McGrath | North

# You're Collecting Sensitive Personal And Financial Data From Your U.S. Clients:

## Are You Doing What Is Required To Protect It?

NAIFA NEBRASKA SUMMER CE DAY
Quarry Oaks
16600 Quarry Oaks Drive
Ashland, Nebraska 68003
August 29, 2018 / 9 – 10 AM

Tom Kelley
McGrath North Mullin & Kratz, PC LLO
(402) 633-9549
tkelley@mcgrathnorth.com
www.mcgrathnorth.com

# Cyber Risk
## Three Golden Rules For Business

1. Don’t collect personal information you don’t need.
2. Hold on to personal information only as long as you have a legitimate business need.
3. Don’t use personal information when it’s not necessary.

# Cyber Risk
## Top 10 Lessons For Business

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.

Source: FTC Start With Security, A Guide For Business, Lessons Learned From FTC Cases, June 2015

# Cyber Risk

## Top 10 Lessons For Business (cont.)

4. Store sensitive personal information securely and protect it during transmission.

5. Segment your network and monitor who's trying to get in and out.

6. Secure remote access to your network.

# Cyber Risk
## Top 10 Lessons For Business (cont.)

7. Apply sound security practices when developing new products.

8. Make sure your service providers implement reasonable security measures.

# Cyber Risk

## Top 10 Lessons For Business (cont.)

9. Put procedures in place to keep your security current and address vulnerabilities that may arise.

10. Secure paper, physical media and devices.

# Cyber Risk – Lesson #1

1. Start with security.

    - Don’t collect personal information you don’t need.
    - Hold on to information only as long as you have a legitimate business need.
    - Don’t use personal information when it’s not necessary.

# Cyber Risk – Lesson #2

2. Control access to data sensibly.

- Restrict access to sensitive data.
- Limit administrative access.

# Cyber Risk – Lesson #3

3. Require secure passwords and authentication.

   - Insist on complex and unique passwords.
   - Store passwords securely.
   - Guard against brute force attacks.
   - Protect against authentication bypass.

# Cyber Risk – Lesson #4

4. Store sensitive personal information securely and protect it during transmission.

   - Keep sensitive information secure throughout its lifecycle.
   - Use industry-tested and accepted methods.
   - Ensure proper configuration.

# Cyber Risk – Lesson #5

5. Segment your network and monitor who's trying to get in and out.

- Segment your network.
- Monitor activity on your network.

# Cyber Risk – Lesson #6

6. Secure remote access to your network.

   - Ensure endpoint security.
   - Put sensible access limits in place.

# Cyber Risk – Lesson #7

7. Apply sound security practices when developing new products.

- Train your engineers in secure coding.
- Follow platform guidelines for security.
- Verify privacy & security features work.
- Test for common vulnerabilities.

# Cyber Risk – Lesson #8

8. Make sure your service providers implement reasonable security measures.

   - Put it in writing.
   - Verify compliance.

# Cyber Risk – Lesson #9

9. Put procedures in place to keep your security current and address vulnerabilities that may arise.

   - Update and patch third-party software.
   - Heed credible security warnings and move quickly to fix them.

# Cyber Risk – Lesson #10

10. Secure paper, physical media, and devices.

- Securely store sensitive files.
- Protect devices that process personal information.
- Keep safety standards in place when data is en route.
- Dispose of sensitive data securely.

# Encryption

# Encryption – HIPAA

Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "***the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key***" (45 CFR § 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

# Encryption – HIPAA (cont.)

i. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

ii. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

# Nebraska Data Breach Law – Encryption (Part I)

Nebraska Data Breach Law (87-802(3)). Encrypted means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

# Nebraska Data Breach Law – Encryption (Part II)

Nebraska Data Breach Law (87-802(3)). Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security of the system.

# Cybersecurity Program

# Where To Begin

| U.S. Cybersecurity Framework Core |
| --- |
| **IDENTIFY**<br>(Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities) |
| **PROTECT**<br>(Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services) |
| **DETECT**<br>(Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event) |
| **RESPOND**<br>(Develop and implement the appropriate activities to take action regarding a detected cybersecurity event) |
| **RECOVER**<br>(Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event) |

M|N

| U.S. Cybersecurity Framework Core | |
|---|---|
| **Function** | **Category** |
| IDENTIFY | Asset Management |
| | Business Environment |
| | Governance |
| | Risk Assessment |
| | Risk Management Strategy |
| PROTECT | Access Control |
| | Awareness and Training |
| | Data Security |
| | Information Protection Processes and |
| | Maintenance |
| | Protective Technology |
| DETECT | Anomalies and Events |
| | Security Continuous Monitoring |
| | Detection Processes |
| RESPOND | Response Planning |
| | Analysis |
| | Mitigation |
| | Improvements |
| RECOVER | Recovery Planning |
| | Improvements |
| | Communications |

# Cyber Insurance Coverage

Third-Party Coverage: Insures for the liability of the policyholder to third parties — including clients and governmental entities — arising from a data breach or cyber attack.

First-Party Coverage: Insures for losses to the policyholder's own data or lost income or for other harm to the policyholder's business resulting from a data breach or cyber attack.

# Cyber Insurance Checklist

- ❑ Identify Your Unique Risks.
- ❑ Understand Your Existing Coverage.
- ❑ Buy What You Need.
- ❑ Secure Appropriate Limits And Sublimits.
- ❑ Beware of Exclusions.
- ❑ Consider Retroactive Coverage.
- ❑ Consider Coverage For Acts And Omissions By Third Parties.
- ❑ Evaluate Coverage For Data Restoration Costs.
- ❑ Involve All Stakeholders.

# Cyber Insurance Checklist

- ❑ Take Advantage Of Risk Management Services.
- ❑ Dovetail Cyber Insurance With Indemnity Agreements.
- ❑ Understand The “Triggers”.
- ❑ Consider Coverage For Loss Of Information On Unencrypted Mobile And Other Remote Devices.
- ❑ Consider Coverage For Regulatory Actions.
- ❑ Consider A Partial Subrogation Waiver.
- ❑ Selection Of Counsel And Other Professionals.
- ❑ Be Wary Of Warranty Statements On Applications.

# General Data Protection Regulation (GDPR)

Effective May 25, 2018 – U.S. Based Businesses

- Branch, office, subsidiary or other establishment in European Union (EU) that collects, receives, transmits, uses, stores or processes personal data?
- Offer paid or free good/services to individuals in EU?
- Monitor behavior of individuals in EU?

Professional Background:

- Admitted
  - Nebraska, 1992
  - Iowa, 2007
  - Illinois, 1989 (Inactive Member)
  - Certified Public Accountant Certificate (Inactive)
- Education
  - Notre Dame Law School J.D., Magna Cum Laude, 1989
  - Creighton University B.A., 1986
- Accomplishments
  - Listed: “Best Lawyers in America” - Privacy and Data Security Law
  - Martindale Hubbell AV Rating
  - Certified Information Privacy Professional/United States (CIPP/US), International Association of Privacy Professionals

# Thank You!

McGrath | North

Tom Kelley
P: 402.633.9549
tkelley@mcgrathnorth.com

McGrath North Mullin & Kratz, PC LLO
First National Tower, Suite 3700 | 1601 Dodge Street | Omaha, NE 68102

www.mcgrathnorth.com