

**UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF INDIANA  
NEW ALBANY DIVISION**

STATE OF INDIANA EX REL. ROKITA,

*Plaintiff,*

v.

JACKSON COUNTY SCHNECK  
MEMORIAL HOSPITAL d/b/a  
SCHNECK MEDICAL CENTER,

*Defendant.*

**CASE NO. 4:23-cv-00155**

**CONSENT JUDGMENT AND ORDER**

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by counsel, Deputy Attorney General Jennifer M. Van Dame, and Defendant, Jackson County Schneck Memorial Hospital d/b/a Schneck Medical Center (“SMC”) (collectively, the “Parties”), have agreed to the Court’s entry of this Consent Judgment and Order without trial or adjudication of any issue of fact or law.

This Order resolves the Plaintiff’s investigation of the data breach described in the Complaint filed in this action regarding SMC’s compliance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and Department of

Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”) (collectively, the “Relevant Laws”).

This Order is not intended and shall not be used or construed as an admission by Defendant of any violation of the Relevant Laws, nor shall it be construed as an abandonment by the State of its allegations that Defendant violated the Relevant Laws.

The Parties consent to entry of this Judgment and Order by the Court as a final determination and resolution of the issues alleged in the Complaint.

#### **THE PARTIES**

1. The Office of the Indiana Attorney General (“OAG”) is charged with enforcement of the Relevant Laws, including HIPAA pursuant to 42 U.S.C. § 1320d-5(d).

2. Jackson County Schneck Memorial Hospital d/b/a Schneck Medical Center (“SMC”) is an Indiana [county hospital corporation / nonprofit] with a principal office located at 411 W. Tipton Street, Seymour, IN 47274.

#### **BACKGROUND**

3. On or around September 29, 2021, SMC experienced a data breach that exposed the Personal Information and/or Protected Health Information of approximately 89,707 Indiana residents.

4. The OAG investigated this incident pursuant to the Relevant Laws.

## **STIPULATIONS**

5. The Parties agree to and do not contest the entry of this Judgment.

6. At all times relevant to this matter, SMC was engaged in trade and commerce affecting consumers in the State of Indiana insofar as SMC provided health care services to consumers in Indiana. SMC was also in possession of the Personal Information and Protected Health Information of Indiana residents.

7. At all times relevant to this matter, SMC was a Covered Entity subject to the requirements of HIPAA.

8. The Parties consent to jurisdiction and venue in this Court for purposes of entry of this Judgment as well as for the purpose of any subsequent action to enforce it.

## **JURISDICTION**

9. The Court finds that it has jurisdiction over the Parties for purposes of entry of this Judgment as well as for the purpose of any subsequent action to enforce it.

10. The Court finds that it has jurisdiction over the subject matter of this Judgment pursuant to 42 U.S.C. § 1320d-5(d), 28 U.S.C. § 1331, and 28 U.S.C. § 1367 for the purpose of entering and enforcing the Judgment, and venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1). Further, the Court retains jurisdiction for the purpose of enabling the Parties to later apply to the Court for such further orders and relief as may be necessary for the construction, enforcement, execution or satisfaction of this Judgment.

## **ORDER**

NOW THEREFORE, the Court has reviewed the terms of this Consent Judgment and based upon the Parties' agreement and for good cause shown, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED AS FOLLOWS:

### **DEFINITIONS**

11. For the purposes of this Judgment, the following definitions shall apply:

- a. "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 meaning "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information."
- b. "Breach" shall be defined in accordance with 45 C.F.R. § 164.402 to mean "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." The definition of "breach" shall also include all exclusions listed in 45 C.F.R. § 164.402(1) and (2).
- c. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103.
- d. "Covered Entity" shall be defined in accordance with 45 C.F.R. § 160.103

meaning “a health plan, health care clearinghouse, or health care provider that transmits health information in electronic form in connection with a transaction” covered by Subchapter C *Administrative Data Standards and Related Requirements*.

