider a business associate?
  - Do they transmit PHI on your behalf? Yes.
  - Are they a conduit?
    - Do they access PHI other than on a random or infrequent basis as necessary to transmit the data or as required by law? Does their activity involve formatting or encrypting/unencrypting the PHI?
    - Do they store the PHI, other than temporary storage incident to transmission?

Educate Patients

I. Disclaimers or warnings:
   - A. Cannot create patient-physician relationship through e-mail.
   - B. No internet-based diagnosis
   - C. Do not use portal for urgent messages.
     1. In emergency, contact emergency room directly.
   - D. May be delay in response to e-mail.
   - E. Info provided through portal may be seen by others, e.g.,
     1. Those who access the patient's device.
     2. Those to whom the patient shares access.
     3. Info submitted that becomes part of the medical record.

Educate Patients

Disclaimers or warnings:

A. Protect passwords and do not share with others.

B. E-mails and texts outside portal may not be secure.

C. Notify provider of improper access or use.

D. Provider not responsible for third party content, e.g., educational material provided from others.

E. No warranty concerning any product.

F. User assumes risk related to viewing info on user's computer via a third-party network.

G. Prohibit reproduction or personal use of info protected by copyright, trademark, etc.

Portal Documentation

I. Registration form
   A. Sufficient info to identify patient and link to record.
II. Access agreement
   A. Terms and conditions of portal use.
   B. Instructions for portal use.
   C. Disclaimers and warnings.
   D. Reserve right to terminate for misuse.
   E. Acknowledgment, agreement and signature
III. Proxy agreement
   A. Sufficient info to identify patient and proxy.
   B. Define scope and warn patient of proxy rights.
   C. Signed by patient.

Train Staff

I. Flag or exclude records that should not be accessed via portal.

II. Review portal communications in timely manner.

III. Consider sending unsecure e-mail advising patient of message that is waiting for them.

IV. Do not rely on portals to communicate important info.

A. Patients may not pick it up.

B. Communicate separately by:

1. Phone or letter.

2. Unsecure e-mail or text, if patient has agreed and comply with HIPAA requirements.

Train Staff

I. Do not use e-mail to establish a patient-provider relationship.

II. Beware state telemedicine rules.

   A. Portal may trigger state limits on telemedicine, e.g.,

      1. Require in-person evaluations to prescribe medication or engage in certain other actions.

      2. Require specified consents.

   B. May cross state lines and result in unauthorized practice in the other state.

III. Ensure you comply with applicable standard of care.

IV. See AMA Guidelines for e-communication.

Train Staff

Portal may increase patient's exercise of HIPAA rights:

- Request to access records.
  - See OCR Guidance re patient's right to access information at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/.
  - Must provide records in requested format if reasonable.
- Request amendment of records.
- Accounting of disclosures.
  - HITECH allows patient to get a report of certain disclosures.
  - Proposed rule would allow patient to get a report of access for treatment, payment and operations.

(45 CFR 164.522 to .528)

The TCPA in the Health Care Context

Telephone Consumer Protection Act of 1991 (TCPA)

I. Enacted by Congress in 1991 to protect consumers by placing limitations on telemarketing "calls"

- Distinction between: residential vs. wireless calls
- Also applies to all text messaging

II. FCC issues Declaratory Rulings (DR) that sheds light on the TCPA

- July 10, 2015 DR responds to 21 requests to seek clarification under the TCPA

Residential Lines & Consent

I. Residential Lines

- Restriction on use of artificial/prerecorded voice to deliver message
  1. Unless prior express written consent
- Exemption from consent:
  1. Emergencies
  2. Noncommericial purpose
  3. Commercial purpose but not telemarketing (no advertisement)
  4. Delivery of a health care message by/on behalf of a CE or BA
  5. Message by/on behalf of tax-exempt NFP

Wireless Numbers & Consent

Contacting Wireless Numbers

- More restrictive than residential lines
- Wireless (e.g., cellphone; any service that charges a party for a call)
- Prohibitions:
  1. On use of an automatic telephone dialing system/artificial or prerecorded voice to initiate calls:
     - Advertisements and Telemarketing
       - Express, written consent required
  2. Express consent oral or written if not for advertising or telemarketing

Proskauer

Davis Wright

July 10, 2015 DR

I. TCPA applies to calls and all forms of text messages

II. Text messaging - not more similar to emailing

III. Phone-to-Phone texting similar to Internet-to-Phone text messaging

IV. TCPA and the CAN-SPAM Act
both apply to unsolicited messages

V. Limited exception for healthcare calls (calls that are subject to HIPAA)

TCPA's Healthcare Call Exception

Prior Express Consent is achieved by

- Giving a health care provide your number
  1. Only "health care" messages from a provider
     - Health care as defined under HIPAA
- Use - "within the scope of the consent given"
  1. Closely related to purpose for which the number was provided
- Providers should consider:
  1. Does the call meet HIPAA's definition of health care?
  2. Is the call within the scope of the consent?

TCPA's HealthCare Call Exception

I. Express Consent (Period of Incapacity)

- Exception applies if a person is incapacitated and a third party provides prior express consent for health care calls

II. Non-Telemarketing Healthcare Calls Exemption

- No charge to consumer for text messages, exempted from prior express consent
- Calls must be exigent and have a health care treatment purpose (e.g., appointments)
- Applies to calls subject to HIPAA (Privacy Rule)

TCPA's Healthcare Call Exception

I. Several Conditions for the non-telemarketing healthcare calls exemption include:

- Voice calls/text message - only to a patient who provides wireless number
- Voice calls/text messages – include name/contact info. of provider
- Voice calls/text messages - limited in purpose
  1. No telemarketing, solicitation, advertising or financial purpose (billing, debt collec accounting)
  2. Must comply with HIPAA
- Opting-out must be available and be honored


QUESTIONS?
COMMENTS?
CONCERNS?

Proskauer

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Thank You

Ryan P. Blaney

rblaney@proskauer.com

Adam H. Greene

adamgreene@dwt.com