- e. “DCSA” means the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.*, and any related statutes and rules adopted pursuant thereto in effect on or prior to May 13, 2022. The DCSA is incorporated fully herein including all terms and definitions set forth therein.
- f. “DSBA” means the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.*, and any related statutes and rules adopted pursuant thereto in effect on or prior to May 13, 2022. The DSBA is incorporated fully herein including all terms and definitions set forth therein.
- g. “Effective Date” shall mean the date on which this Judgment is approved by the Court.
- h. “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- i. “Encrypt” or “Encryption” shall mean to render unreadable, indecipherable, or unusable to an unauthorized person through a security technology or methodology accepted generally by the National Institute of Standards and Technology (“NIST”).
- j. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the

Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and any related Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* HIPAA is incorporated fully herein including all terms and definitions set forth therein.

- k. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).
- l. “Personal Information” or “PI” shall be defined in accordance with DSBA, Ind. Code § 24-4.9-2-10.
- m. “Privacy Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ medical records and other Protected Health Information, including ePHI, that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.
- n. “Protected Health Information” or “PHI” shall be defined in accordance

with 45 C.F.R. § 160.103.

- o. “Security Incident” shall be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in accordance with 45 C.F.R. § 164.304.
- p. “Security Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ Electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.
- q. “Technical Safeguards” shall be defined in accordance with 45 C.F.R. § 164.304 and means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

### **INJUNCTIVE PROVISIONS**

WHEREFORE, TO PROTECT CONSUMERS AND ENSURE FUTURE COMPLIANCE WITH THE LAW:

#### **Compliance with Federal and State Laws**

- 8. Defendant shall comply with the HIPAA Privacy and Security Rules and shall implement all Administrative and Technical Safeguards required by HIPAA.
- 9. To the extent applicable to the Defendant, the Defendant shall comply

with DSBA and DCSA in connection with its collection, maintenance, and safeguarding of PI, PHI, and ePHI.

10. Defendant shall not make a misrepresentation which is capable of misleading consumers or fail to state a material fact if that failure is capable of misleading consumers regarding the extent to which Defendant maintains and/or protects the privacy, security, confidentiality, or integrity of PI, PHI, or ePHI.

11. Defendant shall comply with the breach notification requirements of DSBA and HIPAA, as applicable.

### **Information Security Program**

12. Overview: Within ninety (90) days after the Effective Date, Defendant shall develop, implement, and maintain an information security program (“Information Security Program” or “Program”) that shall be written and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Defendant’s operations; (ii) the nature and scope of Defendant’s activities; and (iii) the sensitivity of the personal information that Defendant maintains. At a minimum, the Program shall include the Specific Technical Safeguards and Controls in Paragraphs 18 through 31 below. Defendant may satisfy the requirements to implement and maintain the Program through review, maintenance, and as necessary, updating of an existing information security program and related safeguards, provided that such program and safeguards meet the requirements of this Judgment. Defendant shall provide the resources and support necessary to fully implement the Program so that it functions as required and



intended by this Judgment.

13. Governance: Defendant shall designate an executive or officer whose responsibility will be to implement, maintain, and monitor the Program (hereinafter referred to as the “Chief Information Officer” or “CIO”). The CIO shall have appropriate training, expertise, and experience to oversee the Program and shall regularly report to the Board of Directors (“Board”) and Chief Executive Officer (“CEO”) regarding the status of the Program, the security risks faced by the Defendant, resources required for implementation of the Program, and the security implications of Defendant’s business decisions. At a minimum, the CIO shall report any future Security Incident in accordance with the Plan identified in Paragraph 14.

14. Incident Response Plan: Defendant shall implement and maintain a written incident response plan (“Plan”) to prepare for and respond to any future Breaches. Defendant shall review and update the Plan as necessary. At a minimum, the Plan shall provide for the following phases:

- a. Preparation;
- b. Detection and Analysis;
- c. Containment;
- d. Notification and Coordination with Law Enforcement;
- e. Eradication;
- f. Recovery;
- g. Consumer and Regulator Notification; and
- h. Post-Incident Analysis and Remediation.

15. Table-Top Exercises: Defendant shall conduct, at a minimum, biannual incident response plan exercises to test and assess its preparedness to respond to Security Incidents and Breaches.

16. Training: Within ninety (90) days of the Effective Date, and at least annually thereafter, Defendant shall provide data security and privacy training to all personnel with access to PI, PHI, or ePHI. Defendant shall provide this training to any employees newly hired to, or transitioned into, a role with access to PI, PHI, or ePHI, within thirty (30) days of hire or transition. Such training shall be appropriate to employees' job responsibilities and functions. Defendant shall document the trainings and the date(s) upon which they were provided.

17. Minimum Necessary Standard: Defendant shall design and update the Program consistent with the Minimum Necessary Standard.

### **Specific Technical Safeguards and Controls**

18. Password Management: Defendant shall implement and maintain password policies and procedures requiring the use of strong, complex passwords with reasonable password-rotation requirements and ensuring that stored passwords are protected from unauthorized access.

19. Account Management: Defendant shall implement and maintain policies and procedures to manage, and limit access to and use of, all accounts with access to PI or ePHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Defendant shall not permit use of shared accounts with access to PI or ePHI.

20. Access Controls: Defendant shall implement and maintain policies and procedures to ensure that access to PI and ePHI is granted under the principle of least privilege. Such policies and procedures shall further include a means to regularly review access and access levels of users and remove network and remote access within twenty-four (24) hours of notification of termination for any employee whose employment has ended.

21. Multi-Factor Authentication: Defendant shall require the use of multi-factor authentication for remote access to Defendant's systems. Such multi-factor authentication methods should not include telephone or SMS-based authentication methods, but can include mobile applications, physical security keys, or other more secure options.

22. Asset Inventory: Defendant shall regularly inventory and classify all assets that comprise Defendant's network. The asset inventory shall, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the network; (e) the asset's criticality rating; (f) whether the asset collects, processes, or stores PI or ePHI; and (g) each security update or patch applied or installed during the preceding period.

23. Vulnerability Scanning: Defendant shall conduct regular vulnerability scanning using industry-standard tool and shall take appropriate steps to remediate identified vulnerabilities.

- a. Any vulnerability that is associated with a Security Incident shall be remediated within forty-eight (48) hours of the identification of the

vulnerability. If the vulnerability cannot be remediated within forty-eight (48) hours of its identification, Defendant shall implement compensating controls or decommission the system within forty-eight (48) hours of the identification of the vulnerability. Defendant shall maintain documentation regarding the analysis of the vulnerabilities and timeline for remediation, compensating controls and/or documentation why remediation is not available.

24. Software Updates and Patch Management: Defendant shall implement and maintain a policy to update and patch software on its network.
  - a. Defendant shall employ processes and procedures to ensure the timely scheduling and installation of any security update or patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of the Defendant's network, the impact on Defendant's operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by a U.S. government authority.
  - b. In connection with the scheduling and installation of any update and/or patch rated critical or high, Defendant shall verify that the update and/or patch was applied and installed successfully throughout the network.
25. Segmentation: Defendant shall implement and maintain policies and procedures designed to appropriately segment its network, which shall, at a

minimum, ensure that systems communicate with each other only to the extent necessary to perform their business and/or operational functions.

26. Encryption: Defendant shall Encrypt PI and ePHI at rest and in transit as appropriate, and in accordance with applicable law.

27. Logging and Monitoring: Defendant shall implement and maintain reasonable controls to centralize logging and monitoring of Defendant's network; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance. Defendant shall ensure that logs of system activity are regularly and actively reviewed and analyzed in as close to real-time as possible, that logs are protected from unauthorized access or deletion, and that appropriate follow-up and remediation steps are taken with respect to any Security Incident.

28. Intrusion Detection and Prevention: Defendant shall implement and maintain intrusion detection and prevent tools, including but not limited to firewalls and antivirus/antimalware software.

29. Penetration Testing: Defendant shall implement and maintain a risk-based penetration testing program reasonably designed to identify, assess, and remediate potential security vulnerabilities. Such testing shall occur on at least an annual basis and shall include penetration testing of Defendant's internal and external network defenses. Defendant shall review the results of such testing, take steps to remediate findings revealed by such testing, and document such remediation.

Defendant shall document the penetration test results and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon request.

30. HIPAA Risk Analysis and Risk Management Plan: Defendant shall obtain an annual risk assessment by a qualified, independent third party, which shall, at a minimum, include: the identification of internal and external risks to the security, confidentiality, or integrity of PHI or ePHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information; an assessment of the safeguards in place to control these risks; an evaluation and adjustment of the Program considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and documentation of safeguards implemented in response to such annual risk assessments. Defendant shall document the risk assessments and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon request.

31. Information Security Program Assessment: Defendant shall, within one hundred and eighty (180) days of the Effective Date, and thereafter biennially for a period of seven (7) years, submit to an assessment of its compliance with this Judgment by a qualified, independent third party (“Assessor”). Following each such assessment, the Assessor shall prepare a report including its findings and recommendations (“Security Report”), a copy of which shall be provided to the Indiana Attorney General within thirty days (30) of its completion.

- a. Within ninety (90) days of receipt of each Security Report, Defendant shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the Security Report.
- b. Within one hundred eighty (180) days of Defendant's receipt of each Security Report, Defendant shall forward to the Indiana Attorney General a description of any action Defendant takes and, if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

**Payment to the State**

32. Within thirty (30) days of the Effective Date, Defendant shall pay Two Hundred Fifty Thousand Dollars (\$250,000.00) to the Office of the Indiana Attorney General, to be used for any purpose allowable under Indiana law. For purposes of IRS Form 1098-F, all payments shall be reported in Box 2 as "Amount to be paid for violation or potential violation." To effectuate this payment and reporting, the State shall provide Defendant with an IRS Form W-9 and ACH instructions, and Defendant shall provide the State with an IRS Form W-9 upon execution of this Judgment.

**Release**

33. Following full payment of the amount due by Defendant under this Judgment, the State shall release and discharge Defendant from all civil claims that the State could have brought under the Relevant Laws, based on Defendant's conduct as set forth in the Complaint. Nothing contained in this paragraph shall be construed to limit the ability of the State to enforce the obligations that Defendant or its officers,

subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Judgment. Further, nothing in the Judgment shall be construed to create, waive, or limit any private right of action.

34. All obligations under this Consent Judgment shall expire seven (7) years from the effective date.

35. Notwithstanding any term of this Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 33 above as to any entity or person, including Defendant:

- a. Any criminal liability that any person or entity, including Defendant, has or may have;
- b. Any civil liability or administrative liability that any person or entity, including Defendant, has or may have under any statute, regulation, or rule not expressly covered by the release in Paragraph 33 above, including but not limited to, any and all of the following claims: (i) State or federal antitrust violations; (ii) State or federal securities violations; (iii) State insurance law violations; or (iv) State or federal tax claims.

### **Consequences of Noncompliance**

36. Defendant represents that it has fully read this Judgment and understands the legal consequences attendant to entering into this Judgment. Defendant understands that any violation of this Order may result in the State seeking all available relief to enforce this Order, including an injunction, civil penalties, court and investigative costs, attorneys' fees, restitution, and any other



relief provided by the laws of the State or authorized by a court. If the State is required to file a petition to enforce any provision of this Judgment against Defendant, Defendant agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Judgment against such Defendant.

### **General Provisions**

37. Any failure of the State to exercise any of its rights under this Judgment shall not constitute a waiver of any rights hereunder.

38. Defendant hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Judgment. Defendant is and has been represented by legal counsel and has been advised by its legal counsel of the meaning and legal effect of this Judgment.

39. This Judgment shall bind Defendant and its officers, subsidiaries, affiliates, agents, representatives, employees, successors, future purchasers, acquiring parties, and assigns.

40. Defendant shall deliver a copy of this Judgment to its executive management having decision-making authority with respect to the subject matter of this Judgment within thirty (30) days of the Effective Date.

41. The settlement negotiations resulting in this Judgment have been undertaken by the Parties in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

42. Defendant waives notice and service of process for any necessary filing relating to this Judgment, and the Court retains jurisdiction over this Judgment and the Parties hereto for the purpose of enforcing and modifying this Judgment and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Judgment shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Judgment is filed, and then only to the extent specifically set forth in such Judgment. The Parties may agree in writing, through counsel, to an extension of any time period specified in this Judgment without a court order.

43. Defendant does not object to *ex parte* submission and presentation of this Judgment by the Plaintiff to the Court, and do not object to the Court's approval of this Judgment and entry of this Judgment by the Clerk of the Court.

44. The Parties agree that this Judgment does not constitute an approval by the State of any of Defendant's past or future practices, and Defendant shall not make any representation to the contrary.

45. The requirements of the Judgment are in addition to, and not in lieu of, any other requirements of federal or state law. Nothing in this Judgment shall be construed as relieving Defendant of the obligation to comply with all local, state, and federal laws, regulations, or rules, nor shall any of the provisions of the Judgment be deemed as permission for Defendant to engage in any acts or practices prohibited by such laws, regulations, or rules.

46. This Judgment shall not create a waiver or limit Defendant's legal rights, remedies, or defenses in any other action by the Plaintiff, except an action to enforce the terms of this Judgment or to demonstrate that Defendant was on notice as to the allegations contained herein.

47. This Judgment shall not waive Defendant's right to defend itself, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of the Judgment, except with regard to an action by the Plaintiff to enforce the terms of this Judgment.

48. This Judgment shall not waive, release, or otherwise affect any claims, defenses, or position that Defendant may have in connection with any investigations, claims, or other matters not released in this Judgment.

49. Defendant shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Judgment or for any other purpose which would otherwise circumvent any part of this Judgment.

50. If any clause, provision, or section of this Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Judgment and this Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or other provision had not been contained herein.

51. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which shall be considered one and the same Judgment.

52. To the extent that there are any, Defendant agrees to pay all court costs associated with the filing of this Judgment.

### **Notices**

53. Any notices or other documents required to be sent to the Parties pursuant to the Judgment shall be sent by (A) email; and (B) United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. The required notices and/or documents shall be sent to:

a. For the State:

Douglas S. Swetnam  
Section Chief – Data Privacy & Identity Theft Unit  
Office of Attorney General Todd Rokita  
302 West Washington Street  
IGCS-5th Floor  
Indianapolis, IN 46204  
douglas.swetnam@atg.in.gov

Jennifer M. Van Dame  
Deputy Attorney General  
Office of Attorney General Todd Rokita  
302 West Washington Street  
IGCS-5th Floor  
Indianapolis, IN 46204  
jennifer.vandame@atg.in.gov

b. For Defendant:

James Giszczak  
McDonald Hopkins  
39533 Woodward Avenue, Suite 318  
Bloomfield Hills, MI 48304  
jgiszczak@mcdonaldhopkins.com

**IT IS STIPULATED:**

FOR THE STATE OF INDIANA

Office of Indiana Attorney General



By \_\_\_\_\_

Date: 08/14/2023

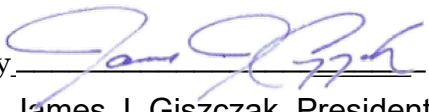
Jennifer M. Van Dame  
Attorney No. 32788-53  
Deputy Attorney General  
Office of the Indiana Attorney General  
302 West Washington Street  
Indianapolis, IN 46037  
Phone: 317-232-0486  
jennifer.vandame@atg.in.gov

FOR DEFENDANT



By \_\_\_\_\_  
Eric D. Fish, MD, President/CEO

Date: August 18, 2023 \_\_\_\_\_



By \_\_\_\_\_  
James J. Giszczak, President

Date: August 23, 2023 \_\_\_\_\_

**SO ORDERED, ADJUDGED, AND DECREED:**

By \_\_\_\_\_ Date: \_\_\_\_\_  
JUDGE

Service will be made electronically on all ECF-registered counsel of record via email generated by the court's ECF system.

Service will be made via U.S. Mail on:

Jackson County Schneck Memorial Hospital  
d/b/a Schneck Medical Center  
c/o James Giszczak  
McDonald Hopkins  
39533 Woodward Avenue, Suite 318  
Bloomfield Hills, MI 48304  
jgiszczak@mcdonaldhopkins.com